



7450 ETHERNET SERVICE SWITCH 7750 SERVICE ROUTER VIRTUALIZED SERVICE ROUTER

MULTISERVICE INTEGRATED SERVICE ADAPTER GUIDE RELEASE 16.0.R4

3HE 14142 AAAB TQZZA 01

Issue: 01

November 2018

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2018 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.

Table of Contents

1	Getting Started	15
1.1	About This Guide	15
1.2	ISA Configuration Process	17
2	ISA Hardware	19
2.1	In This Section	19
2.2	MS-ISA2 Overview	20
2.3	MS-ISA Overview	21
2.4	MS-ISM Overview	22
2.5	Application Assurance Hardware Features	23
2.5.1	AA System Support	23
2.5.2	Host IOM Support for AA on ISAs	23
3	Application Assurance	25
3.1	Application Assurance (AA) Overview	25
3.1.1	Application Assurance: Inline Policy Enforcement	26
3.1.2	AA Integration in Subscriber Edge Gateways	27
3.1.3	Fixed Residential Broadband Services	29
3.1.3.1	Dual-Stack Lite – DS-Lite	30
3.1.3.2	6to4 /6RD	32
3.1.4	Wireless LAN Gateway Broadband Services	34
3.1.5	Application-Aware Business VPN Services	35
3.1.6	Business Mobile Backhaul	37
3.1.7	SeGW Firewall Service	38
3.2	Application Assurance System Architecture	39
3.2.1	AA ISA Resource Configuration	39
3.2.1.1	AA ISA Groups	39
3.2.1.2	Redundancy	41
3.2.1.3	ISA Load Balancing	43
3.2.1.4	Asymmetry Removal	44
3.2.1.5	ISA Overload Detection	53
3.2.2	AA Packet Processing	55
3.2.2.1	Divert of Traffic and Subscribers	56
3.2.2.2	Application Identification	79
3.2.2.3	Statistics and Accounting	88
3.2.2.4	Application QoS Policy (AQP)	122
3.2.2.5	Application Assurance Firewall	145
3.2.3	Service Monitoring and Debugging	161
3.2.4	CPU Utilization	162
3.2.5	CLI Batch: Begin, Commit and Abort Commands	162
3.3	Configuring Application Assurance with CLI	165
3.3.1	Provisioning AA ISA MDA	165
3.3.2	Configuring an AA ISA Group	166
3.3.2.1	Configuring Watermark Parameters	168
3.3.3	Configuring a Group Policy	168

3.3.3.1	Beginning and Committing a Policy Configuration	168
3.3.3.2	Aborting a Policy Configuration	169
3.3.3.3	Configuring an IP Prefix List	169
3.3.3.4	Configuring AA Session Filters	170
3.3.3.5	Configuring an Application Group	172
3.3.3.6	Configuring an Application	173
3.3.3.7	Configuring an Application Filter	173
3.3.3.8	Configuring an Application Profile	174
3.3.3.9	Configuring Suppressible App-Profile with SRRP	175
3.3.3.10	Configuring Application Service Options	176
3.3.3.11	Configuring a Policer	177
3.3.3.12	Configuring an Application QoS Policy	177
3.3.3.13	Configuring an Application and DNS IP Cache for URL Content Charging Strengthening	179
3.3.3.14	Configuring an HTTP Error Redirect	182
3.3.3.15	Configuring HTTP Header Enrichment	183
3.3.3.16	Configuring an HTTP Redirect Policy	184
3.3.3.17	Configuring a Captive Redirect HTTP Redirect Policy	185
3.3.3.18	Configuring ICAP URL Filtering	188
3.3.3.19	Configuring Local URL-List Filtering	192
3.3.3.20	Configuring HTTP Notification	193
3.3.4	Configuring AA Volume Accounting and Statistics	195
3.3.4.1	Configuring Cflowd Collector	197
3.3.4.2	Configuring AA Volume, TCP and RTP Performance Reporting	197
3.4	Application Assurance Command Reference	201
3.4.1	Application Assurance Command Reference	201
3.4.1.1	Hardware Commands	201
3.4.1.2	Admin Commands	201
3.4.1.3	ISA Commands	201
3.4.1.4	Application Assurance Commands	203
3.4.1.5	AA Interface Commands	217
3.4.1.6	Persistence Commands	218
3.4.2	Command Descriptions	218
3.4.2.1	Generic Commands	219
3.4.2.2	Admin Commands	222
3.4.2.3	Application Assurance Commands	222
3.4.2.4	Group Commands	253
3.4.2.5	ISA Commands	354
3.5	Show, Tools, Clear, and Debug Command Reference	365
3.5.1	Command Hierarchies	365
3.5.1.1	Show Commands	365
3.5.1.2	Tools Commands	368
3.5.1.3	Clear Commands	369
3.5.1.4	Debug Commands	369
3.5.2	Command Descriptions	371
3.5.2.1	Show Commands	371
3.5.2.2	Tools Commands	437
3.5.2.3	Clear Commands	456
3.5.2.4	Debug Commands	457

4	IP Tunnels.....	467
4.1	IP Tunnels Overview	467
4.1.1	Tunnel ISAs	469
4.1.1.1	Public Tunnel SAPs.....	470
4.1.1.2	Private Tunnel SAPs	471
4.1.1.3	IP Interface Configuration.....	472
4.1.1.4	GRE and IP-IP Tunnel Configuration	473
4.1.1.5	IP Fragmentation and Reassembly for IP Tunnels.....	475
4.1.1.6	TCP MSS Adjustment.....	476
4.1.2	Operational Conditions	478
4.1.2.1	Dynamic Configuration Change Support for IPsec Gateway.....	479
4.1.3	QoS Interactions.....	480
4.1.4	OAM Interactions.....	480
4.1.5	Redundancy	481
4.1.6	Statistics Collection	481
4.1.7	Security.....	482
4.1.7.1	GRE Tunnel Multicast Support.....	482
4.1.7.2	IPv6 over IPv4 GRE Tunnel	483
4.1.8	IKEv2.....	483
4.1.8.1	IKEv2 Traffic Selector and TS-List	484
4.1.8.2	IKEv2 Fragmentation.....	486
4.1.9	SHA2 Support.....	487
4.1.10	IPsec Client Lockout.....	487
4.1.11	IPsec Tunnel CHILD_SA Rekey.....	488
4.1.12	Multiple IKE/ESP Transform Support	489
4.2	X.509v3 Certificate Overview	490
4.2.1	SR OS X.509v3 Certificate Support	490
4.2.2	Local Storage	491
4.2.3	CA-Profile	492
4.2.4	CA Chain Computation.....	493
4.2.5	Certificate Enrollment	493
4.2.6	Certificate Revocation Check	494
4.2.7	Certificate/CRL Expiration Warning.....	495
4.2.8	Certificate/CRL/Key Cache.....	496
4.2.9	Auto CRL Update	496
4.2.10	IPsec Client Database.....	497
4.3	Using Certificates For IPsec Tunnel Authentication	500
4.3.1	IKEv2 Digital Signature Authentication.....	500
4.4	Trust-Author Profile.....	502
4.5	Cert-Profile	503
4.6	Certificate Management Protocol Version 2 (CMPv2).....	505
4.7	OCSP	506
4.8	Video Wholesale Example.....	507
4.9	Multi-Chassis IPsec Redundancy Overview.....	508
4.9.1	Architecture	508
4.9.2	MC-IPsec Mastership Protocol (MIMP)	509
4.9.2.1	MIMP Protocol States.....	510
4.9.2.2	Election Logic	511
4.9.2.3	Protection Status	512

4.9.2.4	Other Details.....	512
4.9.3	Routing	513
4.9.3.1	Routing in Public Service.....	513
4.9.3.2	Routing in Private Services	513
4.9.3.3	Other Details About Shunting	514
4.9.4	MC-IPsec Aware VRRP	514
4.9.5	Synchronization.....	514
4.9.5.1	Automatic CHILD_SA Rekey	515
4.9.6	Responder Only	515
4.10	IPsec Deployment Requirements	516
4.11	IKEv2 Remote-Access Tunnel.....	518
4.11.1	IKEv2 Remote Access Tunnel – RADIUS-Based PSK/Certificate Authentication	518
4.11.1.1	IKEv2 Remote-Access Tunnel – EAP Authentication.....	521
4.11.2	IKEv2 Remote-Access Tunnel – Authentication without RADIUS	524
4.11.3	IKEv2 Remote-Access Tunnel – Address Assignment.....	525
4.11.3.1	DHCPv4 Address Assignment.....	526
4.11.3.2	DHCPv6 Address Assignment.....	527
4.11.3.3	DHCPv4/v6 Usage Notes	527
4.11.4	IPv6 IPsec Support	530
4.11.4.1	IPv6 as Payload.....	530
4.11.4.2	IPv6 as Payload: Static LAN-to-LAN Tunnel	530
4.11.4.3	IPv6 as Payload: Dynamic LAN-to-LAN Tunnel	531
4.11.4.4	IPv6 as Payload: Remote-Access Tunnel	531
4.11.4.5	IPv6 as Encapsulation	531
4.12	MLDv2 over IPsec	533
4.12.1	MLDv2 over IPsec – Traffic Selector	533
4.12.2	MLDv2 over IPsec – Configuration	534
4.13	Configuring IPsec with CLI	535
4.13.1	Provisioning a Tunnel ISA	535
4.13.2	Configuring a Tunnel Group	535
4.13.3	Configuring Router Interfaces for IPsec	536
4.13.4	Configuring IPsec Parameters.....	536
4.13.5	Configuring IPsec in Services.....	536
4.13.6	Configuring X.509v3 Certificate Parameters	537
4.13.7	Configuring MC-IPsec	539
4.13.7.1	Configuring MIMP.....	539
4.13.7.2	Configuring Multi-Chassis Synchronization	540
4.13.7.3	Configuring Routing for MC-IPsec.....	540
4.13.8	Configuring and Using CMPv2	542
4.13.9	Configuring OCSP	543
4.13.10	Configuring IKEv2 Remote — Access Tunnel	543
4.13.11	Configuring IKEv2 Remote — Access Tunnel with Local Address Assignment	546
4.14	IP Tunnel Command Reference	549
4.14.1	Command Hierarchies.....	549
4.14.1.1	Configuration Commands.....	550
4.14.1.2	Service Configuration Commands.....	555
4.14.2	Command Descriptions	569

4.14.2.1	Generic Commands.....	569
4.14.2.2	Hardware Commands.....	570
4.14.2.3	ISA Commands	571
4.14.2.4	Certificate Profile Commands.....	575
4.14.2.5	Client Database Commands.....	578
4.14.2.6	Internet Key Exchange (IKE) Commands.....	584
4.14.2.7	IPsec Transform Commands.....	597
4.14.2.8	IPsec Static Security Association Commands.....	601
4.14.2.9	Trust Anchor Profile/TS Commands.....	604
4.14.2.10	Tunnel Template Commands	607
4.14.2.11	Service Configuration Commands.....	611
4.14.2.12	Interface SAP Tunnel Commands	623
4.14.2.13	RADIUS Policy Commands	640
4.14.2.14	CMPv2 Commands	645
4.14.2.15	Auto-Update Command Descriptions	655
4.14.2.16	IPsec Mastership Election Commands.....	662
4.14.2.17	Show Commands	667
4.14.2.18	Debug Commands.....	717
4.14.2.19	Tools Commands	720
4.14.2.20	Clear Commands.....	723
4.14.2.21	Admin Commands.....	725
5	L2TPV3 Tunnels.....	729
5.1	L2TPv3 Overview	729
5.2	Control Plane.....	730
5.3	Public SAP.....	731
5.4	Private SAP	732
6	Video Services	733
6.1	Video Services.....	733
6.1.1	Video Groups.....	733
6.1.2	Video SAP	734
6.1.3	Video Interface	734
6.1.4	Multicast Information Policies	734
6.1.5	Duplicate Stream Protection.....	736
6.1.6	Duplicate Stream Selection	737
6.1.6.1	Stream Identification.....	737
6.1.6.2	Initial Sequence Identification.....	738
6.1.6.3	Packet Selection.....	738
6.1.6.4	Clock Recovery	739
6.1.6.5	Playout.....	740
6.1.6.6	Loss of Transport.....	740
6.1.7	Video Quality Monitoring	740
6.1.7.1	VoIP/Video/Teleconferencing Performance Measurements	747
6.1.7.2	Mean Opinion Score (MOS) Performance Measurements Solution Architecture	748
6.2	Retransmission and Fast Channel Change.....	749
6.2.1	RET and FCC Overview	749
6.2.1.1	Retransmission.....	749

6.2.1.2	Fast Channel Change (FCC).....	750
6.2.1.3	RET and FCC Server Concurrency.....	756
6.2.2	Separate Timers for FCC and RET.....	757
6.2.3	Peak Bandwidth and Sessions per ISA.....	757
6.3	Ad Insertion.....	758
6.3.1	Local/Zoned Ad Insertion.....	758
6.3.1.1	Transport Stream Ad Splicing.....	758
6.3.1.2	Ad Zones.....	760
6.3.1.3	Local/Zoned ADI Prerequisites and Restrictions.....	761
6.4	Configuring Video Service Components with CLI.....	763
6.4.1	Video Services Overview.....	763
6.4.1.1	Configuring an ISA-MS Module.....	765
6.4.1.2	Configuring a Video Group.....	765
6.4.1.3	Configuring a Video SAP and Video Interface in a Service.....	766
6.4.1.4	Basic Multicast Information Policy Configuration.....	767
6.4.2	Sample Configurations.....	768
6.5	Configuring RET/FCC Video Components with CLI.....	775
6.5.1	Configuring RET/FCC Video Features in the CLI.....	775
6.5.1.1	Configuring the RET Client.....	775
6.5.1.2	Configuring the RET Server.....	778
6.5.1.3	Configuring the FCC Server.....	782
6.5.1.4	Logging and Accounting Collection for Video Statistics.....	785
6.6	Configuring ADI Components with CLI.....	787
6.6.1	Configuring ADI in CLI.....	787
6.6.1.1	Configuring the RET Client.....	787
6.6.1.2	Configuring a Video Group.....	787
6.6.1.3	Configuring NTP.....	788
6.6.1.4	Configuring Channel Parameters.....	788
6.6.1.5	Configuring Service Entities.....	789
6.7	Video Services Command Reference.....	791
6.7.1	IP-TV Command Hierarchies.....	791
6.7.1.1	Hardware Commands.....	791
6.7.1.2	Video Group Commands.....	791
6.7.1.3	Video Policy Video Commands.....	792
6.7.1.4	Bundle and Channel Commands.....	793
6.7.1.5	Service Video Interface Commands.....	796
6.7.2	Command Descriptions.....	799
6.7.2.1	Generic Commands.....	799
6.7.2.2	LNS Group Commands.....	800
6.7.2.3	Video Group Commands.....	801
6.7.2.4	Multicast Info Policy Commands.....	806
6.7.2.5	Video Policy Commands.....	814
6.7.2.6	Bundle and Channel Commands.....	822
6.7.2.7	Service Video Interface Commands.....	833
6.8	Show, Clear, and Debug Command Reference.....	841
6.8.1	Command Hierarchies.....	841
6.8.1.1	Show Commands.....	841
6.8.1.2	Clear Commands.....	841
6.8.1.3	Debug Commands.....	842

6.8.2	Command Descriptions	842
6.8.2.1	Show Commands	843
6.8.2.2	Clear Commands.....	856
6.8.2.3	Debug Commands.....	859
7	Network Address Translation	863
7.1	Terminology	863
7.2	Network Address Translation (NAT) Overview	866
7.2.1	Principles of NAT	866
7.2.2	Application Compatibility	867
7.3	Large Scale NAT	869
7.3.1	Port Range Blocks.....	869
7.3.1.1	Reserved Ports and Priority Sessions	870
7.3.1.2	Preventing Port Block Starvation.....	871
7.3.2	Timeouts.....	874
7.3.3	Watermarks	874
7.4	L2-Aware NAT	875
7.5	One-to-One (1:1) NAT	877
7.5.1	Static 1:1 NAT	877
7.5.1.1	Protocol Agnostic Behavior	879
7.5.1.2	Modification of Parameters in Static 1:1 NAT	879
7.5.1.3	Load Distribution over ISAs in Static 1:1 NAT	880
7.5.1.4	NAT-Policy Selection.....	880
7.5.1.5	Mapping Timeout.....	882
7.5.1.6	Logging.....	882
7.5.1.7	Restrictions.....	882
7.5.2	ICMP.....	882
7.6	Deterministic NAT.....	883
7.6.1	Overview.....	883
7.6.2	Supported Deterministic NAT Types	883
7.6.3	Number of Subscribers per Outside IP and per Pool	884
7.6.4	Referencing a Pool	884
7.6.5	Outside Pool Configuration.....	884
7.6.6	Mapping Rules and the map Command in Deterministic LSN44	890
7.6.7	Hashing Considerations in Deterministic LSN44	893
7.6.7.1	Distribution of Outside IP Addresses Across MS-ISAs in an MS-ISA NA Group.....	895
7.6.8	Sharing of Deterministic NAT Pools	895
7.6.9	Simultaneous support of dynamic and deterministic NAT	895
7.6.10	Selecting Traffic for NAT	895
7.6.11	Inverse Mappings	896
7.6.11.1	MIB approach	896
7.6.11.2	Off-line Approach to Obtain Deterministic Mappings	896
7.6.12	Logging.....	898
7.6.13	Deterministic DS-Lite.....	898
7.6.13.1	Hashing Considerations in DS-Lite.....	900
7.6.13.2	Order of Configuration Steps in Deterministic DS-Lite	901
7.7	Destination Based NAT (DNAT).....	905
7.7.1	Combination of SNAPT and DNAT.....	905

7.7.2	Forwarding Model in DNAT	906
7.7.3	DNAT Traffic Selection via NAT Classifier	907
7.7.4	Configuring DNAT	907
7.7.4.1	DNAT Traffic Selection and Destination IP Address Configuration	908
7.7.4.2	Micro-Netting Original Source (Inside) IP Space in DNAT-Only Case	909
7.8	LSN – Multiple NAT Policies per Inside Routing Context	911
7.8.1	Restrictions.....	911
7.8.2	Multiple NAT Policies Per Inside Routing Context.....	911
7.8.3	Routing Approach for NAT Diversion	913
7.8.4	Filter-Based Approach.....	914
7.8.5	Multiple NAT Policies with DS-Lite and NAT64	914
7.8.6	Default NAT Policy	915
7.8.7	Scaling Considerations.....	915
7.8.8	Multiple NAT Policies and SPF Configuration Considerations	916
7.8.8.1	Multiple NAT Policies and Forwarding Considerations.....	917
7.8.9	Logging.....	918
7.9	L2-Aware NAT Destination-Based Multiple NAT Policies.....	921
7.9.1	Logging.....	922
7.9.1.1	RADIUS Logging and Nat-Policy Change via CoA.....	922
7.9.1.2	Delay Between the NAT Resource Allocation and Logging During CoA.....	925
7.9.2	Static Port Forwards	925
7.9.3	L2-Aware Ping	926
7.9.4	UPnP	928
7.10	NAT and CoA	929
7.10.1	CoA and NAT Policies	929
7.10.2	CoA and DNAT.....	930
7.10.3	Modifying an Active NAT Prefix List or Nat Classifier via CLI.....	934
7.11	Port Control Protocol (PCP)	936
7.12	Universal Plug and Play Internet Gateway Device Service	939
7.12.1	Configuring UPnP IGD Service	940
7.13	NAT Point-to-Point Tunneling Protocol (PPTP) Application Layer Gateway (ALG).....	941
7.13.1	PPTP Protocol.....	941
7.13.1.1	Supported Control Messages	941
7.13.1.2	GRE Tunnel.....	942
7.13.2	PPTP ALG Operation	943
7.13.3	Multiple Sessions Initiated From the Same PPTP Client Node	946
7.13.4	Selection of Call IDs in NAT	947
7.14	Modifying Active Nat-Prefix-List or NAT Classifier via CLI	948
7.15	NAT Logging.....	950
7.15.1	Syslog/SNMP/Local-File Logging	950
7.15.1.1	Filtering LSN Events to System Memory.....	951
7.15.1.2	NAT Logging to a Local File	958
7.15.2	SNMP Trap Logging	958
7.15.3	NAT Syslog.....	959
7.15.4	LSN RADIUS Logging	960
7.15.4.1	Periodic RADIUS Logging	966

7.15.4.2	RADIUS Logging and L2-Aware NAT	968
7.15.5	LSN and L2-Aware NAT Flow Logging	969
7.15.5.1	IPFIX Flow Logging	970
7.15.5.2	Template Formats	971
7.15.5.3	Template Format1 and Format2	974
7.15.5.4	Configuration Example	975
7.15.5.5	Syslog Flow Logging	977
7.16	DS-Lite and NAT64 Fragmentation	982
7.16.1	Overview	982
7.16.2	IPv6 Fragmentation in DS-Lite	983
7.16.3	NAT64	984
7.17	DS-lite Reassembly	985
7.17.1	Interpreting Fragmentation Statistics	985
7.18	Enhanced Statistics in NAT — Histogram	988
7.18.1	Configuration	989
7.19	NAT Redundancy	991
7.19.1	NAT Stateless Dual-Homing	992
7.19.1.1	Configuration Considerations	994
7.19.1.2	Troubleshooting Commands	996
7.19.2	Active-Active ISA Redundancy Model	999
7.19.2.1	Start Up Conditions	1002
7.19.2.2	Recovery	1002
7.19.2.3	Adding Additional ISAs in the ISA Group	1003
7.19.3	L2-Aware Bypass	1003
7.19.3.1	Sharing IP Addresses in L2-Aware NAT	1005
7.19.3.2	Recovery	1005
7.19.3.3	Default Bypass During Reboot or MS-ISA Provisioning	1006
7.19.3.4	Logging	1006
7.20	ISA Feature Interactions	1007
7.20.1	MS-ISA Use with Service Mirrors	1007
7.20.2	LNS, Application Assurance and NAT	1007
7.20.3	Subscriber Aware Large Scale NAT44	1007
7.21	Mapping of Address and Port Using Translation (MAP-T)	1017
7.21.1	MAP-T Rules	1019
7.21.2	A+P Mapping Algorithm	1020
7.21.3	Routing Considerations	1021
7.21.4	Forwarding Considerations in the BR	1023
7.21.4.1	IPv6 Addresses	1023
7.21.4.2	1:1 Translations and IPv4 Prefix Translations	1024
7.21.4.3	Hub-And-Spoke Topology	1024
7.21.4.4	Rule Prefix Overlap	1025
7.21.5	BMR Rules Implementation Example	1025
7.21.6	ICMP	1027
7.21.7	Fragmentation	1028
7.21.7.1	Fragmentation in the Downstream Direction	1028
7.21.7.2	Fragmentation in the Upstream Direction	1029
7.21.7.3	Fragmentation Statistics	1030
7.21.8	Maximum Segment Size (MSS) Adjust	1032
7.21.9	Statistics Collection	1032

7.21.10	Logging.....	1033
7.21.11	Licensing	1034
7.21.12	Configuration	1034
7.21.12.1	Modifying MAP-T Parameters When the MAP-T Domain is Active	1035
7.21.13	Inter-Chassis Redundancy	1036
7.22	Configuring NAT	1037
7.22.1	ISA Redundancy.....	1037
7.22.2	NAT Layer 2-Aware Configurations.....	1039
7.22.3	Large Scale NAT Configuration.....	1041
7.22.4	NAT Configuration Examples	1043
7.23	Configuring VSR-NAT	1047
7.23.1	VSR-NAT Licensing.....	1047
7.23.2	Statistics Collection For LSN Bindings	1048
7.23.3	Statistics Collection For LSN Bandwidth	1049
7.23.4	Statistics Collection and HA	1049
7.23.5	VSR-NAT Show Command Examples	1050
7.24	VSR Scaling Profiles on BB-ISA.....	1052
7.24.1	Scaling Profiles on the VSR	1052
7.24.2	Scale Profile Modification.....	1052
7.25	Network Address Translation Command Reference	1053
7.25.1	Command Hierarchies.....	1053
7.25.1.1	ISA Configuration Commands	1053
7.25.1.2	NAT Service Configuration Commands.....	1054
7.25.1.3	NAT Subscriber Management Commands.....	1062
7.25.1.4	NAT Router Configuration Commands.....	1063
7.25.1.5	NAT DNAT Commands	1065
7.25.1.6	NAT Admin Configuration Commands	1066
7.25.1.7	NAT MAP Domain Configuration Commands	1066
7.25.1.8	TCP MSS Adjustment Commands	1066
7.25.1.9	NAT MAP-T Configuration Commands	1067
7.25.1.10	Residential Firewall Subscriber Management Commands.....	1067
7.25.1.11	Residential Firewall Domain Commands.....	1067
7.25.1.12	Residential Firewall Commands.....	1068
7.25.1.13	Tools Commands	1069
7.25.1.14	Show Commands	1069
7.25.1.15	Clear Commands.....	1071
7.25.1.16	Tools Commands	1071
7.25.1.17	Filter Commands	1072
7.25.2	Command Descriptions	1073
7.25.2.1	Generic Commands.....	1073
7.25.2.2	ISA Configuration Commands	1075
7.25.2.3	NAT Configuration Commands.....	1080
7.25.2.4	NAT Service Configuration Commands.....	1112
7.25.2.5	NAT Outside Epipe Commands	1133
7.25.2.6	IPFlow Information Export Protocol Commands.....	1134
7.25.2.7	AAA Policy Commands	1137
7.25.2.8	NAT Syslog Commands	1154
7.25.2.9	NAT Subscriber Management Commands.....	1160
7.25.2.10	NAT Subscriber Management BRG Commands	1163

7.25.2.11	NAT DNAT Commands	1168
7.25.2.12	NAT MAP-T Commands	1177
7.25.2.13	NAT Filter Commands	1182
7.25.2.14	Residential Firewall Commands	1183
7.25.2.15	NAT Show Commands	1185
7.25.2.16	MAP-T Show Commands	1210
7.25.2.17	NAT Clear Commands	1217
7.25.2.18	MAP-T Clear Commands	1218
7.25.2.19	NAT Tools Commands	1219
8	Residential Firewall	1225
8.1	Residential Firewall Overview	1225
8.1.1	Supported Protocols and Extension Headers	1225
8.1.1.1	Unknown Protocols	1226
8.1.1.2	TCP and UDP	1226
8.1.1.3	ICMPv6	1226
8.1.2	Application Layer Gateway	1227
8.1.3	Additional Filtering Control	1227
8.1.4	TCP MSS Adjustment	1227
8.1.5	Static Port Forwards and DMZ	1228
8.2	Residential Firewall Provisioning	1229
8.2.1	Domains and Addressing	1229
9	TCP MSS Adjustment	1231
9.1	Overview	1231
9.2	TCP MSS Adjustment for ESM Hosts	1232
9.3	TCP MSS Adjustment for NAT Services	1233
9.4	TCC MSS Adjustment Commands	1234
9.4.1	Command Hierarchy	1234
9.4.1.1	TCC MSS Adjustment Command Descriptions	1234
10	L2TP Network Server	1237
10.1	Subscriber agg-rate-limit on LNS	1237
10.2	LNS Reassembly	1240
10.2.1	Overview	1240
10.2.2	Reassembly Function	1240
10.2.3	Load Sharing Between the ISAs	1242
10.2.4	Inter-chassis ISA Redundancy	1242
10.3	MLPPPoE, MLPPP(oE)oA with LFI on LNS	1243
10.3.1	Terminology	1243
10.3.2	LNS MLPPPoX	1243
10.3.3	MLPPP Encapsulation	1244
10.3.4	MLPPPoX Negotiation	1244
10.3.5	Enabling MLPPPoX	1245
10.3.6	Link Fragmentation and Interleaving (LFI)	1246
10.3.6.1	MLPPPoX Fragmentation, MRRU and MRU Considerations	1247
10.3.7	LFI Functionality Implemented in LNS	1248
10.3.7.1	Last Mile QoS Awareness in the LNS	1250
10.3.7.2	BB-ISA Processing	1251

10.3.7.3	LNS-LAC Link.....	1252
10.3.7.4	AN-RG Link	1253
10.3.7.5	Home Link	1253
10.3.7.6	Optimum Fragment Size Calculation by LNS	1253
10.3.8	Upstream Traffic Considerations	1256
10.3.9	Multiple Links MLPPPoX With No Interleaving	1256
10.3.10	MLPPPoX Session Support.....	1256
10.3.11	Session Load Balancing Across Multiple BB-ISAs	1257
10.3.12	BB-ISA Hashing Considerations.....	1258
10.3.13	Last Mile Rate and Encapsulation Parameters	1259
10.3.14	Link Failure Detection.....	1262
10.3.15	CoA Support.....	1262
10.3.16	Accounting	1263
10.3.17	Filters and Mirroring.....	1263
10.3.18	PTA Considerations.....	1263
10.3.19	QoS Considerations	1264
10.3.19.1	Dual-Pass	1264
10.3.19.2	Traffic Prioritization in LFI.....	1264
10.3.19.3	Shaping Based on the Last Mile Wire Rates	1266
10.3.19.4	Downstream Bandwidth Management on Egress Port	1267
10.3.20	Sub/Sla-Profile Considerations	1267
10.3.21	Example of MLPPPoX Session Setup Flow	1268
10.3.22	Other Considerations.....	1269
10.4	Configuration Notes.....	1270
10.5	L2TP Network Server Command Reference	1273
10.5.1	Command Hierarchies.....	1273
10.5.1.1	ISA Commands	1273
10.5.1.2	MLPPP on LNS Commands.....	1273
10.5.2	Command Descriptions	1275
10.5.2.1	Generic Commands.....	1275
10.5.2.2	LNS Commands	1276
10.5.2.3	Network Address Translation (NAT) Commands	1278
10.5.2.4	MLPPP on LNS Commands.....	1280
11	Standards and Protocol Support	1289

1 Getting Started

1.1 About This Guide

This guide describes details pertaining to Integrated Services Adapters (ISAs) and the services they provide.

This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

The topics and commands described in this document apply to the:

- 7450 ESS
- 7750 SR
- VSR

[Table 1](#) lists the available chassis types for each SR OS router.

Table 1 Supported SR OS Router Chassis Types

7450 ESS	7750 SR
• 7450 ESS-7/12 running in standard mode (not mixed-mode)	• 7450 ESS-7/12 running in mixed-mode (not standard mode) • 7750 SR-a4/a8 • 7750 SR-c4/c12 • 7750 SR-1e/2e/3e • 7750 SR-7/12 • 7750 SR-12e • 7750 SR-7s/14-s • 7750 SR-1

For a list of unsupported features by platform and chassis, refer to the *SR OS 16.0.Rx Software Release Notes*, part number 3HE 14220 000x TQZZA or the *VSR Release Notes*, part number 3HE 14204 000x TQZZA.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.



Note: This guide generically covers Release 16.0.Rx content and may contain some content that will be released in later maintenance loads. Refer to the *SR OS 16.0.Rx* Software Release Notes, part number 3HE 14220 000x TQZZA or the *VSR Release Notes*, part number 3HE 14204 000x TQZZA, for information about features supported in each load of the Release 16.0.Rx software.

1.2 ISA Configuration Process

[Table 2](#) lists the tasks necessary to configure ISAs and the services they provide.

This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 2 Configuration Process

Area	Task	Section
Application Assurance	Configure Application Assurance entities	Configuring Application Assurance with CLI
IP tunnels	Determine IPsec deployment requirements	IPsec Deployment Requirements
	Configure IPsec	Configuring IPsec with CLI
L2TPV3 tunnels	Configure the L2TPV3 control plane	Control Plane
	Configure public SAP	Public SAP
	Configure private SAP	Private SAP
Video services	Configure video services components	Configuring Video Service Components with CLI
	Configure REF/FCC video components	Configuring RET/FCC Video Components with CLI
	Configure ADI components	Configuring ADI Components with CLI
Network Address Translation	Configure destination based NAT	Destination Based NAT (DNAT)
	Configure universal plug and play Internet gateway device service	Configuring UPnP IGD Service
	Configure enhanced statistics in NAT	Enhanced Statistics in NAT — Histogram
	Configure mapping of address and port using translation (MAP-T)	Mapping of Address and Port Using Translation (MAP-T)
	Provision residential firewall	Residential Firewall Provisioning
	Configure NAT with CLI	Configuring NAT
	Configure VSR-NAT	Configuring VSR-NAT
TCP MSS adjustment	Configure TCP MSS adjustments	TCP MSS Adjustment

2 ISA Hardware

2.1 In This Section

This section provides an overview of Nokia's implementation of the ISA hardware.



Note: Cards must be configured using the commands described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*.

2.2 MS-ISA2 Overview

The MS-ISA2 (or ISA2-MS in CLI) is a second generation Integrated Services Adapter for Multi-Service processing, as a resource module within the router system providing packet buffering and packet processing.

The MS-ISA2 fits in an MDA/ISA slot on an IOM4-e and has no external ports, so all communication passes through the Input/Output Module (IOM), making use of the network processor complex on the host IOM for queuing and filtering functions like other MDAs and ISAs.

The actual ingress and egress throughput will vary depending on the buffering and processing demands of a given application, but the MS-ISA2 hardware can support 40 Gb/s of throughput processing. The processed rate (up to 40 Gb/s) is the sum of the upstream and downstream rates (for example, 10 Gbps up and 30 Gbps down, or 20 Gbps up and 20 Gbps down).

2.3 MS-ISA Overview

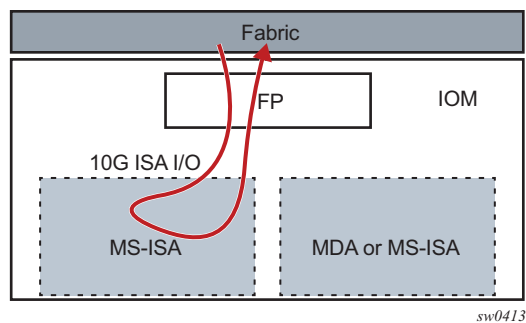
The MS-ISA (or ISA-MS in CLI) is an Integrated Services Adapter for Multi-Service processing, as a resource module within the router system providing packet buffering and packet processing.

The MS-ISA fits in an MDA/ISA slot on an IOM and has no external ports, so all communication passes through the IOM, making use of the network processor complex on the host IOM for queuing and filtering functions like other MDAs and ISAs.

The actual ingress and egress throughput will vary depending on the buffering and processing demands of a given application, but the ISA-MS hardware can support slightly more than 10 Gb/s of throughput ingress and egress.

With the introduction of the MS-ISM and ISA2 processing, ISA-MS may also be referred to as ISA1, as the first generation ISA hardware.

Figure 1 MS-ISA on Host IOM

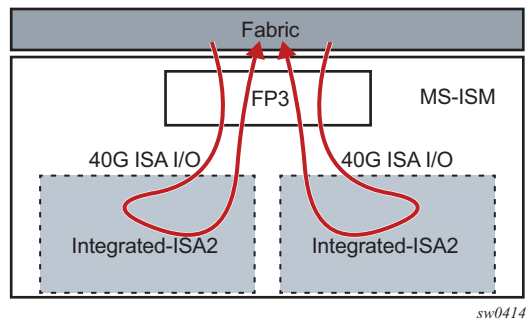


2.4 MS-ISM Overview

The Multi-Service Integrated Services Module (MS-ISM) card contains two ISA2 processing modules providing increased packet processing throughput and scale compared to the MS-ISA platform. Each ISA2 processing module supports a 40G datapath for packet processing; as with ISA1 the actual throughput varies by function. The processed rate (up to 40 Gb/s) is the sum of the upstream and downstream rates (for example, 10 Gbps up and 30 Gbps down, or 20 Gbps up and 20 Gbps down).

The IOM base card is an imm-2pac-fp3 with two embedded positions for ISA2s. Hot swap or field replacement of the ISA2s within an MS-ISM assembly is not supported. IMM cards offering 10x10GE media plus one ISA2, or 1x100GE media plus one ISA2.

Figure 2 MS-ISM with ISA2s



The MS-ISA2 remains as a common base hardware assembly to be used as a generic CPU processing platform for multiple applications. The functions supported on the MS-ISA2 and MS-ISM include the following software based capabilities:

- Application Assurance (AA)
- Tunnel (IPSec, GRE)
- Broadband (NAT, LNS)
- Video (FCC, RET)

2.5 Application Assurance Hardware Features

2.5.1 AA System Support

The Application Assurance Integrated Services Adapter (AA ISA) is a resource adapter, which means that there are no external interface ports on the AA ISA itself. Instead, any other Input Output Modules on a system in which the AA ISA is installed are used to switch traffic internally MS ISA to the AA ISA. [Table 3](#) describes Application Assurance ISA support on the 7750 SR and 7450 ESS.

Table 3 Application Assurance System Support

System	AA on MS-ISA	AA on MS-ISM	AA on MS-ISA2
7750 SR-12	Yes	Yes	Yes
7750 SR-12e	Yes	Yes	Yes
7750 SR-7	Yes	Yes	Yes
7750 SR-c12	Yes	No	No
7750 SR-c4	Yes	No	No
7750 SRe-1	No	No	Yes
7750 SRe-2	No	No	Yes
7750 SRe-3	No	No	Yes
7710 SR	No	No	No
7450 ESS-12	Yes	Yes	Yes
7450 ESS-7	Yes	Yes	Yes

2.5.2 Host IOM Support for AA on ISAs

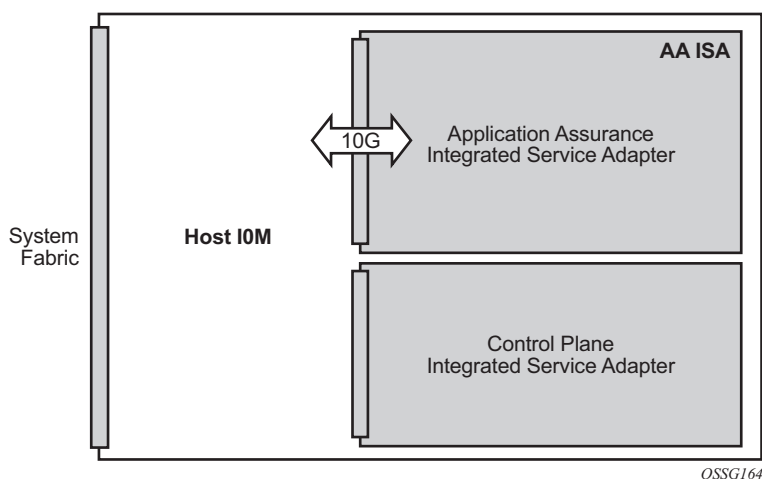
The AA MS-ISA is supported on IOM3-XP, CFM-XP (c12), and IOMc4-xp. The MS-ISM versions contain one or two ISA2s embedded on a IMM card. The MS-ISA2 is supported on the IOM4-e.

Each IOM can support a maximum of two AA ISA modules. To maximize AA ISA redundancy, deployment of AA ISAs on separate host IOMs is recommended as it provides IOM resilience. Traffic from any supported IOM (for example, IOM3-XP, a fixed port IOM (IMM)) can be diverted to an AA ISA host IOM.

The MS-ISA is field replaceable and supports hot insertion and removal. See [Figure 1](#). A system can support up to seven active AA MS-ISA cards providing up to 70 G of processing capacity (a system with seven active ISA2s on MS-ISMs provides up to 280G processing).

AA ISA software upgrades are part of the ISSU functionality. Upgrades to AA ISA software, for example to activate new protocol signatures, do not impact the second MDA slot for the IOM carrying the AA ISA, nor do upgrades impact the router itself (for example, a new AA ISA software image can be downloaded without a need to upgrade other software images).

Figure 3 AA ISA on Host IOM 2-20G Example



3 Application Assurance

3.1 Application Assurance (AA) Overview

Network operators are transforming broadband network infrastructures to accommodate unified architecture for IPTV, fixed and mobile voice services, business services, and High Speed Internet (HSI), all with a consistent, integrated awareness and policy capability for the applications using these services.

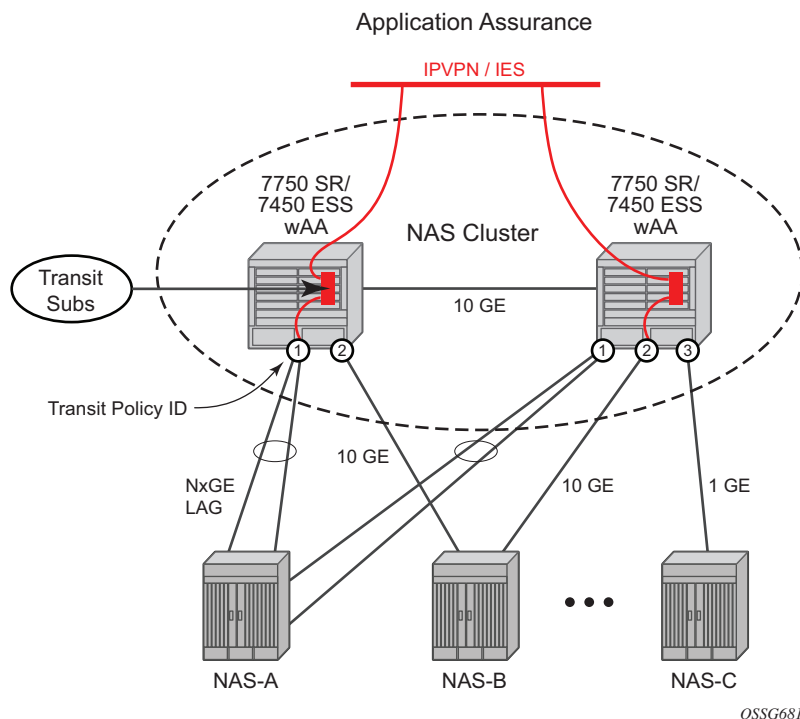
As bandwidth demand grows and application usage shifts, the network must provide consistent application performance that satisfies the end customer requirements for deterministic, managed quality of experience (QoE), according to the business objectives for each service and application. Application Assurance (AA) is the enabling network technology for this evolution in the service router operating system.

Application Assurance, coupled with subscriber and/or VPN access policy control points enables any broadband network to provide application-based services. For service providers, this unlocks:

- the opportunity for new revenue sources
- content control varieties of service
- control over network costs incurred by various uses of HSI
- complementary security aspects to the existing network security
- improved quality of service (QoS) sophistication and granularity of the network
- the ability to understand and apply policy control on the transactions traversing the network

3.1.1 Application Assurance: Inline Policy Enforcement

Figure 4 AA ISA Inline Identification, Classification and Control



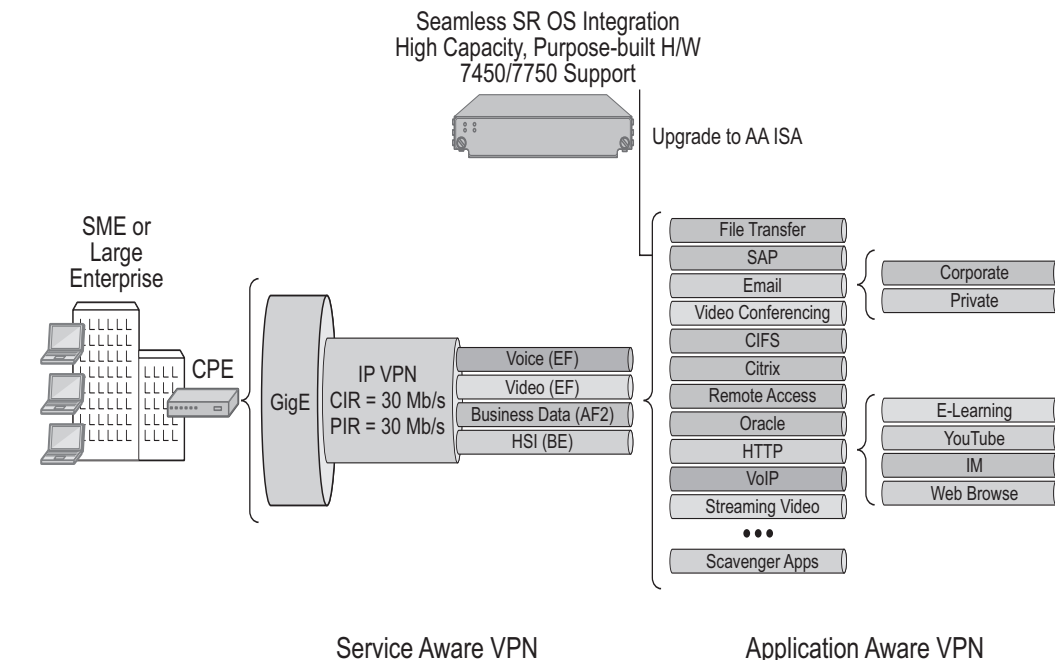
The integrated solution approach for Application Assurance recognizes that a per-AA subscriber and per-service capable QoS infrastructure is a pre-condition for delivering application-aware QoS capabilities. Enabling per-application QoS in the context of individual subscriber's VPN access points maximizes the ability to monetize the application service, because a direct correlation can be made between customers paying for the service and the performance improvements obtained from it. By using an integrated solution there is no additional cost related to router port consumption, interconnect overhead or resilience to implement in-line application-aware policy enforcement.

3.1.2 AA Integration in Subscriber Edge Gateways

Multiple deployment models are supported for integrating application assurance in the various subscriber edge and VPN PE network topologies. In all cases, application assurance can be added by in-service upgrade to the installed base of equipment rather than needing to deploy and integrate a whole new set of equipment and vendors into the network for Layer 4-7 awareness.

Integrating Layer 4-7 application policy with the 7750 SR or 7450 ESS subscriber edge policy context is the primary solution to address both residential broadband edge or Layer 2/Layer 3 application aware business VPN. Placement of Layer 4-7 analysis at the distributed subscriber edge policy point simplifies AA deployments in the following ways:

- For residential markets, CO-based deployment allows deployment-driven scaling of resources to the amount of bandwidth needed and the amount of subscribers requiring application-aware functionality.
- For AA business VPNs, a network deployment allows large scale application functionality at a VPN provider edge access point, vastly reducing complexity, cost, and time-to-market required to offer application-aware VPN services.
- Traffic asymmetry is avoided. Any subscriber traffic usually passes through one CO subscriber edge element so there is no need for flow paths to be recombined for stateful analysis.
- PE integration provides a single point of policy enforcement.
- SeGW integration provides firewall protection for NMS, MME and SGW.

Figure 5 AA Deployment Topologies

OSSG237

There are residential topologies where it is not possible or practical to distribute ISAs into the same network elements that run ESM, including for legacy edge BRASs that still need Application Assurance policy (reporting and control) for the same Internet services, and which needs to be aligned and consistent with the ESM AA policy. This is supported using transit AA subscribers, typically in the first routed element behind the legacy edge.

Application Assurance enables per AA subscriber (a residential subscriber, or a Layer 2/Layer 3 SAP or spoke SDP), per application policy for all or a subset of AA subscriber's applications. This provides the ability to:

- implement Layer 4-7 identification of applications using a multitude of techniques from a simple port-based/IP address based identification to behavioral techniques used to identify, for example, encrypted or evasive applications
- once identified, to apply QoS policy on either an aggregate or a per-AA subscriber, per-application basis
- provide reports on the identification made, the traffic volume and performance of the applications, and policies implemented

An integrated AA module allows the SR and ESS product families to provide application-aware functions that previously required standalone devices (either in residential or business environment) at a fraction of the cost and operational complexity that additional devices in a network required.

A key benefit of integrating AA in the existing IP/MPLS network infrastructure (as opposed to an in-line appliance) is the ability to select traffic for treatment on a granular, reliable basis. Only traffic that requires AA treatment is simply and transparently diverted to the ISA. Other traffic from within the same service or interface will follow the normal forwarding path across the fabric. In the case of ISA failure, ISA redundancy is supported and in the case where no backup ISAs are available, the AA traffic reverts to the normal fabric matrix forwarding, also known as “fail to fabric”.

Table 4 Traffic Diversion to the ISA

Deployment Case	System Divert ID	AA Subscriber Type	App-Profile on:
Residential Edge (BNG)	ESM Sub-ID	ESM	ESM sub (All IPs, not per-host)
vRGW Bridged Residential Gateway (BRG) subscriber	ESM Sub-ID	ESM	ESM sub (All IPs, not per-host)
vRGW BRG session	ESM-MAC	ESM-MAC	ESM-MAC (by device, for any hosts assigned to a device)
Wireless LAN GW	ESM or DSM	ESM or DSM	ESM or DSM
Business Edge	L2/L3 SAP	SAP	SAP (Aggregate)
Residential Transit	Parent L3 SAP or spoke SDP	Transit AA	Transit Sub
Spoke Attached Edge	Spoke SDP	Spoke SDP	Spoke SDP (Aggregate)
SeGW	Parent SAP or spoke SDP or L2/L3 SAP	Transit AA SAP	Transit AA SAP

3.1.3 Fixed Residential Broadband Services

Fixed residential HSI services as a single edge Broadband Network Gateway (BNG), virtualized Residential Gateway (vRGW), or as part of the Triple Play Service Delivery Architecture (TPSDA) are a primary focus of Application Assurance performance, subscriber and traffic scale.

To the service provider, application-based service management offers:

- application aware usage metering packages (quotas, 0-rating and so on)
- new revenue opportunities to increase ARPU (average revenue per user) (for gaming, peer-to-peer, Internet VoIP and streaming video, and so on)
- fairness: Aligns usage of HSI network resources with revenue on a per-subscriber basis
- operational visibility into the application usage, trends, and pressure points in the network

To the C/ASP, service offerings can be differentiated by improving the customer's on-line access experience. The subscriber can benefit from this by gaining a better application experience, while paying only for the value (applications) that they need and want.

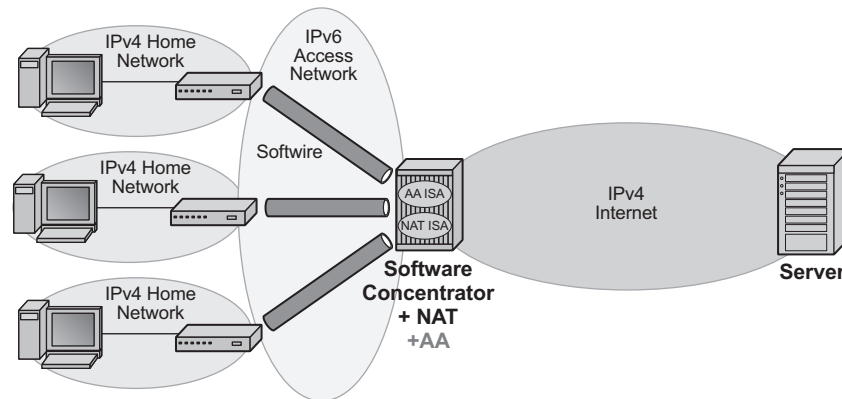
3.1.3.1 Dual-Stack Lite – DS-Lite

Dual Stack Lite is an IPv6 transition technique that allows tunneling of IPv4 traffic across an IPv6-only network. Dual-stack IPv6 transition strategies allow service providers to offer IPv4 and IPv6 services and save on OPEX by allowing the use of a single IPv6 access network instead of running concurrent IPv6 and IPv4 access networks. Dual-Stack Lite has two components: the client in the customer network (the Basic Bridging BroadBand element (B4)) and an Address Family Transition Router (AFTR) deployed in the service provider network.

Dual-Stack Lite leverages a network address and port translation (NAPT) function in the service provider AFTR element to translate traffic tunneled from the private addresses in the home network into public addresses maintained by the service provider. On the 7750 SR, this is facilitated through the Carrier Grade NAT function.

When a customer's device sends an IPv4 packet to an external destination, DS-Lite encapsulates the IPv4 packet in an IPv6 packet for transport into the provider network. These IPv4-in-IPv6 tunnels are called softwires. Tunneling IPv4 over IPv6 is simpler than translation and eliminates performance and redundancy concerns.

Figure 6 DS-Lite Deployment



The IPv6 source address of the tunnel represents a unique subscriber. Only one tunnel per customer (although more is possible), but the IPv6 addresses cannot overlap between different customers. When encapsulated traffic reaches the softwire concentrator, the device treats the source-IP of the tunnel to represent a unique subscriber. The softwire concentrator performs IPv4 network address and port translation on the embedded packet by re-using Large Scale NAT and L2-Aware NAT concepts.

Advanced services are offered through Application Assurance multi service ISA to the DS-Lite connected customers. Subscribers' traffic (ESMs or transit-ip) are diverted to AA ISA for Layer 3 to Layer 7 identification and classifications, reporting and control based on the IPv4 packets (transported within the IPv6 DS-Lite tunnel). This AA classification, reporting and control of subscribers' traffic take effect before any NAT44 functions. In specific, AA sites on the subscriber side of NAT44.

The absence of a control protocol for the IP-in-IP tunnels simplifies the operational/management model, since any received IPv6 packet to the AA ISA can be identified as a DS-Lite tunneled packet if:

- protocol 4 in the IPv6 header, and
- the embedded IP packet is IPv4 (inside)

Fragmented IPv4 packets are supported only if tunneled through non-fragmented IPv6 packets.

Fragmentation at the IPv6 layer is not supported by AA ISA (when used to tunnel fragmented or non-fragmented IPv4 packets). These packets are cut-through with sub-default policy applied with a possibility of re-ordering.

If DSCP AQP action is applied to DS-Lite packet, both IPv4 and IPv6 headers are modified. AQP mirroring action is applied at the IPv6 layer. All collected statistics include the tunnel over-head bytes (also known as IPv6 header size).

3.1.3.2 6to4 /6RD

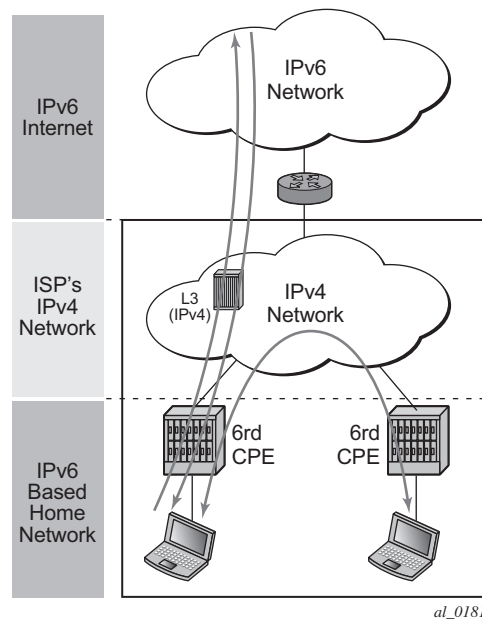
6RD/6to4 tunneling mechanism allows IPv6 sites to communicate over an IPv4 network without the need to configure explicit tunnels, as well as and for them to communicate with native IPv6 domains via relay routers. Effectively, 6RD/6to4 treats the wide area IPv4 network as a unicast point-to-point link layer. Both ends of the 6RD/6to4 tunnel are dual-stack routers. Because 6RD/6to4 does not build explicit tunnels, it scales better and is easier to manage after setup

6to4 encapsulates an IPv6 packet in the payload portion of an IPv4 packet with protocol type 41. The IPv4 destination address for the encapsulating IPv4 packet header is derived from the IPv6 destination address of the inner packet (which is in the format of 6to4 address) by extracting the 32 bits immediately following the IPv6 destination address's 2002:: prefix. The IPv4 source address in the encapsulating packet header is the IPv4 address of the outgoing interface (not system IP address).

6RD is very similar to 6to4; the only difference is that the fixed 2002 used in 6to4 prefix is replaced by a configurable prefix.

An important deployment of 6RD/6to4 deployment is in access network as shown in [Figure 7](#).

Figure 7 6to4 in Access Network Deployment



To provide IPv6 services to subscribers, 6RD is deployed in these access networks to overcome the limitations of IPv4 only access network gear (for example, DSLAMs) with no dual stack support.

From an AA ISA point of view, deployment of 6RD in the access network is similar to that of the general deployment case between IPv6 islands with the added simplification that each 6RD tunnel carries traffic of a single subscriber.

When AA ISA sees an IPv4 packet with protocol type 41 and a payload that includes an IPv6 header, it detects that this is a 6rd/6to4 tunneled packet.

AA ISA detects, classifies, reports, and applies policies to 6rd/6to4 packet for ESM, SAP, spoke-SDP, and transit-IP (ip-policy) AA subscriber types.

Fragmented IPv6 are supported only if tunneled through non-fragmented IPv4 packets.

Fragmentation at the IPv4 layer is not supported by AA ISA (when used to tunnel fragmented or non-fragmented IPv6 packets). These packets are cut-through with sub-default policy applied with a possibility of re-ordering.

If the packet has IPv4 options then AA ISA will not look into the IPv6 header. The packet will be classified as IPv4 “unknown TCP/UDP”. Furthermore, TCP/UDP checksum error detection is only applied for IPIPE and routed services.

If the DSCP AQP action is applied to 6RD6to4 packets, both IPv4 and IPv6 headers are modified. AQP mirroring action is applied at the IPv4 layer. All collected statistics include the tunnel over-head bytes, aka. IPv4 header size.

3.1.4 Wireless LAN Gateway Broadband Services

Application Assurance enables a variety of use cases important for Wireless LAN Gateway deployments in residential, public WiFi or VPN wireless LAN services. These include:

- HTTP redirect for subscriber authentication with HTTP whitelist — Redirects all non-authenticated subscriber HTTP traffic to an authentication portal and blocks the rest of Internet access, but allows user access to specific whitelisted websites, download Apps and software needed to authenticate.
- HTTP redirect by policy — URL or application blocking or usage threshold notification. Redirects some or all subscriber HTTP traffic to an portal landing site based on static or dynamic policy. This can be done while not interrupting selected HTTP based services such as streaming video.
- Inline HTTP browser notification — Provides messaging in the form of web banners, overlays, or http-redirection. This can always be enabled, One-time per sub at authentication (greeting message “Welcome to our WiFi Service”), one time per COA, or periodically.
- ICAP for large scale URL filtering — ICAP client in AA interacts with offline ICAP URL filtering services, for parental control or large blacklists. Reduces cost as only URLs for specific flows are sent to server, rather than full inline traffic.
- Analytics — Provides operator insight into the following: Application and App-group volume usage by time of day/day of week, top subs, devices, and so on.
- Traffic control for fair use policy — Prevents some users of the hotspot from consuming a disproportionate amount of resources by limiting to volume of such use across all subscribers as a traffic management tool, or on a per-subscriber basis.
- Stateful Firewall — Prevents unsolicited sessions from attacking devices.

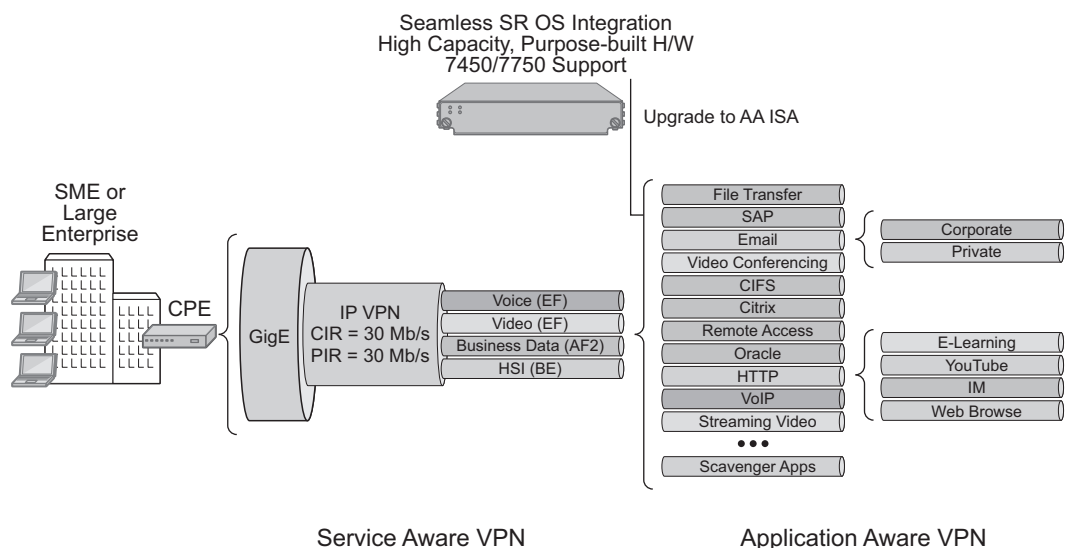
3.1.5 Application-Aware Business VPN Services

AA for business services can be deployed at the Layer 2 or Layer 3 network provider edge (PE) policy enforcement point for the service or at Layer 2 aggregation policy enforcement point complimentary to the existing Layer 3 IP VPN PE. In a business environment, an AA subscriber represents a VPN access point. A typical business service can have a much larger average bandwidth rate than the residential service and is likely to have a smaller AA subscriber count than a residential deployment.

Up to seven active ISAs can be deployed per PE, each incrementally processing up to 10Gb/s. The in-network scalability is a key capability that allows a carrier to be able to grow the service bandwidth without AA throughput affecting the network architecture (more edge nodes, application-aware devices).

Application-aware Layer 2 and Layer 3 VPNs implemented using AA ISA equipped 7750 SR and 7450 ESS together with rich network management (NSP NFM-P, 5750 RAM, end customer application service portals) give operators a highly scalable, flexible, and cost effective integrated solution for application-based services to end customers. These services may include:

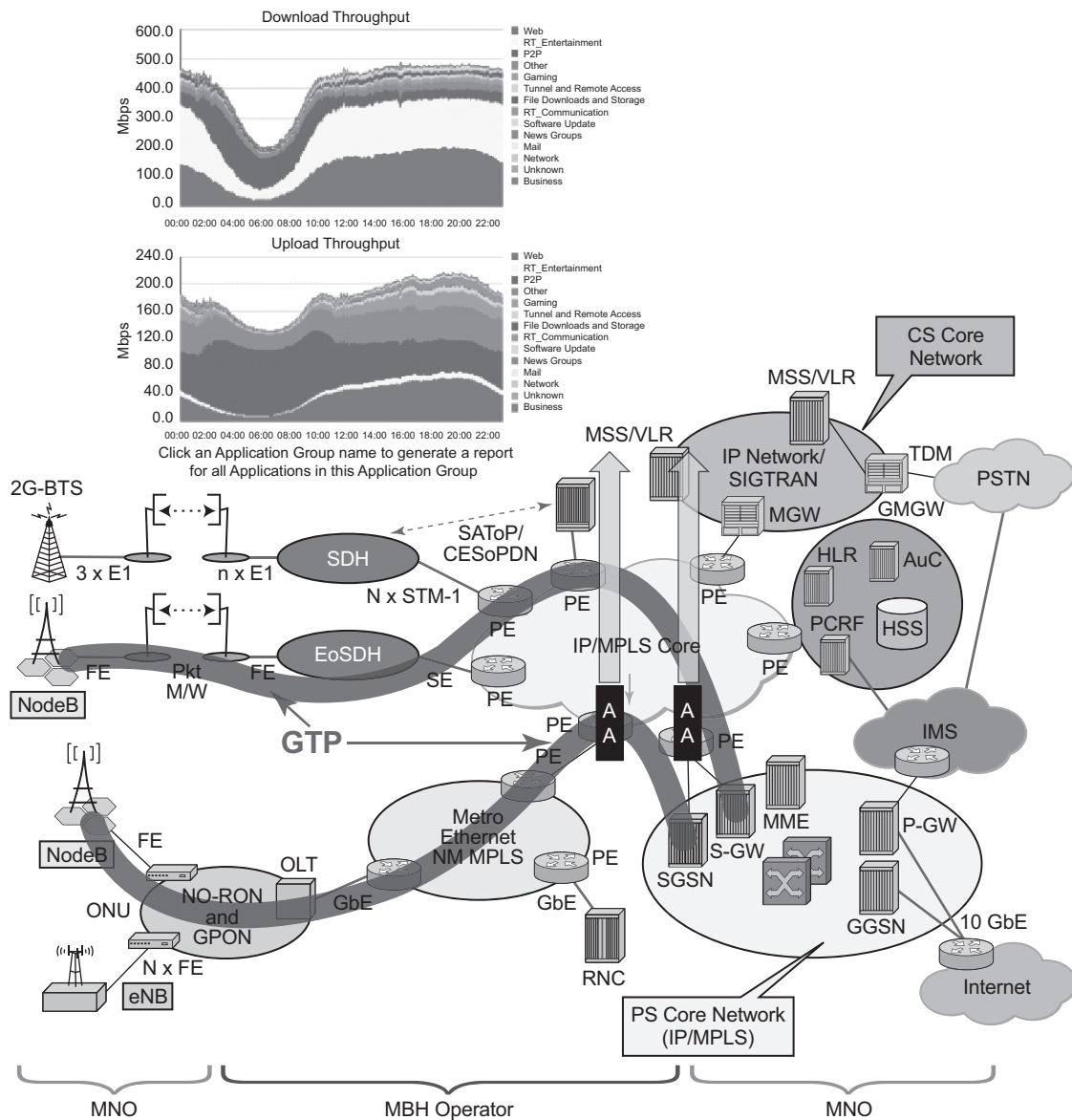
- Rich application reporting with VPN, access site visibility
- Right-sizing access pipes into a VPN service to improve/ensure application performance
- Application-level QoS (policing, session admission, remarking, and so on) to ensure application-level performance, end-customer QoE objectives are met.
- Value-added services such as application verification, new application detection, application mirroring
- Performance reporting for real time (RTP) and non-real time (TCP) based applications
- Dual Stack IPv4 – IPv6 support
- GTP, 6RD tunneling support
- Control unauthorized or recreational applications by site, by time of day.

Figure 8 AA BVS Services Integrated into the Provider Edge

OSSG237

3.1.6 Business Mobile Backhaul

Figure 9 GTP-MBH AA Deployment



1000

In addition to SeGW FireWall deployments that require AA to support handling of GTP encapsulated traffic (S1-U interface), there are a number of deployments that require AA to support detection such as, classification and control of traffic encapsulated within GTP tunnels. These deployments are very similar in nature to AA support for other tunneling mechanisms such as 6RD, 6to4, DsLite. and so on. For GTP tunnels, two main deployment use cases are identified: WiFi offload and mobile backhaul.

In Mobile Backhaul (MBH) deployment, operators provide business network services called Mobile Data Roaming traffic service (that is, GPRS roaming exchange/service) to Mobile Network operators (MNOs) utilizing MPLS network. MNOs, in turn, utilize MBH networks to create GTP tunnels across the MBH network between their mobile access network (for example, eNBs/SGSN/SGW) and PGSN/PGW network devices.

MNOs look into their MBH network providers to provide more analytical reporting of the applications running over the GTP-U tunnels.

AA-ISA is used to report on diverted business SAPs, regardless of how the traffic is encapsulated (GTP-U and 6RD, for example). From AA-ISA point of view, the diverted business SAP represents the subscriber. The subscriber is the MNO itself. No transit AA subscriber support is required in this deployment.

In this situation, multiple GTP-U tunnels are carried per SAP. AA reports on the actual content of these tunnels and not on the GTP-U tunnel themselves. For example, AA reports on the applications per SAP and not applications per GTP-u tunnel.

While this use case does not require any form of AA control functions, all AA actions/control functions can be used except for actions that require packet modifications (such as HTTP enrichments, HTTP redirect, remarking, DSCP Remark, HTTP notification).

3.1.7 SeGW Firewall Service

Application Assurance deployed within a 7750 SR Security gateway in ultra-broadband access networks (3G/4G/Femto) provides the operator with back-end core network security protection. For detailed information see [SeGW Firewall Protection](#).

3.2 Application Assurance System Architecture

3.2.1 AA ISA Resource Configuration

AA ISAs are flexible embedded, packet processing resource cards that require configuration such that services may be associated with the resources. This includes assigning ISAs to groups, optionally defining group partitions, and setting the redundancy model. Load balancing is affected by how ISAs are grouped.

3.2.1.1 AA ISA Groups

An AA ISA group allows operators to group multiple AA ISAs into one of several logical groups for consistent management of AA resources and policies across multiple AA ISA cards configured for that group. The following operations can be performed at the group level:

- Define one or multiple AA ISA groups to allow AA resource partitioning/reservation for different types of AA service.
- Define the AA subscriber scale mode for the group. Residential, VPN and distributed subscriber management modes are supported.
- Assign physical AA ISAs to a group.
- Select forwarding classes to be diverted for inspection by the AA subscribers belonging to the group and select the AA policy to be applied to the group.
- Configure redundancy and bypass mode features to protect against equipment failure.
- Configure QoS on IOMs which host AA ISAs for traffic toward AA ISAs and from AA ISAs.
- Configure ISA capacity planning using low and high thresholds.
- Enable partitions of a group.
- Configure the ISA traffic overload behavior for the group to either back pressure to the host IOM (resulting in possible network QoS-based discards) or to cut-through packets through the ISA without full AA processing. Cut-through is typically enabled for AA VPN groups but not for residential groups.

Residential services is an example where all AA services might be configured as part of a single group encompassing all AA ISAs, for operator-defined AA service. This provides management of common applications and reporting for all subscribers and services, with common or per customer AQP (using ASOs characteristics to divide AA group's AQP into per app-profile QoS policies).

Multiple groups can be further used to create separate services based on different sets of common applications, different traffic divert needs (such as for capacity planning) or different redundancy models. Cases where multiple groups might be used can include:

- For mix of residential and business customers.
- Among different business VPN verticals.
- For business services with a common template base but for different levels of redundancy, different FC divert, or scaling over what is supported per single group.
- System level status statistics have AA ISA group/partition scope of visibility.

3.2.1.1.1 AA Group Partitions

VPN-specific AA services are enabled using operator defined partitions of an AA Group into AA policy partitions, typically with one partition for each VPN-specific AA service. The partition allows VPN specific custom protocols/application/application group definition, VPN specific policy definition and VPN specific reporting (some VPNs with volume-only reports, while others with volume and performance reports). Each partition's policy can be again divided into multiple application QoS policies using ASOs.

The use of ISA groups and partitions also improves scaling of policies, as needed with VPN-specific AA policies.

If partitions are not defined, all of the AA group acts as a single partition. When partitions are configured, application identification, policy and statistics configuration applies only to the given partition and not any other partitions configured under the same AA group.

The definition of application profiles (and related ASO characteristics/values) are within the context of a given partition (however, application profiles names must have node-wide uniqueness)

The definition of applications, application groups and AQP are also specific to a given partition. This allows:

- The definition of unique applications and app-groups per partition.

- The definition of AQP policy per partition.
- The definition of common applications and app-groups per partition with per partition processing and accounting.

Partitions also enable accounting/reporting customization for every AA subscriber associated with a partition, for example:

- The ability to define different types of reporting/accounting policies for different partitions in a single AA group, such as uniquely define which application, protocols, app groups are being reported on for every AA subscriber that uses a given partition.
- AA group level protocol statistics with partition visibility (for example, protocol counts reported for each partition of the group separately).

The system provides independent editing and committing of each partition config (separate begin/commit/abort commands).

Policer templates allow group-wide policing, and can be referenced by partition policies.

3.2.1.1.2 Bypass Modes

If no active AA ISA is available (for example, due to an operational failure, misconfiguration) the default behavior is to forward traffic as if no AA was configured, the system does not send traffic to the AA ISA (equivalent to fail to closed). Alarms are raised to flag this state externally. There is an optional “fail to open” feature where AA ISA service traffic is dropped if no active AA ISA is present (such as no AA ISA is present and operationally up).

3.2.1.2 Redundancy

AA ISA group redundancy is supported, to protect against card failure and to minimize service interruption during maintenance or protocol signature upgrades.

3.2.1.2.1 No AA ISA Group Redundancy

AA can be configured with no ISA redundancy within the AA group. All AA ISAs are configured as primary with no backup (up to the limit of active AA ISAs per node). There is no fault state indicating that a spare AA ISA is missing. If a primary is configured but not active, there will be a “**no aa-isa**” fault.

3.2.1.2.2 Failure to Fabric

In the event that no ISA redundancy is deployed or insufficient ISAs are available for needed sparing, the system implements “failure to fabric”. When the ISA status shows the ISA is not available and there is no redundant ISA available, the ingress IOMs simply do not divert the packets that would have been sent to that ISA, but instead these proceed to the next hop directly across the fabric. When the ISA becomes available, the divert eligible packets resume divert through the ISA. This behavior is completely internal to the system, without affecting the forwarding or routing configuration and behavior of the node or the network.

3.2.1.2.3 N+1 AA ISA Card Warm Redundancy

The system supports N+1 AA ISA equipment warm redundancy (N primary and 1 backup). If a backup is configured and there is no ISA available (a primary and backup failed), there will be a “**no aa-isa**” fault. The backup AA ISA is pre-configured with isa-aa.tim and the group policies. Data path traffic is only sent to active AA ISAs, so the backup has no flow state. If a backup ISA is unavailable, there will be a “backup missing” fault.

An AA subscriber is created and assigned to a primary AA ISA when an application profile is assigned to a subscriber, SAP, or spoke SDP. By default, AA subscribers are balanced across all configured primary AA ISAs.

Upon failure of a primary AA ISA, all of its AA subscribers and their traffic are operationally moved to the newly active backup AA ISA but the current flow states are lost (warm redundancy). The new AA ISA will identify any session-based active flows at a time of switchover as an **existing** protocol, while the other flows will be re-identified. The **existing** protocol-based application filters can be defined to ensure service hot redundancy for a subset of applications. Once the backup AA ISA has taken control, it will wait for operator control to revert activity to the failed primary AA ISA module.

The user can disable a primary AA ISA for maintenance by triggering a controlled AA ISA activity switch to do the AA ISA software field upgrade (a shutdown of an active AA ISA is recommended to trigger an activity switch).

The activity switch experiences the following AA service impact:

- All flow states for the primary ISA are lost, but existing flows can be handled with special AQP rules for the existing flows by the newly active backup AA ISA until sessions end.
- All statistics gathered on the active AA ISA since the last interval information that was sent to the CPM will be lost.

3.2.1.3 ISA Load Balancing

Capacity-cost based load balancing allows a cost to be assigned to diverted AA subscribers (by the app-profile). Load Balancing uses the total allocated costs on a per-ISA basis to assign the subscriber to the lowest sum cost ISA resource. Each ISA supports a threshold as the summed cost value that notifies the operator if or when capacity planning has been exceeded.

The load balancing decision is made based on the AA capacity cost of an AA subscriber. The capacity cost is configured against the app-profile. When assigning a new diverted AA subscriber to an ISA, the ISA with the lowest summed cost (that also has sufficient resources) is chosen. Examples of different load-balancing approaches that may be implemented using this flexible model include:

- AA subscriber count balancing — Configure the capacity cost for each app-profile to the same number (for example, 1).
- AA subscriber stats resource balancing — Configure the capacity cost to the number of stats collected for AA subscribers using the app-profile. This might be used if different partitions have significantly different stats requirements.
- Bandwidth balancing — Configure the capacity cost to the total bandwidth in both directions (in kb/s) expected for those AA subscribers. This might be used if different AA subscribers have highly varying bandwidth needs.

Load balancing operates across ISAs within an AA group, and will not balance across groups. The system will ensure that app-profiles assigned to AA subscribers (ESM subscribers, SAPs and spoke SDPs) that are within a single VPLS/Epipe/IES/VP RN service are all part of the same AA group (partitions within an AA group are not checked/ relevant).

Users can replace the app-profile assigned to an AA subscriber with another app-profile (from the same group/partition) that has a different capacity cost.

Regardless of the preferred choice of ISA, the system takes into account.

- Resource counts have per-ISA limits. If exceeded on the ISA of choice, that ISA cannot be used and the next best is chosen.
- Divert IOM service queuing resources may limit load-balancing. If queuing resources are exhausted, the system attempts to assign the AA subscriber to the ISA where the first AA subscriber within that service (VPLS/Epipe) or service type (IES/VP RN) was allocated.

For prefix transit AA subscriber deployments using the **remote-site** command, traffic for the remote transit subs are processed a second time. The ISA used by the parent AA subscriber will be used by all transits within the parent. In remote-site cases there may be a need to increase capacity cost of parent since the transits stay on same ISA as the parent.

Prefix transit AA subscribers are all diverted to the same Group and partition as the parent SAP.

3.2.1.4 Asymmetry Removal

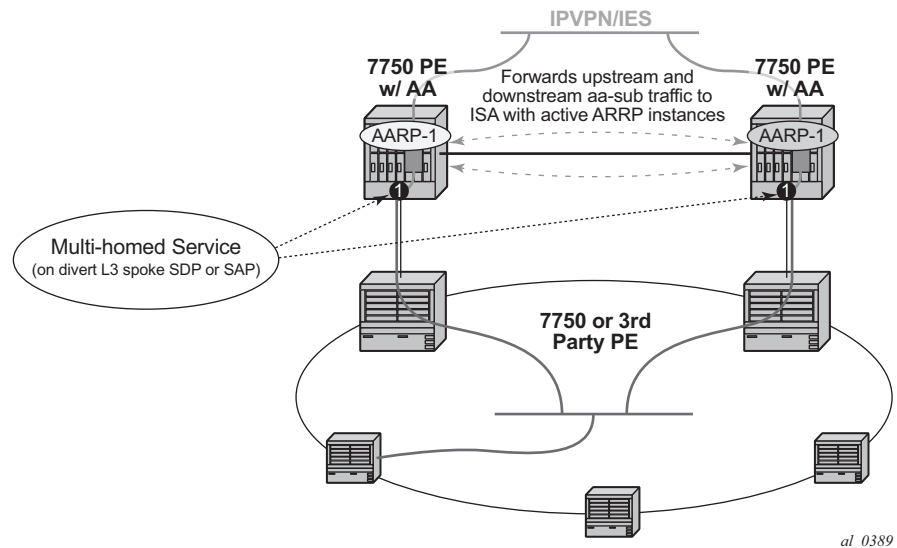
Asymmetry removal is only supported on 7750 SR routed services. Asymmetry removal is a means of eliminating traffic asymmetry between a set of multi-homed SAP or spoke-sdp endpoints. This can be across endpoints within a single node or across a pair of inter-chassis link connected routers. Asymmetry means that the two directions of traffic for a given flow (to-sub and from-sub) take different paths through the network. Asymmetry removal ensures that all packets for each flow, and all flows for each AA subscriber are diverted to a given AA ISA.

Traffic asymmetry is created when there are multi-homed links for a given service, and the links are simultaneously carrying traffic. In this scenario packets for flows will use any reachable paths, thus creating dynamic and changing asymmetry. Single node or multi-chassis asymmetry removal is used for any case where traffic for an AA subscriber may be forwarded over diverse paths on active AA divert links in a multi-homed topology. This includes support for SAP or spoke AA subscribers as well as business and residential transit AA subscribers within the diverted service.

Asymmetry removal must be implemented in the first routed hop on the network side of the subscriber management point, such that there will be a deterministic and fixed SAP / spoke-SDP association between the downstream subscriber management the parent divert service.

Asymmetry removal allows support for the SAP or spoke SDPs to the downstream element to be multi-homed on active links to redundant PE AA nodes as shown in [Figure 10](#).

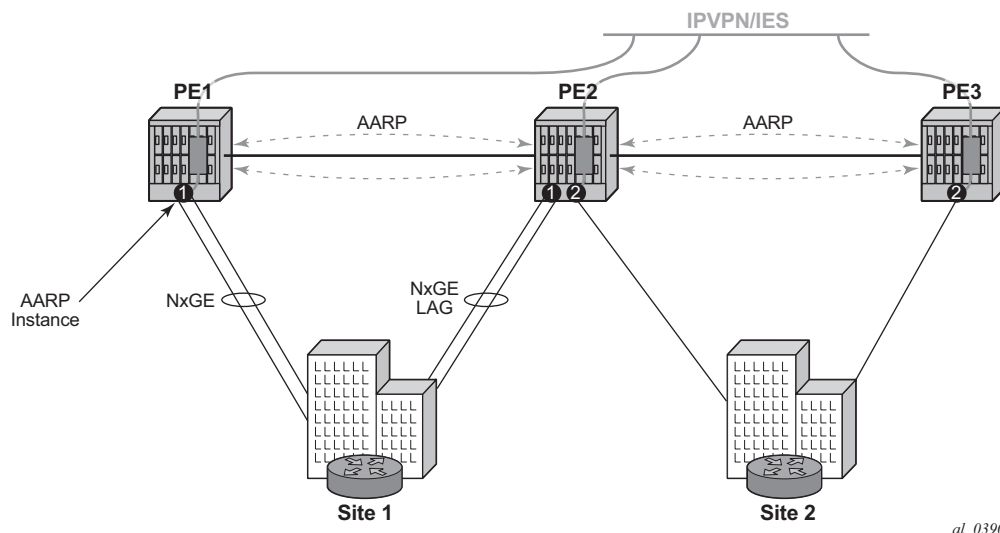
Figure 10 Transit Sub SAP and Spoke SDP Multi-Homing with Asymmetry



AA for transit-ip subscribers is commonly deployed behind the point of the subscriber policy edge after aggregation. This includes cases where AA needed is behind:

- Any node running ESM but where there is not desire, need or space to deploy distributed AA ISAs.
- Legacy BRAS that do not support integrated application policy.

Asymmetry removal also allows a VPN site ([Figure 11](#)) to be connected with multi-homed, dual-active links while offering AA services with the ISA.

Figure 11 VPN Site Multi-Homing with Asymmetry

al_0390

Asymmetry removal is supported for Layer 3 AA divert services:

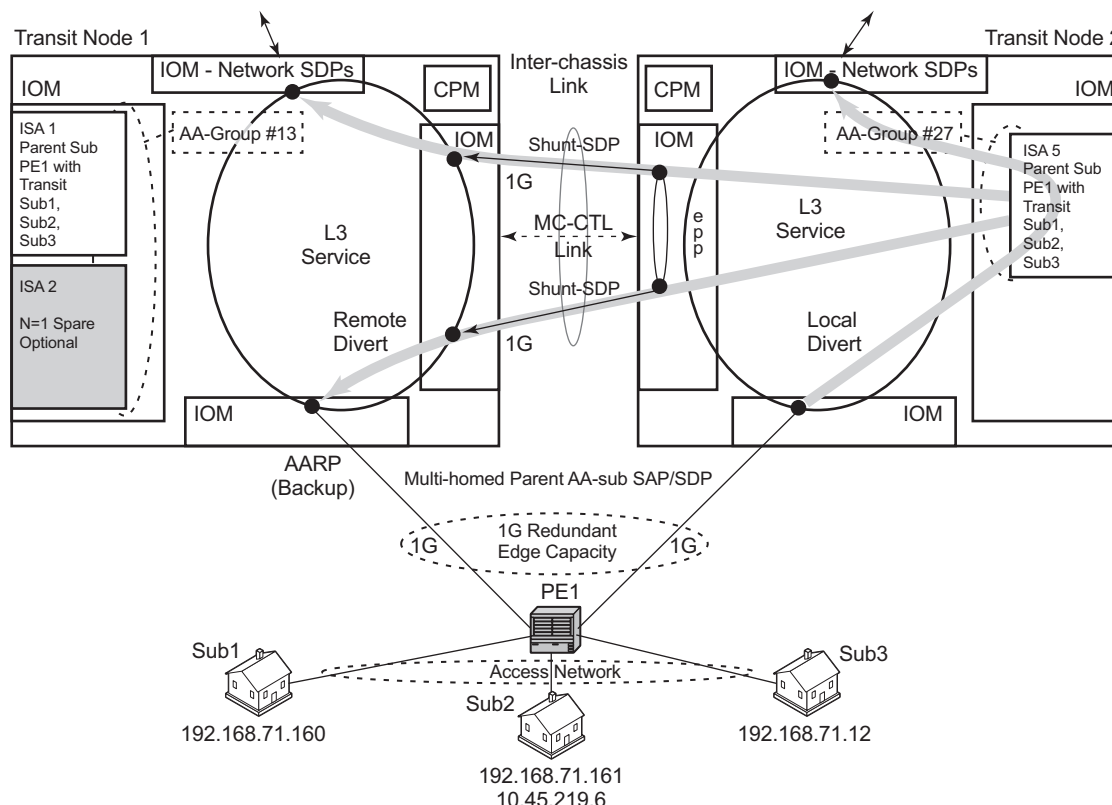
- IES SAP and spoke SDP
- VPRN SAP and spoke SDP

When asymmetry exists between multi-chassis redundant systems, Ipipe spoke SDPs are used to interconnect these services between peer nodes over an Inter-Chassis Link (ICL).

Asymmetry removal supports multiple endpoints of a service with a common AARP instance, with a primary endpoint assigned the app-profile (and transit policy for transit subs). The remaining endpoints are defined as secondary endpoints of the AARP instance. All SAP or spoke endpoints within a given AARP instance are load balanced to the same ISA in that node. Multi-endpoint AARP instances allow single-node asymmetry removal and multi-chassis asymmetry removal with multiple active links per node.

3.2.1.4.1 Asymmetry Removal Overview

Figure 12 Multi-Chassis Asymmetry Removal Functional Overview



al_0391

For a Multi-homed parent AA subscriber, the parent SAP/SDP that is Active/Inactive per chassis is agreed by the inter-chassis AA Redundancy Protocol (AARP). For single node multi-homed endpoints, the AARP state is determined within a single node, as explained later in the AARP operational states section.

- Divert AA subscribers are cost-based load balanced across ISAs in each chassis/AA group (node-local decision).
- Divert AA subscriber multi-homed pairing is supported by AA Redundancy Protocol (AARP) over inter-chassis link.
 - The same AARP ID is assigned to the divert SAP in both nodes.
 - AARP state in one node is master when all AARP conditions are met.
 - Packets arriving on node with the master AARP ID divert locally to ISA.

- From sub packets on a node with backup AARP ID remote diverted over the subscriber side shunt, appearing to the ISA as if it was a local packet from the AA subscriber and returned to the network side interface spoke SDP shunt after ISA processing. To-sub packets on node with backup AARP ID remote divert over the network side shunt, appearing to the ISA as if it was a local network side divert packet for the AA subscriber, then returned to the subscriber side interface spoke-sdp shunt after ISA processing.
- All packets are returned to the original node for system egress (sent back over the inter-chassis shunts).
- If ISA N+1 sparing is available in a node, ISA sparing activates before AARP activity switch.
- Supports asymmetry for business SAPs and spoke SDPs, with or without transit AA subs.
- The AARP master-selection-mode is in minimize-switches mode by default, which is non-revertive and does not factor endpoint status. This can be configured per AARP instance using the master-selection-mode. The priority-rebalance configuration will rebalance based on priority once the master failure condition is repaired. The inter-chassis-efficiency mode does priority based rebalance and includes the EP status for cases where an AARP activity switch is preferred to sustained ICL traffic load (when peer nodes are geographically remote).

3.2.1.4.2 Failure Modes

Failure modes include the following:

- AARP infrastructure failure including shunts: For AARP to remove asymmetry, the AARP link must be synchronized between peers and all components of the shunts (lpipe shunts and interface shunts) must be up and operational. If any of those components has failed, each AARP Id operates as standalone and diverts locally. Asymmetry is not removed.
- Failure of one of the interfaces to the dual homed site: routing will move all traffic to the remaining link/node, if this is the master AARP peer node no action is required. For any traffic the backup node, inter-chassis shunting will be used. There is no change to the AARP master/backup state. Traffic will still be processed by the same ISA as before the failure.
- Network reachability fails to master AARP node: AARP node loses reachability on the network side. This does not trigger an AARP activity switch, the shunt is used to move traffic from the backup node to the master node for the duration of the reachability issue. Routing should take care of traffic reconvergence. However, if the peer AARP is also not reachable, both nodes go on standalone mode and there is no asymmetry removal.

- Master AA ISA failure: AARP activity will flip for all the master AARP instances linked to this local ISA if there is no local spare available. Any traffic arriving on the node with the failed ISA will use the shunt to reach the master ISA.

3.2.1.4.3 AARP Peered Node/Instance Configuration

The multi-homed diverted AA subscriber in each peer node must be configured with the following parameters set in each node of the peer pair as follows:

- Service ID — Node specific
- Interface — Node specific
- SAP or spoke/SDP ID — Node specific
- AA-group ID — Node specific
- App-profile name — Content must be same in both peers to not affect behavior, recommend using same name and content
- Transit policy ID — Same in both (only applies if transits are used)
- AARP ID — Same in both
- shunt-sdp *sdp-id:vc-id* — Node specific but must properly cross-connect the local AA subscriber service with the peer lpipe/service shunt interface in order to operate properly for asymmetry removal for remote divert traffic. Peer AARPs will stay in standalone mode until cross-connect is configured properly.
- Master-selection mode — same in both.
- Other ISA-AA group configuration — Same in both, including fail-to, divert FC, and so on
- IOM traffic classification into a FC — Same in both (can affect AA divert since this is conditioned by the FC). This includes sub side, network side and shunt IOMs.

AARP operation has the following required dependencies:

- For multi-chassis, shunt links are configured and operationally Up.
- For multi-chassis, peer communications established.
- Dual-homed SAP or spoke configured.
- app-profile configured against SAP or spoke with divert (making the subscriber an AA subscriber). This endpoint is called the primary endpoint if more than one endpoint is configured for an AARP instance.
- All endpoints within an AARP instance must be of the same type (SAP or spoke).
- All endpoints with an AARP instance must be within the same service.

3.2.1.4.4 Multi-Chassis Control Link (MC-CTL)

A multi-chassis control link is automatically established between peer AARP instances to exchange configuration and status information. Information exchanged includes configured service, protecting SAP, spoke, redundant-interface name, shunt-sdp, app-profile, priority and operational states.

AARP requires configuration of the peer IPv4 system address in order to establish a session between the two node's system IPv4 addresses.

3.2.1.4.5 Multi-Chassis Datapath Shunts

When traffic needs to be remotely diverted it flows over shunts that are provisioned as *sdp-id:vc-id* between the dual-homed AA subscriber local service and a remote vc-switching lpipe.

Subscriber to Network Direction

The traffic is either handled locally (diverted to a local ISA when the AARP state is Master) or at the peer 7750 SR (redirect over the shunt lpipe when the local AARP state is Backup or Remote). When traffic arrives on the subscriber side spoke SDP of the shunt-lpipe, the system uses the AARP ID of the lpipe to associate with an app-profile, hence triggering lpipe divert. It is diverted to the same ISA used to service the dual-homed SAP or spoke SDP. The ISA then treats this traffic the same as if it was received locally on the dual-homed SAP or spoke SDP context. After ISA processing, the traffic returns on the network side of the lpipe to the peer. When the traffic returns to the original 7750 SR, the shunt lpipe terminates into the routed service and it makes a new routing decision.

Network to Subscriber Direction

The traffic is either handled locally (diverted to a local ISA when the AARP state is Master) or at the peer 7750 SR (remote divert over the shunt lpipe when the local AARP state is Backup or Remote). When traffic arrives on the shunt lpipe from the peer with an AARP ID and associated app-profile, it is diverted through AA on the way to the subscriber-side spoke SDP. After AA processing, the traffic returns on the subscriber side of the lpipe to the peer. When the traffic returns to the original 7750 SR, the shunt lpipe terminates into the routed service and it makes a new routing decision to go out the dual-homed SAP or spoke SDP.

AARP Operational States

In single node operation, there are two operational states, Master or Standalone. A single node AARP instance is Master when all these conditions are met, otherwise AARP is in the standalone state with is no asymmetry removal occurring:

- Dual-homed (primary) and dual-homed-secondary endpoints are configured
- Divert Capability is Up
- App Profile is diverting
- AA subscriber is configured

With multi-chassis operation there are 4 operational states for an AARP instance: master, backup, remote and standalone.

- Master — In multi-chassis operation, an AARP instance can only become operationally Master when the inter-chassis link datapath is operational and the control path is or was up, the received peer node status indicating the peer's AARP instance and similar dependencies is or was up, and the AARP priority is higher than the peer. When the priority is equal then higher system interface IP address is used as a tiebreak.
- The Master state will be immediately switched to Remote for AARP related failures that result in the instance being not ready. ICL datapath shunt SDP failures will cause the peer AARP go standalone. A shunt/Ipipe SDP failure is determined by the failure detection protocol used (BFD on routes, keep-alive on SDPs, LDP/RSVP, and so on).
- When a SAP or spoke SDP with an AARP instance is shutdown nothing changes for AARP, as packets can still use the AARP interface. When the SAP or spoke SDP is deleted, AARP will be disassociated from the spoke SDP/SAP before deleting. The AARP instance will still exist after deleting the SAP or spoke but without an association to an AA subscriber, the AARP state will go to standalone.
- Backup — Backup is the AARP state when all required conditions of the AARP instance are met except the master/backup priority evaluation.
- Remote — When an AARP instance is operating with remote divert set for the protecting SAP or spoke AA subscriber. The peer AARP instance is the Master, there is no Backup as the local system is not ready. This state is entered as a result of a failure in a local resource on the AARP instance, which triggers the divert traffic to the remote peer, such as a ISA failure without ISA backup). AA subscriber traffic is diverted over shunts to the peer.
- Standalone — AARP is not operational between the multi-chassis pair, with AA operating with local AA divert to the ISAs within that node. There is no Master or Backup. This is the starting initial state for the AARP instance, or as a result of a failure in a dependent ICL resource (MC-CTL communication link or shunt down).

An AARP instance activity switch is when one node moves from Master to remote or backup mode, with the peer node becoming Master. This can occur on a per-instance basis using the re-evaluate tool, or for all instances on an ISA that fails. On an AARP activity switch, AA divert changes from local to remote (or vice versa) such that any given packet will not be seen by both nodes, resulting in no missed packet counts or double counts against the AA subscriber.

AARP activity is non-revertive, in order to maximize the ID accuracy of flows. When an AARP instance toggles activity, packets are diverted to the newly active divert ISA and are processed as new flows, which for mid-session flows will often result in “unknown” traffic ID until those flows terminate. When the condition that triggered the AARP activity switch is resolved and the instance remains in backup state, in order to not cause an additional application ID impacting event. This is consistent with AA N+1 ISA activity switches.

Because AA ISA availability is a criteria for AARP switches, any ISA failure or shutdown will move all AARP instance activity to ISAs in the master peer nodes, such as during software upgrades of ISAs. Depending on the nature of the failure or sequence of an upgrade procedure, all AA traffic may be processed by ISAs in one of the peers with no traffic being processed by ISAs on the other node.

If it is desired to rebalance the ISA load between the peer nodes, there is a **tools perform application-assurance aarp aarp-id force-evaluate** command will re-run AARP activity evaluation on a per-ISA basis to determine Master/Backup AARP based on configured priority.

[Table 5](#) shows the interaction and dependencies between AARP states between a local node and its peer.

Table 5 Interaction and Dependencies Between AARP States

Local AARP Operation State	Peer AARP Operational State	Description
Master	Backup	Inter-Chassis Link (ICL) Communication established between AARP peers. AARP dependent resources are up (to-sub/from-sub shunt, aarp control link, dual-homed SAP or spoke SDP). AARP instances have negotiated initial state assignment using configured priority/system IP address. AA service is available for the dual-homed SAP or spoke subscriber. All to-sub/from-sub traffic specific to the dual-homed SAP or spoke SDP will be serviced on the local node. Peer node is available to takeover in the event of a AA service failure on the local node. Asymmetry is removed for the dual-homed SAP or spoke subscribers, serviced by AA on the local (master) node.
Master	Remote	Same as Master/Backup except: AA service is available on the local node. AA service is unavailable on the peer node.
Standalone	Standalone	Initial state of the AARP instances upon creation or a result of a failure in any of the AARP dependent resources. All to-sub/from-sub traffic for the dual-homed SAP or spoke will be serviced on each node independently. aarp instance operational state is outOfService on both sides. Asymmetry is not removed for the dual-homed SAP or spoke subscribers (traffic ID is not optimal).

3.2.1.5 ISA Overload Detection

Capacity cost resource counting does not have a hard per-ISA limit, since the cost values are decoupled from actual ISA resources. However, the value of the total summed cost per-ISA can be reported, and a threshold value can be set which will raise an event when exceeded.

ISA capacity overload detection and events are supported within the system resource monitoring / logging capabilities if the traffic and resource load crosses the following high and low load thresholds on a per-ISA basis:

- ISA capacity cost
- Flow table consumption (number of allocated flows)

- Flow setup rate
- Traffic volume
- Host IOM egress weighted average shared buffer pool use (within the egress QoS configuration for each group). These thresholds are also used for overload cut-through processing

While an app-profile is assigned to AA subscribers, the capacity-cost for that app-profile can be modified. The system makes updates in terms of the load balancing summary, but this does not trigger a re-balance.

In the absence of user configuration, the App-profile default capacity cost is 1. The range for capacity cost is 1 to 65535 (for example, for bandwidth based balancing the value 100 could represent 100 kb/s). 0 is an invalid value.

If the re-balancing of AA subscribers is required (for instance after the addition of new ISAs), there is a **tools** command to re-balance AA subscribers between ISAs within a group. Re-balance affects which AA subscribers divert to which ISAs based on capacity cost. Transit subs cannot be rebalanced independent of the parent (they move with the parent divert), and DSM subs cannot be load balanced as all subs on an ISA-AA are from the associated ISA-BB pair. The system attempts to move AA subscribers from the most full ISA to the least full ISA based on the load balancing mode. If the load becomes balanced or an AA subscriber move fails due to ISA resources or divert IOM service queuing resources, the load balancing terminates.

Alternatively, load balancing can be manually accomplished by the AA subscriber being removed and re-added. This will trigger a load balancing decision based on capacity-cost. For ESM, SAP, and spoke-sdp subscriber types, this can be accomplished by removing and re-applying the AA subscriber's app-profile. In the case of ESM AA subscribers, shutting down and re-enabling either sub-sla-mgmt or the hosts will have the same effect. Dynamic ESM AA subscribers will re-balance naturally over time as subscribers come and go from the network.

For transit AA subscriber deployments, the parent divert SAPs are load-balanced based on AA capacity cost from the app-profile configured against the SAP/SDP. The parent capacity cost should be configured to represent the maximum expected cost when all transit subs are present.

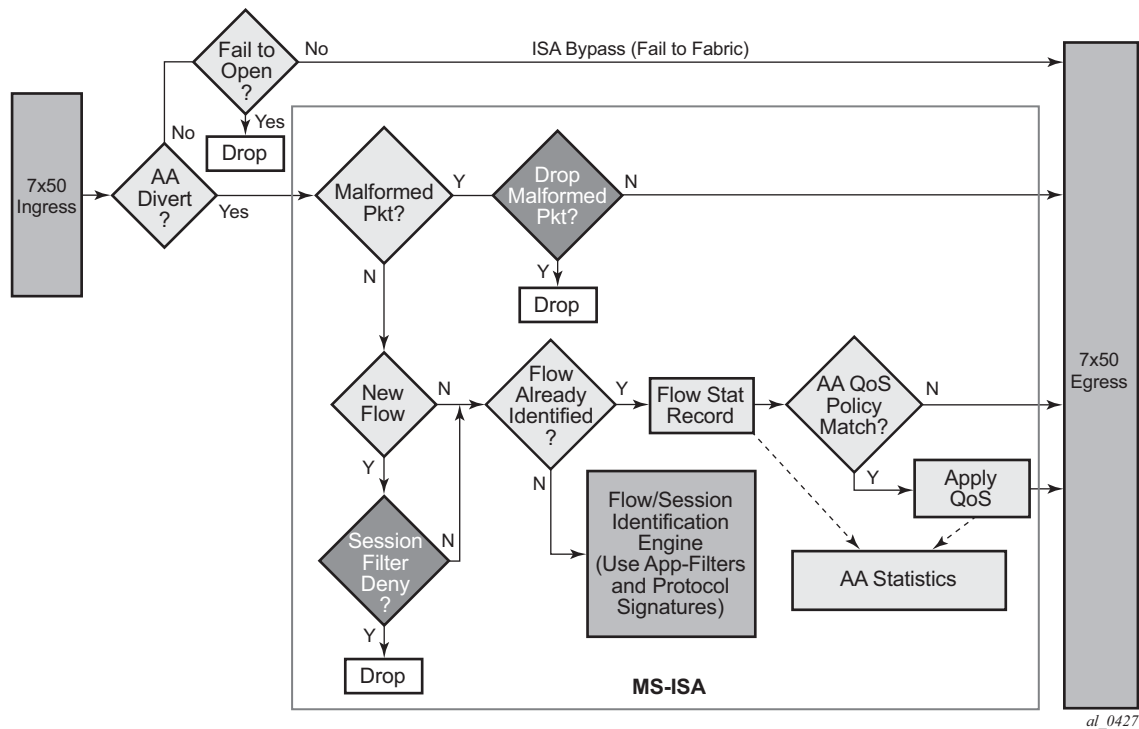
All traffic not matching a configured transit subscribers is dealt with as a member of the parent SAP and according to its app-profile.

3.2.2 AA Packet Processing

There are four key elements of Application Assurance packet processing (Figure 13):

1. Divert: Selection of traffic to be diverted to the AA ISA.
2. Identification of the traffic on a per flow (session) basis.
3. Reporting of the traffic volume and performance.
4. Policy treatment of the identified traffic.

Figure 13 Application Assurance High Level Functional Components



3.2.2.1 Divert of Traffic and Subscribers

Any traffic can be diverted for application-aware processing. Application Assurance is enabled through the assignment of an application profile as part of either an enhanced subscriber management or static configuration. This process enables the AA functionality for all traffic of interest to and from a given subscriber, SAP or spoke SDP. Which traffic is deemed of interest, is configured through an AA ISA group-specific configuration of forwarding classes (FCs) to be diverted to AA and enabled on a per subscriber, SAP, spoke SDP using application profiles.

Figure 14 shows the general mechanism for filtering traffic of interest and diverting this traffic to the appropriate AA ISA module residing on an IOM (referred as the host IOM). This traffic management divert method applies to both bridged and routed configurations.

Figure 14 Application Assurance Ingress Datapath

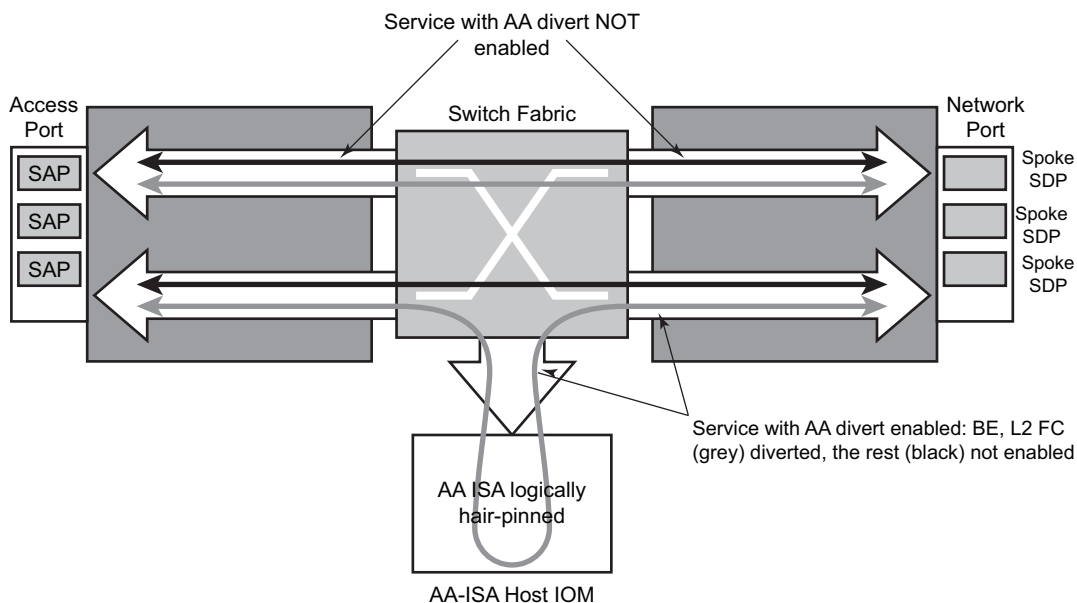


Fig_47

For a SAP, subscribers with application profiles enabling AA, the traffic is diverted to the active AA ISA using ingress QoS policy filters, identifying forwarding and sub-forwarding classes that could be diverted to the Application Assurance. Only single point (SAP, ESM, or DSM subscriber, spoke SDP) configuration is required to achieve divert for both traffic originated by and destined to a given AA subscriber. Diversion (divert) to the AA ISA is conditional based on the AA ISA status (enabled, failed, bypassed, and so on).

Unless the AA subscriber's application profile is configured as "divert" using Application Profiles and the FC is selected to be diverted as well, the normal ingress forwarding occurs. Traffic that is filtered for divert to AA ISAs is placed in the appropriate location for that system's AA ISA destination.

Users can leverage the extensive QoS capabilities of the router when deciding what IP traffic is diverted to the Application Assurance system for inspection. Through AA ISA group-wide configuration, at least one or more QoS forwarding classes with the "divert" option can be identified. The forwarding classes can be used for any AA subscriber traffic the service provider wants to inspect with Application Assurance.

3.2.2.1.1 Services and AA Subscribers

The 7750 SR and 7450 ESS AA ISA provides, for Layer 3 to Layer 7, packet processing used by the Application Assurance feature set. Application Assurance is applied to IPv4 and IPv6 traffic on a per-AA subscriber basis, where an AA subscriber is one of the following:

- ESM subscriber
- ESM-MAC subscriber (bridged residential/vRGW device)
- Distributed sub management (DSM) subscriber
- SAP or spoke
- Transit

Non-IPv4 and IPv6 traffic is not diverted to AA and is forwarded as if AA was not configured; however, AA divert is supported for IP over PPPoE on Layer 2 (Epipe or VPLS) SAPs. An AA subscriber can be contained in the following services:

- IES
- VPLS
- VLL — Epipe and Ipipe
- VPRN

Application Assurance is supported with:

- Bridged CO
- Routed CO
- Multi-homed COs
- Layer 2/Layer 3 VPN service access points and spoke SDPs

The AA ISA feature set uses existing 7750 SR or 7450 ESS QoS capabilities and further enhances them to provide application-aware traffic reporting and management on per individual AA subscriber, AA subscriber-type or group. A few examples of per-application capabilities within the above AA subscriber contexts include:

- Per AA subscriber, application traffic monitoring and reporting.
- Per application bandwidth shaping/policing/prioritization.
- Throttling of flow establishment rate.
- Limiting the number of active flows per application (such as BitTorrent, video or teleconference sessions, and so on).
- Application-level classification to provide higher or lower (including drop) level traffic management in the system (for example, IOM QoS) and network.

The following restrictions are noted — Application Assurance is not supported for tunneled transit traffic (GRE or L2TP tunnels using PPP or DHCP based policy) destined for a remote BRAS.

3.2.2.1.2 Spoke SDPs

AA on spoke SDP services allows AA divert of the spoke SDP, logically representing a remote service point, typically used where the remote node does not support AA. A given SAP or spoke SDP can be assigned an app-profile, and when this app-profile is enabled for **divert** all packets to and from that SAP or spoke SDP will be diverted to an AA ISA (for forwarding classes that are configured as divert eligible).

Table 6 shows spoke SDP divert capabilities.

Table 6 Spoke SDP Divert

Access Node Service (spoke SDP type)	Connected to Service				
	Epipe	VPLS	IES	VPRN	Ipipe
Epipe (Ethernet spoke)	Y	Y	Y	Y	Y
Ipipe (IP spoke)	N/A	N/A	Y	Y	Y
VPLS (Ethernet spoke)	N/A	Y	Y	Y	N

Spoke SDP divert is only supported on services to/from IOM3-XP or newer IOMs or IMMs.

3.2.2.1.3 Transit AA Subscribers

A transit AA subscriber is an ISA local AA subscriber contained within a parent AA subscriber. There are two types of transit AA subs:

- Transit IP AA subscribers: defined by Transit IP Policy as one or more /32 IP addresses per sub
- Transit Prefix AA subscribers: defined by Transit Prefix Policy as one or more prefix IP addresses, used in business VPNs

A transit AA subscriber incorporates the following attributes:

- Name
- IP address (one or more hosts)
- App-profile (the divert/no divert and capacity cost setting of the app-profile does not affect transit AA subscribers since divert occurs only against the parent SAP).

When a SAP or spoke-SDP diverted to AA is configured with transit subs, that SAP or Spoke-SDP is referred to as the parent AA subscriber. Transit AA subscribers are supported on the following parent SAPs or spoke SDPs that support AA divert:

Table 7 Transit AA Subscribers Support

Transit Subscriber Type	Epipe	VPLS	IES	VPRN	Ipipe
Transit IP	Y	N/A	Y	Y	N/A
Transit Prefix	Y	Y	Y	Y	Y

The transit AA subscribers within a given parent AA subscriber can be displayed using the **show application-assurance group transit-ip-policy** or **transit-prefix-policy** command.

For transit IP AA subscribers all packets are accounted for once in the ISA records. Therefore, transit IP AA subscriber counts do not count against the parent SAP in reporting. For transit prefix AA subscriber deployments using the **remote-site** command, traffic for the remote transit subs are processed and counted for both the local parent and the remote transit subscriber.

Transit AA Subscriber App-Profile

The app-profile assigned to the aa-sub-id affects both stats and control of the policy. App-profiles are assigned to the transit AA subscribers either explicitly when the transit-aa-sub is created, or by default (when not specified) according to a default app-profile configured in a transit-ip-policy or transit-prefix-policy. This allows transit AA subscribers to be treated with a different default app-profile than the app-profile (default or specified) set against the parent aa sub. The number of AA subscriber stats used per ISA is proportional to the number of AA subscribers including transit subscribers subs are added.

ASO policy override is supported for static transit subs.

Transit IP Policy and Transit Prefix Policy

A transit policy is associated with the parent (divert) SAP/SDP to define how transit AA subscribers are created within that parent. The transit policy must be defined in the context before it can be assigned to a parent. Transit IP subs can be created by the following methods:

- Static — CLI/SNMP configuration of a transit AA subscriber is done within the transit-ip-policy
- Dynamic — DHCP authentication
- Dynamic — RADIUS accounting to Policy and Charging Rules Function (PCRF) or AAA

Transit prefix subs are created by static CLI/SNMP configuration of a transit AA subscriber within the transit-prefix-policy. The transit prefix policy follows IP filter conventions for first match and ordering of entries. While for residential /32 transits if there is an IP address conflict between any static prefix transit subs, the latter config will be blocked, for business transit subs multiple overlapping address entries are allowed to enable longest match within subnets. IP addresses for a VPN site as an AA subscriber are configured with the transit prefix policy. There are two options:

- **aa-sub-ip** is used when the site is on the same side of the system as the parent SAP
- **network-ip** is used when the site is on the same opposite of the system as the parent SAP

A given transit prefix subscriber may only have either **aa-sub-ip** entries or **network-ip** entries but not both.

The IP addresses defined in the **transit-ip-policy** for a transit sub are full /32 IP addresses. The IP addresses defined in the transit-prefix-policy for a transit sub are any length from /0 to /32.

Multiple IP addresses (from any prefix/pool) can be assigned to a single transit AA sub. IP addresses must be unique within a transit policy, but can be re-used in separate policies (since they have parent specific context).

The transit policy contains the default app-profile for the transit sub if a transit policy is created but app-profile is not specified. An app-profile can be later explicitly assigned to the transit sub after the sub is created (using RADIUS COA, DHCP or static).

For dynamic transit IP subs, a sub-ident-policy (also used by ESM to associate sub ID policies to a SAP) can now also be associated with the AA subscriber parent by defining the sub-ident policy in the transit IP policy. This determines how sub identifying strings are derived from DHCP option 82 fields. The policy also contains app-profile-map which maps the strings to the defined app- profiles. Transit subs do not use the sla-profile or sub-profile aspects of the sub-ident-map.

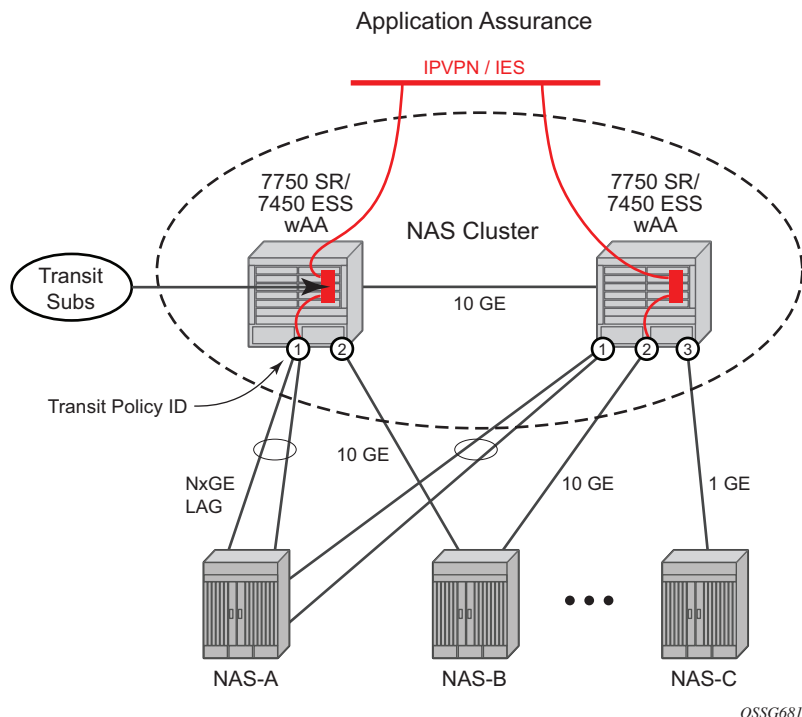
In the case of multi-homed transit subs, the transit-ip-policy must be the same on both nodes of the multi-homed parent link to ensure consistency of sub context and policy.

There are no configurable limit hosts per sub per sub (this is similar to lease-populate which limits the number of dynamic hosts per SAP), or, limit the number of transit subs per transit ip policy (parent). This is a function for the PE doing subscriber management.

If transit sub resource limits are exceeded (hosts per sub, or subs per ISA) the transit sub creation is blocked (for both static and dynamic models).

There is a per-ISA group/partition show list of AA subscribers in a transit-ip-policy which includes a parent field for transit subs (static versus dynamic identified).

Persistent AA statistics is supported dynamic transit AA subs, ensuring that accounting usage information is not lost when the sub disconnects prior to reporting interval end.

Static-remote-aa-sub Command**Figure 15 Static-remote-aa-sub Usage Topology**

This command enables unique ISA treatment of transit prefix subscribers configured on the opposite (remote) side of the system from the parent SAP or spoke SDP. Provisioning a transit sub as remote-aa-sub within a transit prefix policy enables the ISA to treat any network IP-based transit subs in the following ways:

- Treat packets for the parent AA subscriber independent of whether transits are also configured (stats and policers for parent work as usual).
- Subsequently treat the same packet as a transit-sub packet when matching to a configured transit sub (stats, policers).
- Allows natural direction of the packet for both the parent AA subscriber and the transit-AA subscriber, as shown in [Figure 15](#), where a packet from a remote client to a local server will be seen as to-sub for the parent, and from-sub for the transit sub that is logically at the far end site.
- Correct directionality of packet ID for all AA subscribers allows proper operation of app-filter flow-setup-direction

Static Transit AA Subscriber Provisionings

Static (through CLI/SNMP) provisioning of transit AA subscribers is supported. A profile policy override to set policy characteristics by ASO (as opposed to within an app-profile) is supported only for statically configured transit AA subs.

If there is an IP address conflict between a static and dynamic transit sub, the static takes precedence (per ESM). If the static is configured first, the dynamic transit sub will be rejected. If the dynamic is created first, a warning is provided before removing the dynamic transit sub and notifying the sub-manager by COA failure.

DHCP Transit IP AA Subscribers at DHCP Relay Node

DHCP-based transit sub creation provides a sub ID and lease time for IP addresses correlated to the ESM/subscriber context in the PE.

The 7750 DHCP relay agent creates dynamic DHCP AA subscribers when the DHCP ACK is received from the DHCP server, including the sub name, IP address and app-profile from DHCP Option 67 (if present) when the DHCP ACK messages passes through AA node to the downstream subscriber-edge node. If there is no app-profile assigned when the transit AA subscriber is created, a default transit AA subscriber app-profile is used (configured in the transit-ip-policy assigned against the divert parent AA subscriber).

This is compatible with the ESM router edge as well as third-party BRAS and CMTS.

Dynamic AA subscriber stats records are persistent across modem reset/session releases. The end of accounting records are created when transit subs are released.

Multiple IPs per transit AA subscriber are determined by seeing a common the DHCP Option 82 cct ID.

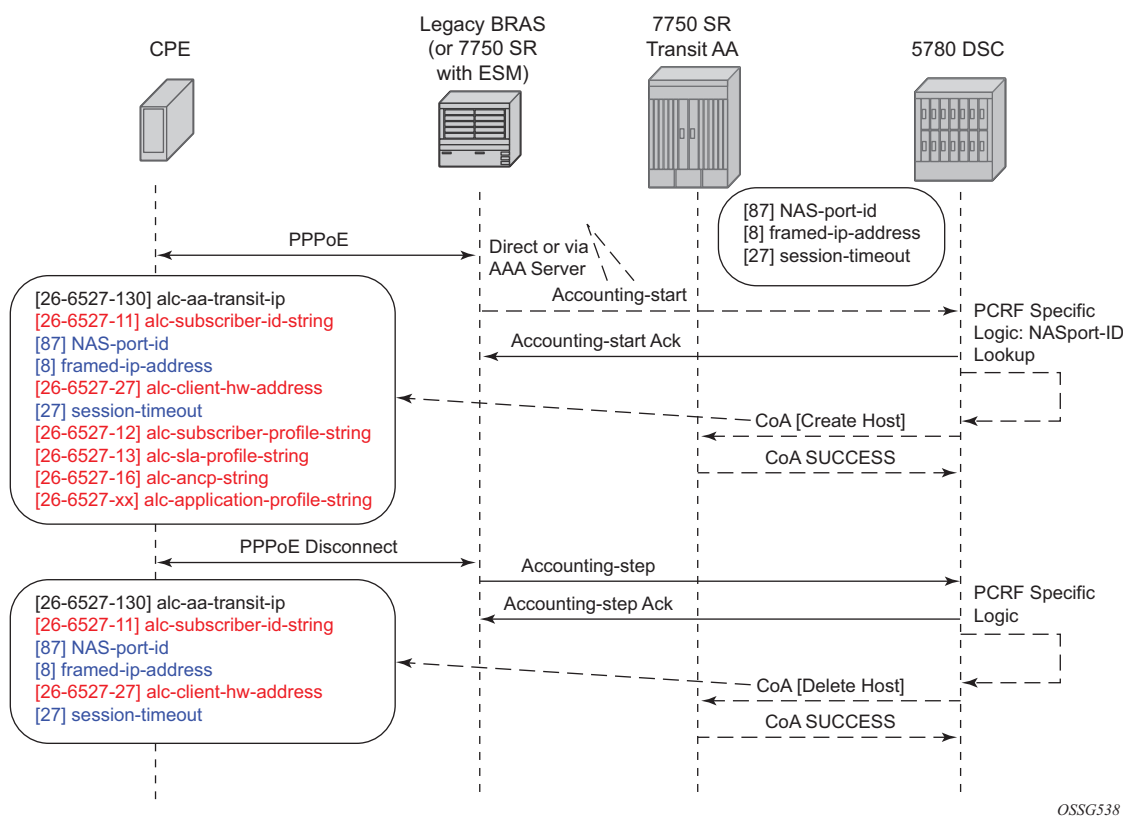
RADIUS Transit AA Subscribers

Transit subs can be dynamically provisioned by RADIUS accounting start messages forwarded by the RADIUS AAA server to a RADIUS sub-manager function at the OSS layer (5780 DSC). This RADIUS sub manager manages dynamic transit AA subscribers on the appropriate ISA and transit-ip-policy based on the RADIUS accounting information. The interface for the sub manager to configure transit AA subscribers is RADIUS COA messages, which are acknowledged with a COA success message to the sub manager.

If a dynamic transit sub cannot be created as requested by a COA due to resource constraints or conflicts, the node replies to the sub manager with a COA fail message so that retries will not continue. This message should contain information as to the cause of the rejection. Multiple IPs per sub are allowed when common sub-ID names are seen, but with differing IP hosts.

When a RADIUS update or COA message is seen, it could contain a modified IP address or app-profile for an existing transit sub which is accepted without affecting transit AA subscriber statistics. These transit AA subscribers are removed by the sub manager when a RADIUS accounting stop message is received.

Figure 16 **RADIUS COA Example**



The attributes in RADIUS COA that identify the downstream transit AA subscribers are:

- Downstream BRAS/ CMTS: NAS-port-ID
- IP address: framed-ip-address
- Subscriber ID: per RADIUS accounting sub-id-string

Seen-IP RADIUS Notification

Seen-IP transit subscriber notification provides RADIUS Accounting Start notification of the IP addresses and location of active subscribers within a parent AA service. This allows a PCRF to dynamically manage RADIUS AA subscriber policy (create, modify, delete) without requiring static network topology mapping of a subscriber edge gateway to the parent transit service.

When **detect-seen-IP** is enabled within a transit policy, the ISA will detect IP flows on an AA parent subscriber that do not map to an existing transit AA subscriber. It will then use a simple RADIUS Accounting Start notification from the transit AA node to the PCRF to initiate subscriber creation, providing information on the location of the transit subscriber traffic. This provides notice for subscriber authentication changes, such as new subscriber sessions or new host IP addresses added to an existing AA subscriber, while being independent of the network topology for how the BNG is homed into the transit AA nodes.

The RADIUS Accounting Start message is sent to the RADIUS Server referenced by the specified **seen-ip-radius-acct-policy**. This RADIUS message contains the following information about the flow:

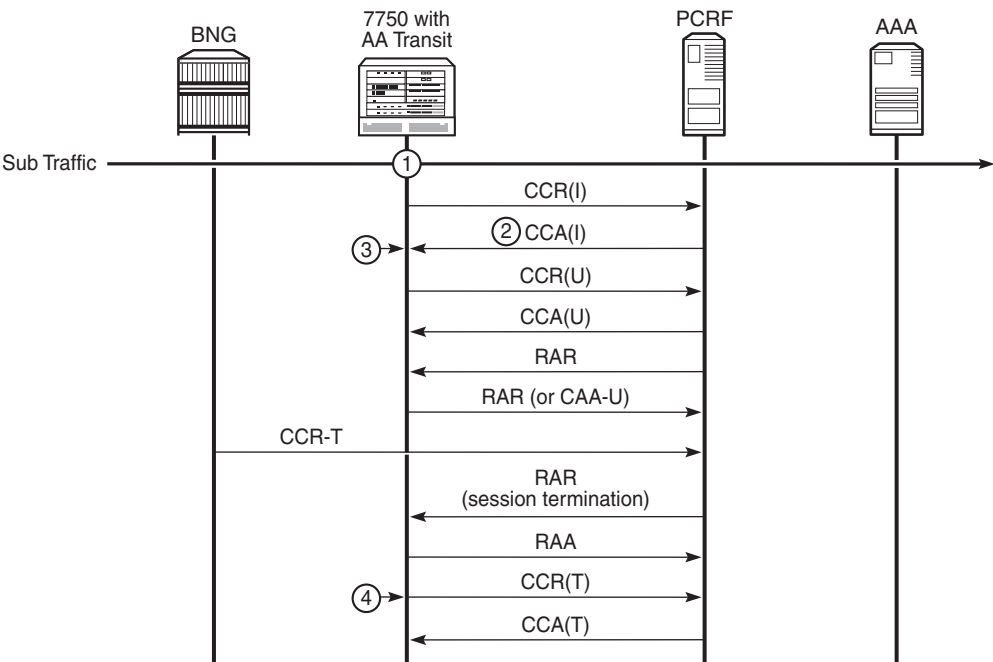
- Subscriber-side IP address
- Parent SAP or spoke-SDP ID (NAS port ID)
- IP address of node making the request
- Peer SAP or spoke-SDP ID (NAS port ID), if configured
- Peer IP address of SR making the request, if configured
- AARP ID, if configured

Diameter Transit AA Subscriber

For Diameter transit AA subscribers, AA auto-detects new IP addresses and notifies the PCRF of new subscribers via a Gx CCR-I message. The PCRF locates the subscriber's AA policy and returns the information via CCA-I message to AA.

[Figure 17](#) shows a 3GPP pull model, whereby AA initiates the Gx session. [Table 8](#) describes the figure. The PCRF can, at any time after the session is established, push new policies using a RAR message. New policies can include new usage-monitoring or AA ASO values.

Figure 17 3GPP Pull Model



25621

Table 8 3GPP Pull Model Description

Legend	Description
1	AA detects a new IP address, and sends a CCR-I containing the subscriber-side IP address
2	CCA(I) contains subscriber AA policy information
3	AA applies an AA appProfile, ASOs, and any AA usage monitoring
4	AA reports usage counters for all specified or enabled usage monitoring keys, and removes the sub

The CCR-I message from the 7750 SR node to PCRF contains the following:

- Session ID
- Subscriber-side IP address
- IP-CAN-Type AVP (if enabled) with the value “tbc”
- Subscription ID AVP, with the following characteristics (if *avp-subscription-id* is configured as *subscriber-id*):

- Type: END_USER_E164 (private by default)
- ID: auto-generated unique ID
- Destination-Realm as configured in Diameter-Peer-Policy
- Destination-Host if configured in Diameter-Peer-Policy

The CCA-I message from PCRF to the 7750 SR node contains the following:

- Session ID
- Charging-Rule-Install containing the following information:

```
Charging-Rule-Definition ::= <AVP Header: 1003>
{Charging-Rule-Name}
[TDF-Application-Identifier]
[Monitoring-Key]
[AA-Functions {]
    AA profile
    AA-App-Service-Options {
        AA-App-Service-Options-Name
        AA-App-Service-Options-Value
    }
}
.....
[AVP]
```

- Charging-Rule-Name
 - Usage monitoring: Starts with “AA-UM:”
 - AppProfile and ASOs: Starts with “AA-Functions:”
- AA-Functions: AVPs to set AA profile and ASO values
- TDF-application-identifier: This field specifies a predefined AA charging group, application group, or application name for which usage monitoring functionality is required.

Termination of the Gx session is only done after AA receives an RAR-T message from PCRF with the session-release-cause AVP meeting the configured threshold. After replying to an RAR message with an RAA message, AA sends a CCR-T message with reports of usage counters, if any are enabled.

[Table 9](#) lists the AVPs used for Diameter transit AA subs.

Table 9 **Used AVPs**

AVP	Category	Details	User Configurable
Session-Id	M	Globally unique Generated for each session as: <peer identity>;<high 32 bits>;<low 32 bits>;[<optional value>;]<subscriber ip>	N
Origin-Host	M	Configurable under aaa diameter-peer-policy	Y

Table 9 **Used AVPs (Continued)**

AVP	Category	Details	User Configurable
Origin-Realm	M	Configurable under aaa diameter-peer-policy	Y
Destination-Realm	M	Configurable under aaa diameter-peer-policy	Y
Auth-Application-Id	M	Set as Gx (16777238)	N
CC-Request-Type	M	Set to INITIAL_REQUEST (1) when initiating a new session Set to TERMINATION_REQUEST (3) when ending a session Set to UPDATE_REQUEST (2) in all other situations	N
CC-Request-Number	M	Generated internally according to Gx specifications Request numbering starts at 0	N
Subscription-Id	M	Configurable using Subscription-Id-Type and Subscription-Id-Data	—
Subscription-Id-Type	M	Configurable under subscriber-mgmt>diameter-application-policy>gx>avp-subscriber-id <i>origin</i>	Y
Subscription-Id-Data	M	Configurable under subscriber-mgmt>diameter-application-policy>gx>avp-subscriber-id <i>origin [type type]</i>	Y
Framed-IP-Address	M	Set to the subscriber's IP address as seen by AA-ISA in the from-sub direction of the data traffic	N

When the Subscription-Id-Type is “Subname”, then Subscription-Id-Data is auto-generated by AA to be unique node-wide, using the transit IP policy, SAP, and sub IP address.

Unlike AA ESM Diameter-controlled subscribers, transit Gx AA subscribers are not required to support ADC rules over Gx.

Transit Gx AA subscribers use PCC rules as per ESM Diameter AA subscriber implementation, and therefore uses AA-Function AVP.

For transit Gx AA subs, similarly to ESM Gx-controlled subs, the PCRF can set the subID in a CCR-I by sending a PCC rule with the name of the charging rule prefixed with “sub-id:”. The AVP appears as follows:

```
charging-rule-install (1001) VM----- [44]
```



```

vendor-id TGPP
data [32] (Grouped)
    charging-rule-name (1005) VM----- [30]
        vendor-id TGPP
        data [18] (UTF8String) : Sub-Id:subID-name

```

In addition to using the AA Function AVP, AA supports the configuration of the application profile and ASOs by the PCRF via a CCR-I, CCR-U, or RAR that has PCC rules with the name of the charging rule prefixed with “AA-Functions:App:” or “AA-Functions:ASO”, such as:

```

charging_rule_install[0].charging_rule_name[0] = AA-Functions:App:<name>
charging_rule_install[0].charging_rule_name[1] = AA-Functions:ASO:<char>:<val>
...
charging_rule_install[0].charging_rule_name[n] = AA-Functions:ASO:<char>:<val>

```

AA allows for the definition of up to 32 ASOs. If the number of ASOs is larger than what can fit within a single charging-rule-install AVP, multiple charging-rule-install AVPs can be used in the CCR-I message.

As the Gx protocol is already supported by the 7750 SR/VSR system, there are no new configurations required. All existing configurations introduced to support ESM GX control on a BNG can be re-used in AA transit deployment.

Transit AA Subscriber Persistence

Transit AA subscribers can be persistent within a single node, since, in some cases, there is not a dual-node BNG subscriber redundancy configuration. This allows a single node that has dynamically created transit subs to retain the subscriber state, context, and statistics across a node or ISA reboot.

If dynamic transit AA subscribers are released, renewed, or otherwise changed during an outage or reboot of a transit AA node, the sub manager will notify the transit node of these changes.

Prefix transit subs are not affected by persistence since they can only be statically configured.

Transit Diameter AA Subscriber Geo-Redundancy

If there is no Multi Chassis Synchronization (MCS) between the two peer nodes, the two geo-redundant nodes are configured as two distinct realm nodes from the PCRF point of view. Each node acts independently of the other node. After a switch-over, AA on the newly active node detects new traffic flows with new IP addresses. AA notifies PCRF with a CCR-I message to retrieve subscriber policies. Once PCRF confirms the same IP address used on a different Gx session ID, it deletes the old session for that IP address.

Similar behavior takes place if an MCS is configured with session IDs and OSI states journaled across, as per ESM implementation. The two geo-redundant nodes are configured with the same host realm, and appear to PCRF as one node. After a switch-over, AA-ISA on the newly active node detects new traffic flows with new IP addresses. AA-ISA notifies PCRF with a CCR-I message to retrieve subscriber policies. The Gx session ID used is unique and different from the session ID used on the previously active node. Once PCRF confirms the same IP address used on a different Gx session ID, it deletes the old session for that IP address.

Policers for Transit AA Subscribers

AA subscriber per-subscriber policers can provide per-SAP policing for the parent SAP, with transit AA subscribers each supporting distinct per-subscriber policers within the parent (packets are only processed once against one AA subscriber – the parent or the transit subscriber). Packets matching transit AA subscribers and policers will not be included in a parent policer.

There is no policer hierarchy unless system wide policers are referred to by both the parent AA subscriber and transit AA subscriber. When the remote-site configuration is not used, system policers can be used to police all traffic for a site containing transits, subject to constraints on system policer scale.

When the remote-AA subscriber config is used, the parent owns all packets for stats and policing, so any transit subscriber configuration within the parent does not affect the stats or policers. AA policers are supported on a transit subscriber basis, across all (multiple) IP prefixes per sub.

ISA Host IOM for Transit Subs

The AA divert IOM is not impacted by transit AA subscribers in the divert parent. The ISA host IOM egress datapath functions to convert the parent SAP into transit AA subscribers that are then handled by the ISA consistent with all other AA subscriber features. The ISA itself treats all AA subscribers equally regardless of whether the AA subscriber is from ESM, from DSM, from an SAP, or from a transit subscriber in a parent SAP or spoke.

Prefix transit subs can only be created on IOM3-xp as host IOM, or with MS-ISM as host for ISA2. Asymmetry removal requires IOM3-xp or MS-ISM as host and IOM3-xp or newer (IMM) as divert IOM.

3.2.2.1.4 AA Subscriber Application Service Definition

- [Application Profile](#)
- [Application Profile Map](#)
- [Application Service Options \(ASOs\)](#)
- [ASO Overrides](#)

Application Profile

Application profiles enable application assurance service for a given ESM or DSM subscriber, Service Access Point or spoke SDP (AA subscriber). Each application profile is unique in the system and defines the AA service that the AA subscriber will receive. An ESM subscriber can be assigned to an application profile which affects every host of the particular subscriber. For SAP or spoke SDP AA subscribers, an application profile can be assigned which affects all traffic originated/destined over that SAP or spoke SDP. By default, ESM and DSM subscribers, SAPs or spoke SDPs are not assigned an application profile.

The following are main properties of application profiles.

- One or more application profiles can be configured in the system.
- Application profiles specify whether or not AA subscriber's traffic is to be diverted to Application Assurance.
- Application profiles are defined by an operator can reference the configured application service options (ASO) characteristics (see [Application Service Options \(ASOs\)](#)).
- Application profiles must only be assigned once AA resources (AA ISA cards) are configured.
- Application profiles can be assigned a capacity cost used for subscriber load balancing among ISAs within the AA group (see [ISA Load Balancing](#)).

- Application profiles can be assigned to a scope from a subscriber or session, which controls whether the application profile is applied to the entire subscriber or to a device.

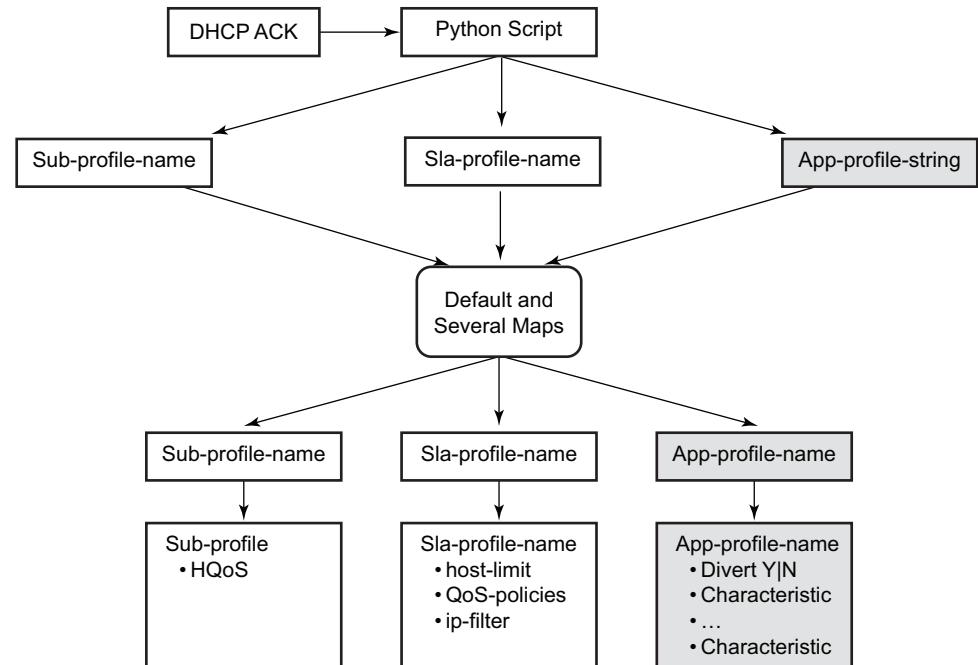
ESM and DSM policy includes an application profile string. The string points to an application profile pre-provisioned within the router and is derived by:

- Parsing the DHCP Option 82 sub-option 1 circuit ID payload, vendor specific sub-option 9, or customer-defined option different from option 82, during authentication and the DHCPDISCOVER, as well as re-authentication and the subscriber's DHCPREQUEST.
- RADIUS using a new VSA: [26-6527-45] Alc-App-Prof-Str
- DIAMETER using "AA-profile-name" AVP under ADC rule.
- Inherited by defaults in the **sap>sub-sla-mgmt** context, to allow default application profile assignment if no application profile was provided.
- Static configuration.

Mid-session (PPP/DHCP) changes to the application profile string allows:

- Modification of the application profile a subscriber is mapped to and pushes the change into the network as opposed to waiting for the subscriber to re-authenticate to the network.
- Change to the subscribers application profile inline, without a need for the subscriber to re-authenticate to RADIUS or perform any DHCP message exchange (renew or discover) to modify their IP information.

Figure 18 Determining the Subscriber Profile, SLA Profile and Application Profile of a Host



OSSG170

Application Profile Map

Application Assurance adds new map (**app-profile-map**) application profile command to associate an *app-profile-string* from dynamic subscriber management to a specific application profile using its app-profile-name that has been pre-provisioned. The application profile map is configured in the **config>subscr-mgmt>sub-ident-pol** context.

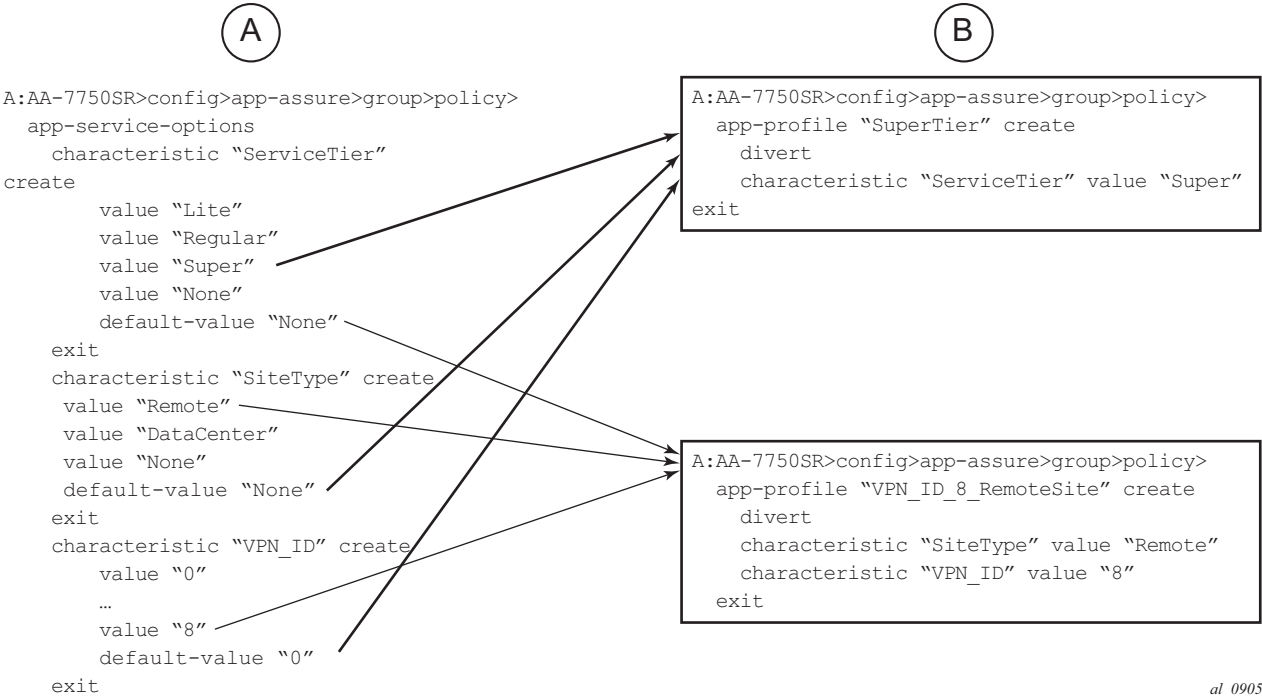
The pre-defined subscriber identification policy has to be assigned to a SAP, which determines the sub-id, sub-, sla-, and app-profiles.

Application Service Options (ASOs)

ASOs are used to define service provider and/or customer visible network control (policy) that is common between sets of AA subscribers (for example, upstream/downstream bandwidth for a tier of AA service). ASO definition decouples every AA subscriber from needing subscriber-specific entries in the AQP for standard network services.

As an example, an operator can define an ASO called ServiceTier to define various HSI services (Super, Lite, and so on) (Figure 19-A). The operator can then reference these defined ASOs when creating the App Profiles that are assigned to AA subscribers (Figure 19-B).

Figure 19 Configuration Example



Then, the defined ASOs are used in the AQP definition to determine the desired treatment or policy (Figure 20).

Figure 20 AQP Definition Example

```
app-qos-policy
  entry 50 create
    description "Limit downstream b/w for Super
subscribers"
    match
      traffic-direction network-to-subscriber
      characteristic "ServiceTier" eq "Super"
    exit
    action
      bandwidth-policer "SuperDown"
    exit
    no shutdown
  exit
entry 110 create
  match
    application-group eq "Tunneling"
    characteristic "SiteType" eq "Remote"
  exit
  action
    remark fc af
  exit
  no shutdown
exit
```

al_0906

Alternatively, if ASOs were not used in the previous example, then the operator would have to define a unique AQP entry for every subscriber. Each of these AQPs will have its “match” criteria setup to point to the subscriber ID, while the action for all of these unique AQPs will be the same for the same service (for Tier 1 service, the policer bandwidth will be the same for all Tier 1 AA subscribers) ([Figure 21](#)).

Figure 21 **Single ASO Example**

```
7750SR>config>aa>group>policy>aqp>
entry 100 create
  match
    aa-sub eq " sub_1"
  exit
  action
    bandwidth-policer "superDown"
  exit
  no shutdown
exit

entry 101 create
  match
    aa-sub eq " sub_2"
  exit
  action
    bandwidth-policer "superDown"
  exit
  no shutdown
exit

entry 102 create
  match
    aa-sub eq " sub_3"
  exit
  action
    bandwidth-policer "superDown"
  exit
  no shutdown
```

al_0907

The example in [Figure 21](#), shows how the use of just a single ASO can save the user from having to provision an AQP entry every time a subscriber is created.

Other example uses of ASO entries include:

- Entry per application group that is to be managed, such as VoIP, P2P, HTTP.
- Several entries where specific applications within an application group can individually be managed as service parameters, for example, HTTP content from a specific content provider, or streaming video from network television or games.
- HSI tiers (for example, Gold, Silver, and Bronze for specifying bandwidth levels).
- VPN customer ID.

Application characteristics are defined as specific to the services offered within the operator network. The operator defines ASO characteristics and assigns to each ASO one or more values to define service offering to the customers.

The following are the main elements of an ASO:

- A unique name is applied to each characteristic.
- The name is unique to the group-partition-policy, but the expectation is that characteristics will be consistent network wide.
- Operator-defined values (variables) are defined for each characteristic and are unique to each characteristic. A default value must be specified from the set of the values configured.

The following lists how ASO characteristics are used:

- Application service options are used as input to application profiles.
- AQP rule sets also use the ASO characteristics to influence how specific traffic is inspected and policies applied.
- Multiple ASO characteristic values are allowed in a single rule.

Syntax checking is performed when defining application profiles and AQPs that include application characteristics. This ensures:

- The characteristic is correctly identified.
- In an app-profile and app-qos-policy when specifying a characteristic, the value must be specified. The “default-value” applies if a characteristic is not specified within an app-profile.

ASO Overrides

This feature enables individual attributes/values to be set against an AA subscriber complementary to using app-profiles. The AA subscriber types supported that can have ASO overrides by CLI/SNMP are provisioned business AA SAPs and spoke SDPs, and statically-provisioned transit AA subs. Dynamic AA subscribers (ESM and transit subs) can have ASO overrides applied by RADIUS override VSAs.

Application profile assignment is still used to obtain the following information:

- The application-assurance group (and partition) to which the AA subscriber is being assigned to
- Whether or not the traffic should be diverted
- Capacity-cost (for load balancing to a multi-isa group)

The information configured in the app-profile is also used, but the following can be overridden:

- ASO characteristics and values (these are from the policy defined in the group and partition)

The overrides are specific to a single AA subscriber. An ASO override does affect any other AA subscriber or the app-profile config itself.

Typically the ASO characteristics in the app-profile would not be specified, thus leaving all characteristics at their default values. This is not mandatory though and the app-profile could specify any ASO characteristic and non-default value.

The AQP has entries that can refer to ASO characteristics (attributes) and values in their match criteria. In the absence of any individual attribute/value override, an AA subscriber will continue to work as before - using the ASO characteristics/values defined inside the app-profile assigned to them. With overrides, the AA subscriber attributes used in AQP lookups are the combination of the following:

- The characteristics/values from the app-profile,
- Any specific characteristics and values overridden for that AA subscriber.

Show command output display the combined set of attributes that apply to the AA subscriber.

The **override** commands can only be used if there is already an app-profile assigned to the AA subscriber, otherwise, the overrides are rejected.

The app-profile attribute override is assigned to a specific AA subscriber (SAP, spoke SDP) within the AA Group:partition with where the subscriber exists. While subscriber names are unique, the Group:partition policy context where apps, app-profiles and ASO characteristics are defined is relevant to the override context. Override for ESM subscribers can be triggered via DIAMETER or RADIUS.

AA Subscriber Scale Mode

An AA VPN policy is generally administered using a per-site (AA subscriber) policy attribute assignment (ASO override), as opposed to a service profile based model commonly used for residential services. Due to this, the number of attributes and values of ASOs that can be needed in an AA VPN service will be much larger than ASO scale needed for residential uses.

On the other hand, the number of AA subscribers needed per node and per ISA is much smaller for VPN services, and the size of each in bandwidth is generally much larger than residential.

In conjunction with App-profile ASO override, an AA-group should be set to a mode optimized for the deployment scenario into a mode optimized for VPN scale requirements:

```
config>isa>aa-group>aa-sub-scale {residential | vpn}
```

3.2.2.2 Application Identification

Application identification means there is sufficient flow information to provide the network operator with a view to the underlying nature and value of the content.

Application ID does not include:

- Anti-virus signatures per IPS/UTM.
- Content inspection (e-mail, text, picture, or video images). The payload data content of flows is typically not examined as part of the application identification.

Application Assurance can identify and measure non-encrypted IP traffic flows using any available information from Layer 2 to Layer 7, and encrypted IP traffic flows using heuristic techniques.

Application Assurance attempts to positively identify the protocols and applications for flows based on a pattern signature observation of the setup and initial packets in a flow. The system correlates control and data flows belonging to the same application. In parallel, statistical and behavioral techniques are also used to identify the application. Until identified, the flow will not have a known application and will be treated according to the default policies (AQP policies defined using all or any ASO characteristics, subscriber Id and traffic direction as match criteria) for traffic for that AA subscriber, app-profile and direction (packets will be forwarded unless an action is configured otherwise). If the identification beyond OSI Layer 2 is not successful, the flow will be flagged as an unknown protocol type, (for example `unknown_tcp` or `unknown_udp`). The unknown traffic is handled as part of all application statistics and policy, including generation of stats on the volume of unknown traffic.

Application Assurance allows operators to optionally define port-based applications for trusted TCP or UDP ports. Operators must explicitly identify a TCP/UDP port or ports in an application filter used for trusted port application definition and specify whether a protocol signature-based application identification is to be performed on a flow or not. Two options are available:

- If no protocol signature processing is required (expected to be used only when (A) AQP policy must be performed from the first packet seen, (B) the protocol signature processing requires more than 1 packet to positively identify a protocol/application, and (C) no other application traffic runs over a given TCP/UDP port), the first packet seen by AA ISA for a given flow on that TCP/UDP port will allow application identification. The traffic for a given flow will be identified as “trusted tcp/trusted_udp” protocols.

- If protocol signature verification of an application is required (expected to be used only when (a) AQP policy must be performed from the first packet seen, (b) the protocol signature processing requires more than 1 packet to positively identify a protocol/application, but (c) other application traffic may run over a given TCP/UDP port, for example TCP port 80), the first packet seen will identify the application but protocol signature-based analysis continues. Once the identification completes, the application is re-evaluated against the remaining application filters allowing detection and policy control of unexpected applications on a “trusted” port.

At Application Assurance system startup or after an AA ISA activity switch, all open flows are marked with the existing protocol signature and have a policy applied according to an application based on the existing protocol until they end or the identification of an in-progress flow is possible. Statistics are generated.

From the first packet of a flow, a default per AA subscriber AQP policy is applied to every packet. Once an application is identified, subsequent packets for a flow will have AA subscriber and application-specific AQP applied. The AA-generated statistics for the flow with AA subscriber and application context are collected based on the final determination of the flow's application. A subset of the applications may be monitored on an ongoing basis to further refine the identification of applications carried with the traffic flow and to identify applications using an external application wrapper to evade detection.

3.2.2.2.1 Application Assurance Identification Components

Figure 22 shows the relationship between the Application Assurance system components used to identify applications and configure Application Assurance related capabilities. Each ID-related component is defined as follows:

- Protocol signatures
- Application filters
- Applications
- Application groups
- Charging groups

Figure 22 Policy Structure

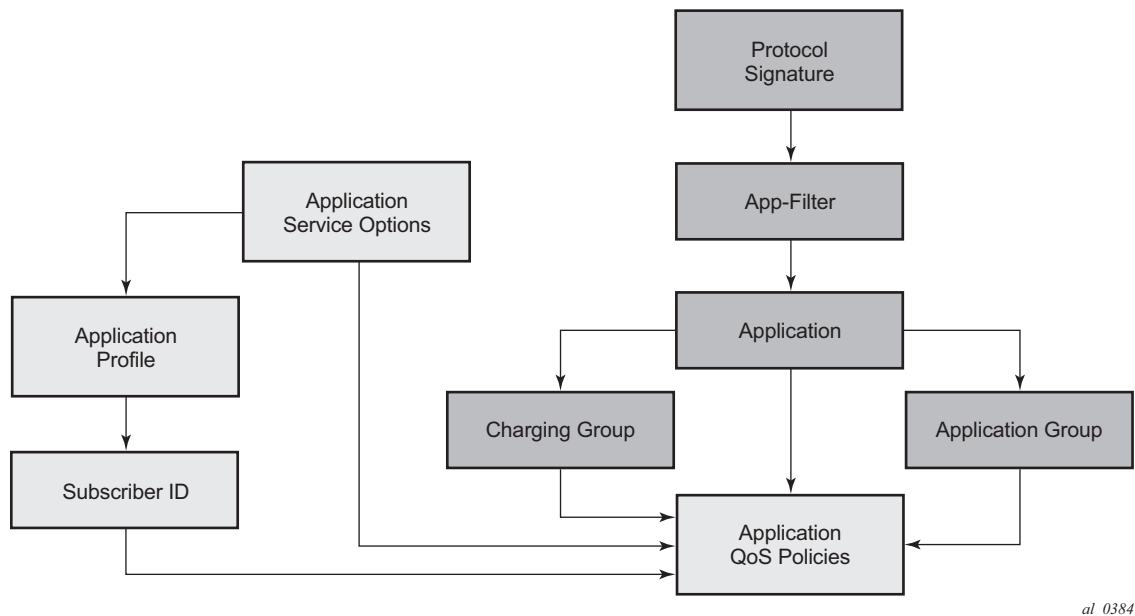


Table 10 provides an overview of how those various components used in Application Assurance to recognize types of flows and sessions.

Table 10 AA Flows and Sessions

Term	Definition	Examples
Protocol Signature	Nokia's proprietary component of AA flow identification provided as part of AA S/W load to identify protocols used by clients. Where a protocol is defined as an agreed upon format for transmitting data between two devices.	Tftp, iMap, msn-msgr, RTP, emule, http_video, bittorrent, SIP Nokia's protocol signatures do not rely on IP port numbers to identify a TCP/UDP port based protocols and applications in order to avoid eliminate false-positives but allow operators to define application filters if a port-based identification is deemed adequate (see an example below).
Application Filter	Operator configurable, optional component of AA flow identification that uses any combination of protocol signatures, server IP address and port, flow set-up direction, configurable expressions (for example an HTTP string match) to identify user's traffic.	http_video + IP address of partner's video server or http_video + an HTTP string to identify partner's video content TCP or UDP + TCP/UDP port number to identify a TCP or UDP based protocol or application.

Table 10 AA Flows and Sessions (Continued)

Term	Definition	Examples
Application	Operator configurable, optional component of AA flow identification that allows defining any specific forms of traffic to and from end user clients by combining application filter entries	Google Talk, POP3, YouTube, iTunes, Shoutcast
Application Charging Group	Operator configurable, optional component of AA flow identification that allows grouping of similar end use applications using operator defined names and groups.	IM, Mail, Multimedia, P2P, Tunneling, Web, Other
Clients	End user programs that generate user traffic for applications and protocols, and that are used in a process of AA flow identification verification.	The list of clients is constantly evolving as new clients or versions are introduced in the marketplace. The following example illustrates clients that may be used to generate Application traffic matching BitTorrent application defined using BitTorrent and DHT protocol signatures: Limewire, BitTorrent, Azureus, Ktorrent, Transmission, Utorrent

3.2.2.2 Protocol Signatures

The set of signatures used to identify protocols is generated by Nokia and included with the Application Assurance software load. The signature set includes:

- The protocols that can be identified with this load, using a combination of pattern and behavioral techniques. The protocols are used in generating statistics by protocol, and are used as input in combination with other information to identify applications.
- Pattern signatures are the set of pattern-match signatures used in analysis.
- Behavior signatures are the set of diagnostic techniques used in analysis.

Dynamic upgrades of the signatures in the system are implemented by invoking an **admin application-assurance upgrade** command and then performing AA ISA activity switches.

The protocol signatures are included in aa-isa.tim software load which is not tightly coupled with software releases allowing for protocol signature updates without upgrading and impacting of routing/forwarding engines as part of an ISSU upgrade that updates only the AA ISA software. Refer to upgrade procedures described in the *SR OS 16.0.Rx Software Release Notes* for detailed information.

Since protocol signatures are intended to be the most basic block of Application Identification, other AA components like Application Filters are provided to further customize Protocol Signatures allowing operators to customize their applications and to reduce a need for a new Protocol Signature load when a new Application may need to be identified. This architecture gives operators more flexibility in responding to ever changing needs in application identifications.

Signature upgrade without a router upgrade is allowed within a major router release independently of system ISSU limits. An AA ISA signature upgrade is supported before the first ISSU router release (for example, operators can upgrade signatures for pre-ISSU minor releases).

In addition, any router release from ISSU introduction release can run any newer aa-isa.tim image within the same major release by performing an aa-isa.tim single step upgrade. For example, release 8.4 may be upgraded in a single step to run release 8.14 of isa-aa.tim.

Each protocol, except internal protocols used for special-case processing statistic gathering (cut-though, for example), can be referenced in the definition of one or multiple applications (through the App-Filter definition). Assignment of a supported protocol to an app-filter or application is not mandatory. Protocols not assigned to an application are automatically mapped by the system to the default **Unknown** application.

3.2.2.2.3 Custom Protocols

Custom protocols are supported using configurable strings (up to 16 hex octets) for pattern-matched application identification in the payload of TCP or UDP based applications (mutually exclusive to other string matches in an app-filter).

The match is specified for the client-to-server, server-to-client, or any direction for TCP based applications, and in the any direction for UDP based applications.

There is a configurable description and custom protocol id for a protocol, with configurable shutdown. When disabled, traffic is identified as if the protocol was not configured.

Custom protocols and ALU-provided protocols are functionally equivalent. Custom protocols are used in application definition without limitations (all app-filter entries except strings are supported). Collection of custom protocol statistics on a partition/ISA group/special study sub level is supported.

3.2.2.2.4 Protocol Shutdown

The protocol **shutdown** feature provides the ability for signature upgrades without automatically affecting policy behavior, especially if some or even all new signatures are not required for a service. All new signatures are disabled on upgrade by default to ensure no policy/service impact because of the signature update.

All protocols introduced at the R1 stage of a given release are designated as “Parent” signatures for a given release and cannot be disabled.

Within a major release, all protocols introduced post-R1 of a major release as part of any isa-aa.tim ISSU upgrade are by default **shutdown**. They must be enabled on a per-protocol basis (system-wide) to take effect.

When shutdown, post R1-introduced protocols do not change AA behavior (app-id, policy, statistics are as before the protocol introduction), for example, traffic maps to the parent protocol on which the new signature is based. In cases where there is more than one parent protocol, all traffic is mapped to a single, most-likely, parent protocol. For example if 80% of a new protocol has traffic mapping to unknown_tcp, and 20% mapping to another protocols, unknown_tcp would be used as parent.

Enabling/disabling of a new protocol takes affect for new flows only. The current status (enabled/shutdown) of a signature and the parent protocol is visible to an operator as part of retrieving protocol information through CLI/SNMP.

3.2.2.2.5 Supported Protocol Signatures

Protocol signatures are release independent and can be upgraded independently from the router’s software and without impacting router’s operations as part of an ISSU upgrade. A separate document outlines signatures supported for each signature software load (isa-aa.tim). New signature loads are distributed as part of the SR/ESS maintenance cycle. Traffic identified by new signatures will be mapped to an **Unknown** application until the AA policy configuration changes to make use of the newly introduced protocol signatures.

3.2.2.2.6 Application Groups

Application groups are defined as a container for multiple applications. The only application group created by default is **Unknown**. Any applications not assigned to a group are automatically assigned to the default **Unknown** group. Application groups are expected to be defined when a common policy on a set of applications is expected, yet per each application visibility in accounting is required. The application group name is a key match criteria within application QoS policy rules.

3.2.2.2.7 Charging Groups

Charging Groups allow usage accounting by application and/or app groups in a manner that does not affect app to app-group mapping. For example, AA app groups statistics for “Streaming Video” includes all streaming apps, independent of whether any specific application is 0-rated for charging. AA charging groups are used for charging related statistics.

As with app-groups, charging groups are defined under an AA policy context for an AA group or partition. Once defined, individual apps and app-groups can be associated with the desired charging group. The charging group name is a key match criteria within application QoS policy rules.

A default charging group can be specified for the AA policy to associate a charging group to any applications or app-groups that are not explicitly assigned to a charging group.

Charging groups are also assigned an export-id number for accounting export purposes.

If no export-id is assigned, that charging group cannot be added to the AA subscriber stats RADIUS export-type. Once a charging group index is referenced, it cannot be deleted without removing the reference.

3.2.2.2.8 Applications

The application context defines and assigns a description to the application names supported by the application filter entries, and assigns applications to application groups.

- Application name is a key match criteria within application QoS policy rules, which are applied to a subscribers IP traffic.
- Each application can be associated with one of the application groups provided by Application Assurance.

The Application Assurance system provides no pre-defined applications other than **Unknown**. Applications must be explicitly configured. Any protocols not assigned to an application are automatically assigned to the default **Unknown** application. Nokia provides sets of known-good application/app-group configurations upon request. Contact the technical support staff for further information.

The applications are used by Application Assurance to identify the type of IP traffic within the subscriber traffic.

The network operator can:

- Define unique applications.
- Associate applications with an application group. The application group must already be configured.

3.2.2.2.9 Application Filters

Application filters (app-filter) are provided as an indirection between protocols and applications to allow the addition of variable parameters (port number, IP addresses, and so on) into an application definition. An application filter is a numbered rule entry that defines the use of protocol signatures and other criteria to define an application. Multiple rules can be used to define what constitutes an application but each rule will map to only one application definition.

The system concept of application filters is analogous to IP filters. Match of a flow to multiple rules is possible and is resolved by picking the rule with the lowest entry number that matches. A flow will only ever be assigned to one application.

The following criteria can be assigned to an application filter rule entry:

- Unique entry ID number
- Application name
- Flow setup direction
- Server IP address (or server IP filter list)
- HTTP port (or HTTP port list) used by HTTP proxies
- Server port (or server port list)
- Protocol signature
- IP protocol number
- String matches against Layer 5+ protocol header fields (for example, a string expression against HTTP header fields)

The application must be pre-configured prior to using it in an app-filter. Once defined, the new application names can be referenced.

3.2.2.2.10 HTTP

HTTP Protocol

The Hyper-Text Transfer Protocol (HTTP) has become the most significant protocol used on the Internet and has expanded its role beyond web browsing with a large number of applications using HTTP for a variety of functions on both desktop and mobile devices.

Application Assurance provides the tools required by residential, mobile and business VPN service providers to accurately classify any web-based applications regardless of where the content is stored and how it is delivered. This is done by using either the default protocol signatures delivered with the AA ISA software or by defining string based signatures from the HTTP header information fields included in the HTTP request messages to further refine the detection.

HTTP Session Persistency

HTTP can use both non persistent connections and persistent connections. Non-persistent connection uses one TCP connection per HTTP request while persistent connection can reuse the same TCP connection for multiple HTTP request to the same server.

Nowadays most applications are using HTTP/1.1 and persistent connection but HTTP/1.0 and non-persistent connections remains on older software and mobile devices.

HTTP flows are classified in a particular application using the first HTTP request of the flow only by default. Optionally, the MS-ISA offers the flexibility to classify each HTTP request within the same flow independently using **http-match-all-request** feature.

HTTP Proxy Support

Application Assurance also supports traffic classification of HTTP between a subscriber and a web proxy. This feature is enabled by default, the ISA monitors and detects HTTP proxy flows automatically, each request within the same persistent connection to the proxy server is classified independently.

3.2.2.2.11 AA IP Prefix Lists

AA ISA allows the match section of session filters, AQPs entries and application filters to include matching against a configured IP filter list or lists. Each IP filter list (aka IP pools) can have up to 64 IP address entries with a configurable mask for each entry.

3.2.2.2.12 Shallow Flow Inspection

When application awareness is not required, but requires other AA value added functions (for example, TCP-O, DEM), significant performance can be gained by not performing pattern or behavior-based identification. A shallow inspection configuration option can disable AA Layer 7 classification to increase throughput performance for deployments that can operate using only AA Layer 3 and Layer 4 shallow flow inspection. This configuration disables all signature-based flow inspection. This configuration can be used with TCP optimization, Dynamic Experience Management, Layer 3 and Layer 4 application filter classification, and Dynamic Experience Management.

3.2.2.3 Statistics and Accounting

Application Assurance statistics provide the operator with information to understand application usage within a network node.

Application Assurance XML record accounting aggregates the flow information into per application group, per application, per protocol reports on volume usage during the last accounting interval. This information is then sent to a statistics collector element for network wide correlation and aggregation into customized graphical usage reports. Application Assurance uses and benefits from the rich 7750 SR or 7450 ESS accounting infrastructure and the functionality it provides to control accounting policy details.

The following types of accounting volume records are generated and can be collected:

- Per ISA group and partition record for each configured application group
- Per ISA group and partition record for each configured application
- Per ISA group and partition record for each configured protocol
- Per each AA subscriber record with operator-configurable field content using custom AA records for operator-selected subset of protocols, applications and application groups

- Per AA subscriber per each configured application record (special study mode)
- Per AA subscriber per each supported protocol record (special study mode)
- Per ISA AA-performance record, containing information about the traffic and resources of each ISA
- Per AA partition stats record for counts of traffic by Layer 3 protocol used to transport L4 protocols. This includes TCP, UDP and NonTcpUdp carried by IPv4, IPv6, DS_Lite, 6to4/6RD, GTP, and Teredo protocols

Application Assurance supports RADIUS accounting export of per AA subscriber charging group statistics.

Each AA group:partition can be configured for AA subscribers stats export by referencing both an accounting policy (for XML statistics) and/or a RADIUS accounting policy. In order to determine how to export various counters for subscriber AA statistics, an export-using keyword is used when enabling AA subscriber level stats export to specify the export method to be used for each, whether accounting-policy or radius-accounting-policy and/or diameter-based usage monitoring.

Per AA flow statistics are provided as described in the cflowd section.

Refer to the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR System Management Guide* for information on general accounting functionality.

3.2.2.3.1 Per-AA Subscriber Special Study

The system can be configured to generate statistical records for each application and protocol that the system identifies for specific AA subscribers. These capabilities are disabled by default but can be enabled for a subset of AA subscribers to allow detailed monitoring of those AA subscriber's traffic.

Per-AA subscriber per-application and per-AA subscriber per-protocol records are enabled by assigning individual AA subscribers to special study service lists. The system and ISA group limit the number of AA subscribers in this mode to constrain the volume of stats generated. When an AA subscriber is in a special study mode, one record for every application and/or one record for every protocol that are configured in the system are generated for that subscriber. For example, if 500 applications are configured and 200 protocols are identified, 700 records per AA subscriber will be generated, if the AA subscriber is listed in both the per-aa-sub-application and per-aa-sub protocol lists.

3.2.2.3.2 System Aspects

Application Assurance uses the existing redundant accounting and logging capability of the 7750 SR and 7450 ESS for sending application and subscriber usage information, in-band or out-of-band. Application Assurance statistics are stored using compressed XML format with other system and subscriber statistics in compact flash modules on the redundant SF/CPMs. A large volume of statistics can be expected under scaled scenarios when per-AA subscriber statistics/accounting is enabled.

AA accounting and statistics can be deployed as part of other system functionality as long as the system's function is compatible with AA accounting or as long as the system-level statistics can become application-aware due to, for example, AA ISA-based classification. An example of this feature interaction includes volume and time-based accounting where AA-based classification into IOM queues with volume and time accounting enabled can, for instance, provide different quota/credit management for off-net and on-net traffic or white/grey applications.

3.2.2.3.3 Application Assurance XML Volume Statistics and Accounting

Application Assurance is configured to collect and report on the following statistics when at least one AA ISA is active. The default Application Assurance statistics interval is 15 minutes.

Statistics to be exported from the node are aggregated into accounting records, which must be enabled in order to be sent. By default, no records are sent until enabled. Each record template type is enabled individually to control volume of statistics to the desired level of interest. Only non-zero records are written to the accounting files for all AA subscriber based statistics to reduce the volume of data.

The operator can further select a subset of the fields to be included in per-AA subscriber records and whether to send records if no traffic was present for a given protocol or application, for example, sending only changed records.

Each record generated contains the record fields as described in [Table 11](#). The header row represents the record type.

Table 11 Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA Subscriber Custom	AA Subscriber Special Study per App	AA Subscriber Special Study Protocol	XML Name
Application Group	Name	X						data name
Application	Name		X			X		data name
Protocol	Name			X			X	data name
Aggregation Type ID	ID (can be protocol, application, charging group or application group record)				X			agg-typ e-name
# Active Subscribers	# of subscribers who had a flow of this category during this interval	X	X	X				nsub
# allowed flows from-sub	# of new flows that were identified and allowed	X	X	X	X	X	X	sfa
# allowed flows to-sub	As above in opposite direction	X	X	X	X	X	X	nfa
# denied flows from-sub	the # of new flows that were identified and denied	X	X	X	X	X	X	sfd
# denied flows to-sub	As above in opposite direction	X	X	X	X	X	X	nfd
# Active flows from-sub	# of flows that were either: closed, opened & closed, opened, or continued during this interval	X	X	X	X	X	X	saf
# active flows to-sub	As above, in opposite direction	X	X	X	X	X	X	naf
Total packets from-sub		X	X	X	X	X	X	spa

Table 11 Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA Subscriber Custom	AA Subscriber Special Study per App	AA Subscriber Special Study Protocol	XML Name
Total packets to-sub		X	X	X	X	X	X	npa
Total bytes from-sub		X	X	X	X	X	X	sba
Total bytes to-sub		X	X	X	X	X	X	nba
Total discard packets from-sub		X	X	X	X	X	X	spd
Total short flows	Number of flows with duration <= 30 seconds that completed up to the end of this interval	X	X	X	X	X	X	sdf
Total medium flows	Number of flows with duration <= 180 seconds that completed up to the end of this interval	X	X	X	X	X	X	mdf
Total long flows	Number of flows with duration > 180 seconds that completed up to the end of this interval	X	X	X	X	X	X	ldf
Total discard packets to-sub		X	X	X	X	X	X	npd
Total discard bytes from-sub		X	X	X	X	X	X	sbd
Total discard bytes to-sub		X	X	X	X	X	X	nbd
Total flows completed	# of to- and from-subscriber flows that have been completed up to the reported interval.	X	X	X	X	X	X	tfc

Table 11 Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA Subscriber Custom	AA Subscriber Special Study per App	AA Subscriber Special Study Protocol	XML Name
Total flow duration	Duration, in seconds, of all flows that have been completed up to the reported interval.	X	X	X	X	X	X	tfd
From AA Sub: Maximum throughput byte count	Maximum of all total byte counts recorded for throughput intervals within this accounting interval for traffic originated by AA subscriber for a given application/app-group. AA ISA discarded traffic is not included.				X			sbm
From AA Sub: Packet count corresponding to the max. throughput byte count interval.	Packet count for the throughput interval with the maximum byte count value for traffic originated by AA subscriber for the application/app-group. AA ISA discarded traffic is not included.				X			spm
To AA Sub: Max throughput time slot index	UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.				X			smt
From AA Sub: Forwarding-class	Observed forwarding-class bits.	X	X	X	X	X	X	sfc
To AA Sub: Forwarding-class	Observed forwarding-class bits.	X	X	X	X	X	X	nfc

Table 11 Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA Subscriber Custom	AA Subscriber Special Study per App	AA Subscriber Special Study Protocol	XML Name
To AA Sub: Maximum throughput byte count	Maximum of all total byte counts recorded for throughput intervals within this accounting interval for traffic originated from Network towards AA subscriber for a given application/app-group. AA ISA discarded traffic is not included.				X			nbm
To AA Sub: Packet count corresponding to the max. Throughput byte count interval.	Packet count for the throughput interval with the maximum byte count value for traffic originated from network towards AA subscriber for a given application / app-group. AA ISA discarded traffic is not included.				X			npm
From AA Sub: Max throughput time slot index	UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.				X			nmt
From AA Sub: Forwarding-class	Observed forwarding-class bits.	X	X	X	X	X	X	X

Table 11 Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA Subscriber Custom	AA Subscriber Special Study per App	AA Subscriber Special Study Protocol	XML Name
From AA Sub: Maximum throughput byte count	Maximum of all total byte counts recorded for throughput intervals within this accounting interval for all traffic originated by AA subscriber. AA ISA discarded traffic is not included.				X			sbm
From AA Sub: Packet count corresponding to the max. Throughput byte count interval.	Packet count for the throughput interval with the maximum byte count value for traffic originated by AA subscriber. AA ISA discarded traffic is not included.				X			spm
From AA Sub: Max throughput time slot index	UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.				X			smt
To AA Sub: Maximum throughput byte count	Maximum of all total byte counts recorded for throughput intervals within this accounting interval for traffic originated from network towards AA subscriber. AA ISA discarded traffic is not included.				X			nbm

Table 11 Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA Subscriber Custom	AA Subscriber Special Study per App	AA Subscriber Special Study Protocol	XML Name
To AA Sub: Packet count corresponding to the max. Throughput Byte Count interval.	Packet count for the throughput interval with the maximum byte count value for traffic originated from network towards AA subscriber. AA ISA discarded traffic is not included.				X			npm
To AA Sub: Max throughput time slot index	UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.				X			nmt
Forwarding Class		X						fc
App-Profile	AA subscriber application profile name				X			app-pro file
App-Service-Options	List of the app-service-options characteristics and values per AA subscriber				X			app-ser vice-op tion

The records are generated per ISA group and partition, with an ISA group identified by the group ID (XML field name “aaGroup”), partition identified by the partition ID (XML field name “aaPart name” and per AA subscriber (if applicable) with the AA subscriber identified by the ESM, DSM, or transit subscriber name, SAP ID (XML field name “subscriber name”, “sap name” or “spoke SDP ID” respectively).

The date, time, and system ID for the records will be visible as part of the existing accounting log capability, thus does not need to be contained inside the Application Assurance records themselves.

The Forwarding Class is included in AA XML records as generally a VPN interconnection SLA is a combination of Bandwidth connection at the site level and Forwarding Class to transport the traffic over the MPLS network, by mapping the end-customer DSCP or 802.1P traffic value into a given FC.

AA accounting stats of the application/application-group volume usage per forwarding class shows the exact volume of each application at the per FC level and better ties the AA reports to the VPN services and SLA.

This can also identify key applications using a non-optimal FC over a given VPN/Site and allow the option for AA to remark these into a higher traffic class, with reporting per FC to show resulting use.

3.2.2.3.4 AA Partition Traffic Type Statistics

AA-ISA provides, at the AA partition level, traffic volume visibility of the Layer 3 protocols used to transport the different Layer 4 protocols. These include a traffic volume break down of TCP, UDP and Non-TCP-UDP carried by IPv4 and IPv6, DS_Lite, 6to4/6RD, GTP, and Teredo protocols.

Traffic-type statistics are broken down by "family" and "protocol":

- Family: IPv4, IPv6, DS-Lite, 6RD/6to4, Teredo, GTP (IP v4/v6 in v4/v6)
- Protocol: TCP, UDP, Other

Therefore, AA-ISA traffic type record provides a collection of 15 sets of traffic volume (bytes) statistics figures, as follows:

- IPv4 — TCP, UDP, Other
- IPv6 — TCP, UDP, Other
- DS-Lite — TCP, UDP, Other (IPv4 tunneled inside IPv6)
- 6to4/6RD — TCP, UDP, Other (IPv6 tunneled inside IPv4)
- Teredo — TCP, UDP, Other (IPv6 tunneled inside IPv4 and UDP)
- v4inv4GTP — TCP, UDP, Other (IPv4 tunneled inside IPv4 GTP)
- v4inv6GTP — TCP, UDP, Other (IPv4 tunneled inside IPv6 GTP)
- v6inv4GTP — TCP, UDP, Other (IPv6 tunneled inside IPv4 GTP)
- v6inv6GTP — TCP, UDP, Other (IPv6 tunneled inside IPv6 GTP)

These statistics are always counted. There is no configuration required to enable/disable tracking. However, the operator has the option to enable/disable export of these statistics via XML.

[Table 12](#) lists the statistic record fields per AA partition.

Table 12 **AA-Partition Traffic Type Statistics**

Record name	Type	Description
nsa	cumulative	sessions admitted (to-sub)
ssa	cumulative	sessions admitted (from-sub)
nca	cumulative	chunks admitted (to-sub)
sca	cumulative	chunks admitted (from-sub)
sba	cumulative	octets admitted (from-sub)
spa	cumulative	packets admitted (from-sub)
sbd	cumulative	octets denied (from-sub)
spd	cumulative	packets denied (from-sub)
nba	cumulative	octets admitted (to-sub)
npa	cumulative	packets admitted (to-sub)
nbd	cumulative	octets denied (to-sub)
npd	cumulative	packets denied (to-sub)
sfa	cumulative	flows admitted (from-sub)
sfd	cumulative	flows denied (from-sub)
saf	intervalized	active flows (from-sub)
nfa	cumulative	flows admitted (to-sub)
nfd	cumulative	flows denied (to-sub)
naf	intervalized	active flows (to-sub)
tfc	cumulative	total terminated flows
tfd	cumulative	total terminated flow duration
sdf	cumulative	short duration flows
mdf	cumulative	medium duration flows
ldf	cumulative	long duration flows
sfc	cumulative	forwarding-class bitmap (from-sub)
nfc	cumulative	forwarding-class bitmap (to-sub)
tet	cumulative	num of subscribers tethered

Table 12 AA-Partition Traffic Type Statistics (Continued)

Record name	Type	Description
nte	cumulative	num of subscribers not tethered

3.2.2.3.5 Configurable AA Subscriber Statistics Collection

Existing average volume statistics collected over an accounting interval are extended to provide the maximum volume (bytes/packets) recorded for a throughput measurement period (5 minutes) within an accounting interval. These additional statistics improve accuracy for the access-pipe right-sizing service.

Maximum throughput statistics can be enabled for the selected applications and/or application groups enabled for custom per AA statistics. In addition, the operator can enable (disabled by default) per AA subscriber “Max-throughput” statistics for total (/aggregate) subscriber traffic, independent of defined applications/application-groups.

Maximum throughput statistics records are allocated from the 2048K records available for use for per subscriber records.

Maximum throughput statistics are not provided for the protocols enabled for custom per AA statistics.

3.2.2.3.6 AA-Performance Record for ISA Load

The AA-performance statistics record provides visibility of ISA loading related statistics to allow operational monitoring and planning of ISA overload:

1. Provides end of reporting interval snapshot of current values of the parameters listed in below into a per AA ISA Planning record. “Current” is the value of a counter at the end of the reporting interval, for rate based values this is the ~10sec short term current rate used in CLI statistics.
2. Provides time-based averages during record interval of the above values: Average(I)
3. Provides peak values of the above values in the reporting interval: Peak(I)

The 5670 RAM provides further analysis and thresholding triggers based on these ISA statistics, suitable for long-range planning trends such as average number of subs or peak numbers of flows.

The node per-ISA planning record values are cleared on accounting read (per all accounting records). Not reading the records means that the average and peak values are the values for the last reporting interval. The time last read is indicated in the record.

The AA performance planning record are listed in [Table 13](#):

Table 13 AA Performance Planning Record Fields

Parameter	Current	Average	Peak
ISA ID			
active subs (with flows)	# subs	# subs	# subs
downloaded subs	# subs	# subs	# subs
ISA AA sub stats resource allocation	# stats records		
ISA capacity cost	sum of cost of active AA subs		
ISA Transit Subs	# subs		
diverted traffic	(packets, octets)		
entered ISA	(packets, octets)		
policy discards in ISA	(packets, octets)		
congestion discards in ISA	(packets, octets)		
error discards in ISA	(packets, octets)		
policy bypass errors	(packets, octets)		
returned traffic	(packets, octets)		
Volume cflowd			
Records reported	# records		
Reports dropped	# records		
Packets sent	# packets		
Comprehensive cflowd			
Records reported	# records		
Reports dropped	# records		
Packets sent	# packets		
TCP performance cflowd			
Flows not allocated	#flows		

Table 13 AA Performance Planning Record Fields (Continued)

Parameter	Current	Average	Peak
Records reported	# records		
Reports dropped	# records		
Packets sent	# packets		
RTP performance cflowd			
Flows not allocated	#flows		
Records reported	# records		
Reports dropped	# records		
Packets sent	# packets		
Number of synchronization sources that had to be aborted	#SSRC aborted		
URL-filter			
url-filter http-requests sent	# http-requests		
url-filter - http-request errors	# http-requests		
url-filter - http-requests dropped	# http-requests		
url-filter - http-requests permitted	# http-requests		
url-filter - http-requests redirected	# http-requests		
url-filter - http-requests blocked	# http-requests		
url-filter - http default actions	# http-requests		
url-filter - subscriber count	# subs		
url-list permits	url local list #http requests allowed		
url-list redirects	url local list #http requests redirected		
url-list drops	url local list #http requests dropped		
ICAP			
icap requests	# messages		
icap request errors	# messages		
icap permits	# messages		

Table 13 AA Performance Planning Record Fields (Continued)

Parameter	Current	Average	Peak
icap redirects	# messages		
icap drops	# messages		
icap late responses	# messages		
icap average rtt	seconds		
icap tcp connections	# icap sessions		

The AA performance records are listed [Table 14](#):

Table 14 AA Performance Records

Record Name	Type	Description	MIB Object (if applicable)
tmo	Cumulative	Octets to MDA	tmnxBsxGrpStatusOctsToMda
tmp	Cumulative	Packets to MDA	tmnxBsxGrpStatusPktsToMda
fmo	Cumulative	Octets from MDA	tmnxBsxGrpStatusOctsFromMda
fmp	Cumulative	Packets from MDA	tmnxBsxGrpStatusPktsFromMda
dco	Cumulative	Octets discarded due to congestion in MDA	tmnxBsxGrpStatusOctsDisCongMda
dcp	Cumulative	Packets discarded due to congestion in MDA	tmnxBsxGrpStatusPktsDisCongMda
dpo	Cumulative	Octets discarded due to policy in MDA	tmnxBsxGrpStatusOctsDiscPolicy
dpp	Cumulative	Packets discarded due to policy in MDA	tmnxBsxGrpStatusPktsDiscPolicy
deo	Cumulative	Octets discarded due to error	tmnxBsxGrpStatusOctsDiscErrors
dep	Cumulative	Packets discarded due to error	tmnxBsxGrpStatusPktsDiscEnors
pbo	Cumulative	Octets policy bypass	tmnxBsxGrpStatusOctsPolicyByyps
pbp	Cumulative	Packets policy bypass	tmnxBsxGrpStatusPktsPolicyByyps
nfl	Cumulative	Number of flows	tmnxBsxGrpStatusFlows
caf	Intervalized	Current active flows	tmnxBsxGrpStatusFlowsCurrent
aaf	Intervalized	Average active flows	tmnxBsxGrpStatusFlowsAverage
paf	Intervalized	Peak active flows	tmnxBsxGrpStatusFlowsPeak

Table 14 AA Performance Records (Continued)

Record Name	Type	Description	MIB Object (if applicable)
cfr	Intervalized	Current flow setup rate	tmnxBsxGrpStatusFlowSetupRate
afr	Intervalized	Average flow setup rate	tmnxBsxGrpStatusFlowSetupRateAvg
pfr	Intervalized	Peak flow setup rate	tmnxBsxGrpStatusFlowSetupRatePk
ctr	Intervalized	Current traffic rate	tmnxBsxGrpStatusTrafficRate
atr	Intervalized	Average traffic rate	tmnxBsxGrpStatusTrafficRateAvg
ptr	Intervalized	Peak traffic rate	tmnxBsxGrpStatusTrafficRatePeak
cpr	Intervalized	Current packet rate	tmnxBsxCflowdStatusPktRateCurr
apr	Intervalized	Average packet rate	tmnxBsxGrpStatusPacketRateAvg
ppr	Intervalized	Peak packet rate	tmnxBsxGrpStatusPacketRatePeak
cas	Intervalized	Current active subscribers (with flows)	tmnxBsxGrpStatusSubsCurrent
aas	Intervalized	Average active subscribers (with flows)	tmnxBsxGrpStatusSubsAverage
pas	Intervalized	Peak active subscribers (with flows)	tmnxBsxGrpStatusSubsPeak
cds	Intervalized	Current diverted subscribers	tmnxBsxGrpStatusSubsDiverted
ads	Intervalized	Average diverted subscribers	tmnxBsxGrpStatusSubsDivertedAvg
pds	Intervalized	Peak diverted subscribers	tmnxBsxGrpStatusSubsDivertedPk
rfi	Intervalized	Flows in use	tmnxBsxGrpStatusFlowResInUse
rcc	Cumulative	ISA capacity cost	tmnxBsxGrpMdaCapacityCost
rss	Cumulative	Subscriber statistics count	tmnxBsxGrpMdaStatsResourceCount
rti	Cumulative	Transit IP address count	tmnxBsxGrpMdaTransitipAdrrs
rtp4	Cumulative	Transit prefix v4 address count	tmnxBsxGrpMdaTransPrefV4Entr
rtp6	Cumulative	Transit prefix v6 address count	tmnxBsxGrpMdaTransPrefV6Entr
rtp6r	Cumulative	Transit prefix v6 remote address count	tmnxBsxGrpMdaTransPrefV6RemEntr
srs	Cumulative	Seen IP, requests sent	tmnxBsxGrpStatusHCSeenIpReqSenp

Table 14 AA Performance Records (Continued)

Record Name	Type	Description	MIB Object (if applicable)
srd	Cumulative	Seen IP, requests dropped	tmnxBsxGrpStatusHCSeenIpReqDrop
tsc	Cumulative	Total subscribers created	tmnxBsxGrpStatusHCSubsCreated
tsd	Cumulative	Total subscribers deleted	tmnxBsxGrpStatusHCSubsDeleted
tsm	Cumulative	Total subscribers modified	tmnxBsxGrpStatusHCSubsModified
vrr	Cumulative	Volume cflowd, records reported	tmnxBsxCflowdStatusRecReported
vrđ	Cumulative	Volume cflowd, records dropped	tmnxBsxCflowdStatusRecDropped
vps	Cumulative	Volume cflowd, packets sent	tmnxBsxCflowdStatusPktsSent
crr	Cumulative	Comprehensive cflowd, records reported	tmnxBsxCflowdStatusRecReported
crđ	Cumulative	Comprehensive cflowd, records dropped	tmnxBsxCflowdStatusRecDropped
cps	Cumulative	Comprehensive cflowd, packets sent	tmnxBsxCflowdStatusPktsSent
trr	Cumulative	TCP performance cflowd, records reported	tmnxBsxCflowdStatusRecReported
trđ	Cumulative	TCP performance cflowd, records dropped	tmnxBsxCflowdStatusRecDropped
tps	Cumulative	TCP performance cflowd, packets sent	tmnxBsxCflowdStatusPktsSent
tfn	Cumulative	TCP performance cflowd, flows but no cflowd resources available	tmnxBsxCflowdStatusFlowsNoRes
rrr	Cumulative	RTP performance cflowd, records reported	tmnxBsxCflowdStatusRecReported
rrđ	Cumulative	RTP performance cflowd, records dropped	tmnxBsxCflowdStatusRecDropped
rps	Cumulative	RTP performance cflowd, packets sent	tmnxBsxCflowdStatusPktsSent
rfn	Cumulative	RTP performance cflowd, flows but no cflowd resources available	tmnxBsxCflowdStatusFlowsNoRes
rsr	Cumulative	RTP performance cflowd, number of synchronization sources that had to be aborted	tmnxBsxCflowdStatusHCUSupSSRCSt

Table 14 AA Performance Records (Continued)

Record Name	Type	Description	MIB Object (if applicable)
res	Cumulative	srflow collector, records sent The new data name is the collector address and port inserted into the XML record.	tmnxBsxCflowdCollStatRecSent
hrs	Cumulative	URL filter, HTTP requests sent	tmnxBsxUrlFiltrStatsHttpRequests
hre	Cumulative	URL filter, HTTP request errors	tmnxBsxUrlFiltrStatsHttpReqErrors
hri	Cumulative	URL filter, HTTP requests dropped	n/a
hrp	Cumulative	URL filter, HTTP requests permitted	tmnxBsxUrlFiltrStatsHttpRespAllow
hrr	Cumulative	URL filter, HTTP requests redirected	tmnxBsxUrlFiltrStatsHttpRespRedir
hrb	Cumulative	URL filter, HTTP requests blocked	tmnxBsxUrlFiltrStatsHttpRespBlock
hda	Cumulative	URL filter, HTTP default actions	tmnxBsxUrlFiltrStatsHttpRespDef
irs	Cumulative	ICAP, icap requests	tmnxBsxlcapServerStatsRequests
ire	Cumulative	ICAP, icap request errors	tmnxBsxlcapServerStatsReqErrors
irp	Cumulative	ICAP, icap permits	tmnxBsxlcapServerStatsReapAllow
irr	Cumulative	ICAP, icap redirects	tmnxBsxlcapServerStatsRespRedir
ird	Cumulative	ICAP, icap drops	tmnxBsxlcapServerStatsRespBlock
ilr	Cumulative	ICAP, icap late responses	tmnxBsxUrlFiltrStatsIcapLateResp
irt	Cumulative	ICAP, icap average rtt	tmnxBsxlcapServerStatsRoundTrip
itc	Cumulative	ICAP, icap TCP connections	tmnxBsxlcapServerStatsConnEst
ifs	Cumulative	URL filter, subscriber count	n/a
rtp4r	Cumulative	Transit prefix, v4 remote address count	tmnxBsxGrpMdaTransPrefV4RemEntr
lrp	Cumulative	URL list permits	tmnxBsxUrlFiltrStatsHttpRespAllow
lrr	Cumulative	URL list redirects	tmnxBsxUrlFiltrStatsHttpRespRedir
lrd	Cumulative	URL list drops	tmnxBsxUrlFiltrStatsHttpRespBlock
fra	Intervalized	Flow resources average	tmnxBsxGrpStatusFlowResAvg
frp	Intervalized	Flow resources peak	tmnxBsxGrpStatusFlowResPeak
frs	Intervalized	Flow resources alarm state	tmnxBsxGrpStatusFlowResState

Table 14 AA Performance Records (Continued)

Record Name	Type	Description	MIB Object (if applicable)
fre	Intervalized	Flow resources alarm count	tmnxBsxGrpStatusFlowResRsdCount
frtm	Intervalized	Flow resources alarm time	tmnxBsxGrpStatusFlowResRaisdTime
feo	Cumulative	Flow exhaust octets	tmnxBsxGrpStatusFlwResCtThruOcts
fep	Cumulative	Flow exhaust packets	tmnxBsxGrpStatusFlwResCtThruPkts
fss	Intervalized	Flow setup rate alarm state	tmnxBsxGrpStatusFlowSetupState
fse	Intervalized	Flow setup rate alarm count	tmnxBsxGrpStatusFlowSetupRsdCnt
fstm	Intervalized	Flow setup rate alarm time	tmnxBsxGrpStatusFlowSetupRsdTime
brs	Intervalized	Bitrate alarm state	tmnxBsxGrpStatusBitRateState
bre	Intervalized	Bitrate alarm count	tmnxBsxGrpStatusBitRateRsdCount
brtm	Intervalized	Bitrate alarm time	tmnxBsxGrpStatusBitRateRsdTime
prs	Intervalized	Packet rate alarm state	tmnxBsxGrpStatusPktRateState
pre	Intervalized	Packet rate alarm count	tmnxBsxGrpStatusPktRateRsdCount
prtm	Intervalized	Packet rate alarm time	tmnxBsxGrpStatusPktRateRaisedTime
ocs	Intervalized	Overload alarm state	tmnxBsxGrpStatusWaSBfFmSubState tmnxBsxGrpStatusWaSBfToSubState
oce	Intervalized	Overload alarm count	tmnxBsxGrpStatusWaSBfFmSubRsdCnt tmnxBsxGrpStatusWaSBfToSubRsdCnt
octm	Intervalized	Overload alarm time	tmnxBsxGrpStatusWaSBfFmSubRsdTm tmnxBsxGrpStatusWaSBfToSubRsdTm
oco	Cumulative	Overload cut-through octets	tmnxBsxGrpStatusOvrldCtThruOcts
ocp	Cumulative	Overload cut-through packets	tmnxBsxGrpStatusOvrldCtThruPkls
mcpua	Intervalized	Management CPU average	tmnxBsxGrpStatusMgmIcPpuAvg
mcpup	Intervalized	Management CPU peak	tmnxBsxGrpStatusMgmtCpuPeak
dcpua	Intervalized	DP CPU average	tmnxBsxGrpStatusDatapathCpuAvg
dcpup	Intervalized	DP CPU peak	tmnxBsxGrpStatusDatapathCpuPeak
dcpus	Intervalized	DP CPU alarm state	tmnxBsxGrpStatusDatapathCpuState
dcpue	Intervalized	DP CPU alarm count	tmnxBsxGrpStatusDatapathCpuRsdCt

Table 14 AA Performance Records (Continued)

Record Name	Type	Description	MIB Object (if applicable)
dcpum	Intervalized	DP CPU alarm time	tmnxBsxGrpStatusDatapathCpuRSDTm

3.2.2.3.7 AA Partition Traffic Type Statistics

AA ISA provides, at the AA partition level, traffic volume visibility of the Layer 3 protocols used to transport the different Layer 4 protocols. These include a traffic volume break down of TCP, UDP and Non-TCP-UDP carried by IPv4, IPv6, DS_Lite, 6to4/6RD and Teredo protocols.

Traffic-type statistics are broken down by family and protocol:

- Family: IPv4, IPv6, DS-Lite, 6RD/6to4, Teredo
- Protocol: TCP, UDP, Other

Therefore, AA ISA traffic type record provides a collection of 15 sets of traffic volume (Bytes) statistics figures as follows:

- IPv4 — TCP, UDP, Other
- IPv6 — TCP, UDP, Other
- DS-Lite — TCP, UDP, Other (IPv4 tunneled inside IPv6)
- 6to4/6RD — TCP, UDP, Other (IPv6 tunneled inside IPv4)
- Teredo — TCP, UDP, Other (IPv6 tunneled inside IPv4 and UDP)
- v4inv4GTP — TCP, UDP, Other (IPv4 tunneled inside IPv4 GTP)
- v4inv6GTP — TCP, UDP, Other (IPv4 tunneled inside IPv6 GTP)
- v6inv4GTP — TCP, UDP, Other (IPv6 tunneled inside IPv4 GTP)
- v6inv6GTP — TCP, UDP, Other (IPv6 tunneled inside IPv6 GTP)

These statistics are always counted. There is no configuration required to enable/disable tracking. However, the operator has the option to enable/disable export of these statistics via XML.

Table 15 Per AA Partition Stats Record Fields

Record Name	Type	Description	MIB object (if applicable)
sba	cumulative	octets admitted (from-sub)	tmnxBsxTrafStatOctsAdmFmSb
spa	cumulative	packets admitted (from-sub)	tmnxBsxTrafStatPktsAdmFmSb

Table 15 Per AA Partition Stats Record Fields (Continued)

Record Name	Type	Description	MIB object (if applicable)
sbd	cumulative	octets denied (from-sub)	tmnxBsxTrafStatOctsDnyFmSb
spd	cumulative	packets denied (from-sub)	tmnxBsxTrafStatPktsDnyFmSb
nba	cumulative	octets admitted (to-sub)	tmnxBsxTrafStatOctsAdmToSb
npa	cumulative	packets admitted (to-sub)	tmnxBsxTrafStatPktsAdmToSb
nbd	cumulative	octets denied (to-sub)	tmnxBsxTrafStatOctsDnyToSb
npd	cumulative	packets denied (to-sub)	tmnxBsxTrafStatPktsDnyToSb
sfa	cumulative	flows admitted (from-sub)	tmnxBsxTrafStatFlwsAdmFmSb
sfd	cumulative	flows denied (from-sub)	tmnxBsxTrafStatFlwsDnyFmSb
saf	intervalized	active flows (from-sub)	tmnxBsxTrafStatActFlwsFmSb
nfa	intervalized	active flows (to-sub)	tmnxBsxTrafStatActFlwsToSb
nfd	cumulative	flows denied (to-sub)	tmnxBsxTrafStatFlwsDnyToSb
naf	intervalized	active flows (from-sub)	tmnxBsxTrafStatActFlwsFmSb
tfc	cumulative	total terminated flows	tmnxBsxTrafStatTermFlws
tfd	cumulative	total terminated flow duration	tmnxBsxTrafStatTermFlwDur
sdf	cumulative	short duration flows	tmnxBsxTrafStatShrtDurFlws
mdf	cumulative	medium duration flows	tmnxBsxTrafStatMedDurFlws
ldf	cumulative	long duration flows	tmnxBsxTrafStatLngDurFlws
sfc	cumulative	forwarding-class bitmap (from-sub)	N/A
nfc	cumulative	forwarding-class bitmap (to-sub)	N/A

3.2.2.3.8 AA Partition Admit–Deny Statistics

At the partition level, AA provides counters that capture events associated with various application QoS policy (AQP) actions related to packet and/or flow drops and admit actions. These statistics are exported via XML using configured accounting policies.

When enabled at the partition level, AA reports the statistics listed below.

- AQP Drop Actions — drop and admit counters for “to” and “from” subscriber directions are provided for the following AQP commands:
 - **error-drop**
 - **overload-drop**
 - TCP validate policy drop
 - **fragment-drop all**
 - **fragment-drop out-of-order**
 - **gtp-sanity-drop**
- Flow policers — drop and admit event counters for both “to” and “from” subscriber directions for flow count and flow rate policers, operating at the system and/or subscriber level.
- Hit counters — counters for “to” and “from” subscriber directions are provided for:
 - GTP filters for each hit on entry of a GTP filter as well as drops related to the GTP maximum size and default action. The GTP maximum size and SCTP PPID range action hit counts only report drop statistics and not permit statistics.
 - SCTP filters for each hit on entry of an SCTP filter as well as hits on PPID range and default actions.
 - Session filters for each hit on entry within a session filter and default action.

[Table 12](#) lists the record names used for AA admit-deny statistics.

Admit–Deny Threshold Crossing Alerts

AA supports Threshold Crossing Alerts (TCAs) that can be configured against any of the statistics counters listed in [AA Partition Admit–Deny Statistics](#). A high watermark and a low watermark can be configured for each counter. Once the counter value reaches the configured high watermark within any 60 second interval, an event (Trap is set) is raised. The event is cleared if the counter goes below the low watermark threshold in any subsequent 60 seconds interval.

3.2.2.3.9 RADIUS Accounting AA Records

AA RADIUS accounting provides per-level, AA subscriber charging group statistics as well as application-group (AG) and application statistics as part of the RADIUS accounting infrastructure. The primary use of this is to enhance RADIUS accounting with AA information useful for usage-based billing plans, providing flexibility to charge and rate application content using IP subnets, HTTP URLs, SIP URIs, and other AA-identified applications.

The system can export AA accounting statistics using accounting policy records exported with RADIUS accounting. For non-DSM subscribers, AA RADIUS accounting is AA subscriber ID-based, where the AA subscriber context IPv4 and IPv6 host addresses for the sub are not reflected in RADIUS accounting. For DSM subscribers, the AA counters are included in the BB RADIUS session which is based on the BB sub and reflects the BB host context.

AA RADIUS accounting is implemented using ALU Vendor Specific Attributes (VSAs). This provides all charging group counters for a given subscriber to be exported with a common accounting session ID. The following statistics are included in each record. Accounting values are for forwarded packets:

- input octets (from-sub)
- input packets (from-sub)
- output octets (to-sub)
- output packets (to-sub)

AA RADIUS accounting is supported for ESM, DSM, transit, and SAP or spoke SDP AA-subtypes. RADIUS accounting is used to export AA charging group, app-group, and application values according to the RADIUS accounting policy interval. Charging group statistics are exported in RADIUS accounting independent of application groups (either or both can be enabled).

For DSM subscribers, RADIUS accounting records can be configured to be exported under the Broadband ISA (BB) configuration. In this case, the AA charging group, application group, application and sub aggregate (total AA traffic) counters are passed to the BB ISA for export to the BB RADIUS accounting sessions.

3.2.2.3.10 AA GX Based Usage Monitoring

Using 3GPP (third generation Partnership Project) diameter (Gx) functionality, AA ISA upon receiving requests from Policy and Charging Rules Function (PCRF), can monitor application usage at the subscriber's level and report back to PCRF whenever the usage exceeds the thresholds set by the PCRF.

Usage-monitoring can be used by operators to report to PCRF when:

- AA ISA detects the start of a subscriber application (by setting usage threshold to be very low)
- A Pre-set usage volume per subscriber application is exceeded.

AA can monitor subscriber's traffic for any defined:

- Application,
- Application group, and/or
- Charging group.

AA ISA Gx-based usage monitoring is restricted to AA ESM and transit AA subscribers' type therefore it is only supported on 7750 SR.

The AA ISA Gx usage monitoring feature builds on 3GPP Release 11 defined Application Detection and Control (ADC) Gx attributes. In addition, AA ISA is compliant with 3GPP Release 12, whereby the ADC rule functionality is integrated in the PCC rules.

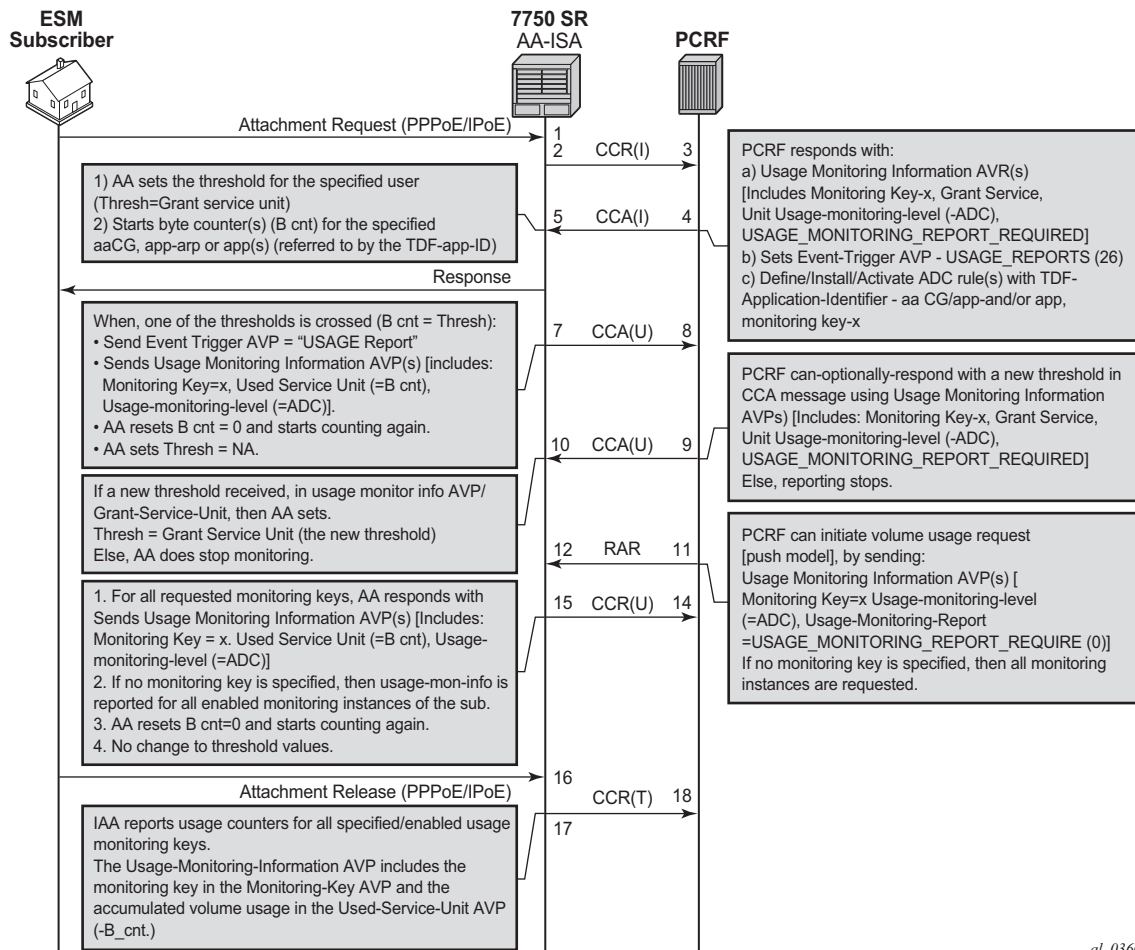
AA ISA reports accumulated usage when:

- A usage threshold is reached
- The PCRF explicitly disables usage monitoring
- The PCRF requests for a report
- When the ADC or PCC rule associated with the monitoring instance is removed or deactivated
- When a session is terminated

An AA defined application, application group and/or charging group is automatically allowed to be referenced by a an ADC rule for the purpose of usage monitoring only if:

- a. It is already selected for either XML or Radius per subscriber accounting or
- b. It is explicitly enabled by the operator for per sub statistics collection and
- c. Usage monitoring is enabled for the given AA group:partition.

[Figure 23](#) illustrates the different messaging /call flows involved in application level usage monitoring. For details about the supported AVPs used in these messages, see section [Supported AVPs](#).

Figure 23 Usage Monitoring

al_0360

AA ISA (the PCEF) supports **Usage-Thresholds** AVPs that refer to the thresholds (in byte) at which point an event needs to be sent back to the PCRF (Figure 23).

No time based thresholds are supported.

AA supports **grant-service-unit** AVP using the following possible values (AVP):

- CC-Input-Octets AVP (code 412): From Subscriber total byte count threshold
- CC-Output-Octet AVP (code 414): To subscriber total byte count threshold
- CC-Total-octets AVP (code 421): Threshold of aggregate traffic (Input and Output byte counters)

As shown in [Figure 23](#) (T=7), AA sends a CCR message with a USAGE_REPORT Event-Trigger AVP to the PCRF when the usage counter reaches the configured usage monitoring threshold for a given subscriber (and given application group). AA counters are reset (to zero) when the monitoring threshold is reached (and an event is sent back to PCRF). The counters, however, do not stop counting newly arriving traffic. AA counters only include “admitted” packets. Any packets that got discarded by AA due to –say- policing actions- are not counted for usage-monitoring purposes.

The TDF-Application-Identifier AVP—within the ADC or PCC rule- refers to AA Charging group, AA application group or to an AA application.

TDF-Application-Identifiers (such as charging-groups) have to be manually entered at the PCRF to match AA charging groups configured on the 7750 SR.

If the TDF-Application-Identifiers refers to a name that is used for both a charging group and an application (or application group), AA monitors the charging group. In other words, AA charging group has higher precedence than AA application group.

3.2.2.3.11 Supported AVPs

ADC Rule AVP

The ADC Rule install appears in the CCA and RAR messages from PCRF towards AA ISA.

- For installing a new ADC rule or modifying an ADC rule already installed, ADC-Rule-Definition AVP shall be used.
- For activating a specific predefined ADC rule, ADC-Rule-Name AVP shall be used as a reference for that ADC rule.

```
ADC-Rule-Definition ::= < AVP Header: 1094 >
{
  ADC-Rule-Name
  [ TDF-Application-Identifier ]
  ; AA charging group /application group / application name
  [ Flow-Status ]*
  [ QoS-Information ]*
  [ Monitoring-Key ]
  [ Redirect-Information ] ::= < AVP Header: 1085 >*
    [ Redirect-Support ] ; *
    [ Redirect-Address-Type ] ;*
    [ Redirect-Server-Address ] ;*
  [ Mute-Notification ]*
}

*[ AVP ]
```

The AVPs marked by an asterisk in the above example are not supported by AA ISA.

The TDF-application-Identifier field specifies a predefined AA charging group, application group or application name for which usage monitoring functionality is required (for a given subscriber).

The Monitoring-Key AVP (AVP code 1066), refers to a predefined (by PCRF) USAGE Monitoring AVP.

The value of the monitoring key is random. However, it should be noted that a monitoring key instance can only be used in a single ADC rule (for example, single app/app-grp/chg-grp). While the standards allow for a monitoring instance to be referenced by one or more ADC rules, AA ISA implementation restricts this to one ADC rule. Hence, if a monitoring key is referenced in one ADC rule, it cannot be referenced by another.

PCC Rule AVP

The PCC rule install appears in the CCA and RAR messages from PCRF towards AA-ISA.

- For installing a new PCC rule or modifying an PCC rule already installed, the ADC-Rule-Definition AVP shall be used.
- For activating a specific predefined ADC rule, ADC-Rule-Name AVP shall be used as a reference for that ADC rule.

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
{ Charging-Rule-Name }
  [ TDF-Application-Identifier ]
  [ Monitoring-Key ]
  .....
  * [ AVP ]
```

Charging-Rule-Name — The name of the charging rule that contains a rule related to usage monitoring of a TDF_application_id has to start with: "AA-UM:" e.g. AA-UM: Peer to peer traffic for APN x"

TDF-application-Identifier — This field specifies a predefined AA charging group, application group or application name for which usage monitoring functionality is required (for a given subscriber).

The Monitoring-Key AVP (AVP code 1066) refers to a predefined (by PCRF) USAGE Monitoring AVP.

The value of the monitoring key is random. However, it should be noted that a monitoring key instance can only be used in a single PCC rule (e.g. single app/app-grp/chg-grp). i.e. while the standards allow for a monitoring instance to be referenced by one or more PCC rules, AA ISA implementation restricts this to one PCC rule. Hence, if a monitoring key is referenced in one PCC rule, it cannot be referenced by another.

Usage-Monitoring-Information AVP

The Usage-Monitoring-Information AVP (AVP code 1067) is of type Grouped, and it contains the usage monitoring control information.

The Monitoring-Key AVP identifies the usage monitoring control instance.

```
Usage-Monitoring-Information ::= < AVP Header: 1067 >
    [ Monitoring-Key ]
    [ Granted-Service-Unit ]
    [ Used-Service-Unit ]
    [ Usage-Monitoring-Level ]
    [ Usage-Monitoring-Report ]
    [ Usage-Monitoring-Support ]
    *[ AVP ]
```

Monitoring-Key-AVP

The Monitoring-Key AVP (AVP code 1066) is of type OctetString and is used for usage monitoring control purposes as an identifier to a usage monitoring control instance.

Granted-Service-Unit AVP

The Granted-Service-Unit AVP shall be used by the PCRF to provide the threshold level to the PCEF.

The CC-Total-Octets AVP shall be used for providing threshold level for the total volume, or the CC-Input-Octets and/or CC-Output-Octets AVPs shall be used for providing threshold level for the uplink volume and/or the downlink volume.

```
Granted-Service-Unit ::= < AVP Header: 431 >
    [ Tariff-Time-Change ]*
    [ CC-Time ]*
    [ CC-Money ]*
    [ CC-Total-Octets ]
    [ CC-Input-Octets ]
    [ CC-Output-Octets ]
    [ CC-Service-Specific-Units ]*
    *[ AVP ]*
```

The AVPs marked by an asterisk in the above example are not supported by AA ISA.

Used-Service-Unit AVP

This AVP is used by AA_ISA (the PCEF) to provide the measured usage to the PCRF. Reporting is done, as requested by the PCRF, in CC-Total-Octets, CC-Input-Octets or CC-Output-Octets AVPs of Used-Service-Unit AVP.

The Used-Service-Unit AVP contains the amount of used units measured from the point when the service became active or, if interim interrogations are used during the session, from the point when the previous measurement ended.

```
Used-Service-Unit ::= < AVP Header: 446 >
    [ Tariff-Change-Usage ]*
    [ CC-Time ]*
    [ CC-Money ]*
    [ CC-Total-Octets ]
    [ CC-Input-Octets ]
    [ CC-Output-Octets ]
    [ CC-Service-Specific-Units ]*
    *[ AVP ]*
```

The AVPs marked by an asterisk in the above example are not supported by AA ISA

CC-Total-Octets AVP — The CC-Total-Octets AVP (AVP Code 421) is of type Unsigned64 and contains the total number of requested, granted, or used octets regardless of the direction (sent or received).

CC-Input-Octets AVP — The CC-Input-Octets AVP (AVP Code 412) is of type Unsigned64 and contains the number of requested, granted, or used octets that can be/have been received from the end user.

CC-Output-Octets AVP — The CC-Output-Octets AVP (AVP Code 414) is of type Unsigned64 and contains the number of requested, granted, or used octets that can be/have been sent to the end user.

Usage-Monitoring-Level AVP

The Usage-Monitoring-Level AVP (AVP code 1068) is of type Enumerated and is used by the PCRF to indicate the level to which the usage monitoring instance applies.

If Usage-Monitoring-Level AVP is not provided, its absence shall indicate the value PCC_RULE_LEVEL (1).

The following values are defined (by the standard):

- SESSION_LEVEL (0)—Not applicable for AA-ISA
- PCC_RULE_LEVEL (1) —This value, if provided within an RAR or CCA command by the PCRF, indicates that the usage monitoring instance applies to one or more PCC rules. This is used in 3GPP Release 12 by the AA Usage Monitoring feature.

- **ADC_RULE_LEVEL (2)** — This value, if provided within an RAR or CCA command by the PCRF, indicates that the usage monitoring instance applies to one or more ADC rules. This is used in 3GPP Release 11 by the AA Usage Monitoring feature.

Usage-Monitoring-Report AVP

The Usage-Monitoring AVP (AVP code 1069) is of type Enumerated and is used by the PCRF to indicate that accumulated usage is to be reported by AA ISA (the PCEF) regardless of whether a usage threshold is reached for certain usage monitoring key (within a Usage-Monitoring-Information AVP).

The following values are defined:

- **USAGE_MONITORING_REPORT_REQUIRED (0)**
- This value, if provided within an RAR or CCA command by the PCRF indicates that accumulated usage shall be reported by the PCEF.

If no monitoring keys are set, AA ISA reports all enabled monitoring instances for the subscriber.

Usage-Monitoring-Support AVP

The Usage-Monitoring-Support AVP (AVP code 1070) is of type Enumerated and is used by the PCRF to indicate whether usage monitoring shall be disabled for certain Monitoring Key.

The following values are defined:

- **USAGE_MONITORING_DISABLED (0)**
- This value indicates that usage monitoring is disabled for a monitoring key.

Event-Trigger AVP (All Access Types)

The Event-Trigger AVP (AVP code 1006) is of type Enumerated. When sent from the PCRF to the PCEF (AA ISA) the Event-Trigger AVP indicates an event that can cause a re-request of ADC rules. When sent from the PCEF to the PCRF the Event-Trigger AVP indicates that the corresponding event has occurred at the gateway.

- **USAGE_REPORT (26)**
- This value is used in a CCA and RAR commands by the PCRF when requesting usage monitoring at the PCEF (AA ISA). The PCRF also provides in the CCA or RAR command the Usage-Monitoring-Information AVPs including the Monitoring-Key AVP and the Granted-Service-Unit AVP.

When used in a CCR command, this value indicates that AA ISA (the PCEF) generated the request to report the accumulated usage for one or more monitoring keys. AA_ISA provides the accumulated usage volume using the Usage-Monitoring-Information AVPs including the Monitoring-Key AVP and the Used-Service-Unit AVP.

The usage_report event must be set by the PCRF, otherwise AA ISA will not report usage-monitoring when a threshold is crossed.

Usage-Monitoring Disabled

Once enabled, the PCRF may explicitly disable usage monitoring as a result of receiving a CCR from AA ISA which is not related to reporting usage, but related to other external triggers (such as subscriber profile update), or a PCRF internal trigger.

When the PCRF disables usage monitoring, AA ISA reports the accumulated usage which has occurred while usage monitoring was enabled since the last report.

To disable usage monitoring for a monitoring key, the PCRF sends the Usage-Monitoring-Information AVP including only the applicable monitoring key within the Monitoring-Key AVP and the Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED.

When the PCRF disables usage monitoring in a RAR or CCA command, AA ISA sends a new CCR command with CC-Request Type AVP set to the value UPDATE_REQUEST and the Event-Trigger AVP set to USAGE_REPORT to report accumulated usage for the disabled usage monitoring keys.

Termination Session

At AA ISA subscriber's session termination, AA ISA sends the accumulated usage information for all monitoring keys for which usage monitoring is enabled in the CCR command with the CC-Request-Type AVP set to the value TERMINATION_REQUEST.

3.2.2.3.12 Cflowd AA Records

AA ISA allows cflowd records to be exported to an external cflowd collector. The cflowd collector parameters (such as IP address and port number) are configured per application assurance group. Operators can choose to export cflowd records directly inband on a configurable VLAN from AA or via the CPM, similar to the way system cflows are exported. By exporting directly inband, a higher rate of cflowd records can be exported compared to export via CPM, as inband export by-passes CPM and hence avoids the CPM bottleneck that could potential lead to cflowd packets discards. All cflowd records collected are exported to the configured collectors. AA ISA supports cflowd Version 10/ IPFIX.

A cflowd record is only exported to the collector once the flow is closed/terminated.

TCP Application Performance

AA ISA allows an operator to collect per flow TCP performance statistics to be exported through cflowd v10/IPFIX.

The operator can decide to collect TCP performance for sampled flows within a TCP enabled group-partition-application/application-group. The flow sampling rate is configurable on per ISA-group level. For example a flow sample rate of 10 means that every 10th TCP flow is selected for TCP performance statistics collection. Anytime a flow is sampled (selected for TCP performance statistics collection) its mate flow in reverse direction is also selected. This allows collectors to correlate the results from the two flows and provide additional statistics (such as round-trip delay). Per-flow cflowd TCP performance records are exported to the configured collectors upon flow closure. The system can gather per flow TCP performance statistics for up to 307,200 concurrent flows.

Two configurable TCP flow sampling rates are available per AA ISA group. Applications and/or Application groups selected for TCP performance monitoring can use of one these two sampling rates. For example, important applications are assigned high sampling rates, while other TCP applications are subjected to TCP performance monitoring using a lower flow sampling rate.

Per-flow TCP performance can be enabled (or disabled), using one of two configurable sampling rates, per application/app-group per partition per AA ISA-group.

Volume Statistics

AA ISA allows an operator to collect per flow volume statistics to be exported for any group partition. The packet sampling rate is configurable per AA- ISA-group level. For example, a packet sample rate of 10 means that one of every 10 packets is selected for volume statistics collection. If a flow has at least a single packet sampled for cflowd volume statistics, its per-flow cflowd volume record is exported to the configured collector upon flow closure.

Comprehensive Statistics

AA ISA allows an operator to collect per flow comprehensive statistics to be exported through cflowd v10/IPFIX.

This record type facilitates two deployments scenarios:

1. HTTP host and device info — Using the new performance cflowd, operators can collect statistics regarding the host names (used, for example, in HTTP GET methods) and device types being used in different flows within the network. These per flow statistics are exported via IPFIX v10 cflowd formatted records to a cflowd collector (such as RAM DCP) to enable intelligent reporting on devices and host fields.
2. Scaling of cflowd — In some situation, operators are mainly interested in augmenting the 5 Tuple IP flow information with AA classification of the flows in terms of application/application group. While AA volume cflowd provides such a function, however it is enabled at AA-partition level, covering all traffic within a partition, which then prohibits the use of high sampling rates. Using AA comprehensive flow- sampled cflowd mechanism, operators can target (or exclude), within an AA partition, certain applications (/application groups) for sampling. Hence providing finer control at the application/application group level, rather than at the partition level (case of volume cflowd).

The operator can decide to collect comprehensive statistics for sampled flows within an enabled group-partition-application/application-group. Parameters such as flow's applications/application groups, host fields (applicable to HTTP traffic only), subscriber's device type (when available), along with other general statistics such as flow's bytes/packets counts are collected in a comprehensive cflowd record.

The flow sampling rate is configurable on per ISA group level. For example, a flow sample rate of 10 means that every 10th flow is selected for comprehensive statistics collection. Any time a flow is sampled (selected for comprehensive statistics collection) its mate flow in reverse direction is also selected. The two flows are exported in a single cflowd record.

Per-flow comprehensive can be enabled (or disabled), using one of two configurable sampling rates, per application/app-group per partition per AA ISA-group.

Applications and/or Application groups selected for comprehensive statistics gathering can use one of these two sampling rates. For example, important applications are assigned high sampling rates, while other applications are subjected to a lower flow sampling rate.

Audio/Video (A/V) Application Performance

AA ISA integrates a third party audio/video performance measurement software stack to perform VoIP and video conferencing MOS-related measurements for RTP based A/V applications.

A passive monitoring technology estimates transmission quality of voice and video over packet technologies by considering the effects of packet loss, jitter and delay in addition to the impairments caused by encoding/decoding technology. A rich set of diagnostic data is provided that can be used to help network managers identify a variety of problems that could impact the quality of voice and video streams and/or service level agreements (SLAs).

This feature provides:

- Call quality analysis using optimized ITU-T G.107, such as listening and conversational quality MOS and R-factor scores – MOS-LQ, MOS-CQ R-LQ and R-CQ.
- Measurements of perceptual effects of burst packet loss and recency using ETSI TS 101 29-5 Annex E Extensions
- Reporting of RTCP XR (RFC 3611, *RTP Control Protocol Extended Reports (RTCP XR)*) VoIP metrics payloads.

Once a flow terminates, AA ISA formats the flow MOS parameters into a cflowd record and forwards the record to a configured IPFIX /10 cflowd collector (such as 5670 RAM). The collector then summarizes these records using route of interest information (source/destinations). In addition, RAM provides the user with statistics (min/max/avg values) for the different performance parameters that are summarized.

Two configurable RTP flow sampling rates are available per AA ISA group. Applications and/or Application groups selected for RTP performance monitoring can use one of these two sampling rates. For example, important applications (such as Cisco's Telepresence video conferencing or operator's VoIP service) are assigned high sampling rates, while other RTP applications are subjected to RTP performance monitoring using a lower flow sampling rate.

Like TCP performance, per flow audio/video performance can be enabled (or disabled), using one of two configurable sampling rates, per application/app-group per partition per AA ISA-group.

The operator can decide to collect RTP A/V performance for sampled RTP flows within an RTP A/ V enabled group-partition-application/application-group. The two available flow sampling rates is are configurable on per ISA group level. For example a flow sample rate of 10 means that every 10th RTP flow is selected for RTP performance statistics collection. Anytime a flow is sampled (selected for RTP A/V performance statistics collection) its mate flow reverse direction is also selected. When RTP dynamic payload types (RTP "PT") are used, only flows that use SIP to signal RTP codec can be selected for RTP performance measurement. Flows that use static RTP payload types can be selected for performance measurement regardless of the signaling channel used to setup the call. The system can gather per flow RTP A/V performance statistics for up to 6000 voice calls.

3.2.2.4 Application QoS Policy (AQP)

An AQP is an ordered set of entries defining application-aware policy (actions) for IP flows diverted to a given AA ISA group. The IP flow match criteria are based on application identification (application or application group name) but are expected to use additional match criteria such as ASO characteristic value, IP header information or AA subscriber ID, for example.

When ASO characteristic values are used in application profiles, the characteristics values can be further used to subdivide an AQP into policy subsets applicable only to a subset of AA subscribers with a given value of an ASO characteristic in their profile. This allows to, for example, subdivide AQP into policies applicable to a specific service option (MOS iVideo Service), specific subscriber class (Broadband service tier, VPN, Customer X), or a combination of both.

A system without AQP defined will have statistics generated but will not impact the traffic that is flowing through the system. However, it is recommended that an AQP policy is configured with at least default bandwidth and flow policing entries to ensure a fair access to AA ISA bandwidth/flow resources for all AA subscribers serviced by a given AA ISA.

AQP rules consist of match and action criteria:

- Match: Refers to application identification determined by application and application group configuration using protocol signatures and user-configurable application filters that allow customers to create a wide range of identifiable applications. To further enhance system-wide per subscriber/service management user configurable application groups are provided.
- An AQP consists of a numbered and ordered set of entries each defining match criteria including AND, NOT and wild card conditions followed by a set of actions.

AQP Entry <#> = <Match Criteria> AND <Match Criteria> <action> <action>

- OR match conditions are supported in AQP through defining multiple entries. Multiple match criteria of a single AQP entry form an implicit AND function. An AQP can be defined for both recognized and unrecognized traffic. IP traffic flows that are in the process of being identified have a default policy applied (AQP entries that do not include application identification or IP header information). Flows that do not match any signatures are identified as unknown-tcp or unknown-udp and can have specific policies applied (as with any other protocol).
- Actions: Defines AA actions to be applied to traffic, a set of actions to apply to the flows like bandwidth policing, packet discards, QoS remarking and flow count or/and rate limiting.

3.2.2.4.1 AQP Match Criteria

Match criteria consists of any combination of the following parameters:

- The source/destination IP address and port/port-list, or IP-prefix list
- Application name
- Application group name
- Charging group name
- One or more ASO characteristic and value pairs
- Direction of traffic (subscriber-to-network, network-to-subscriber, or both, or spoke SDP)
- DSCP name
- AA subscriber (ESM, DSM, or transit subscriber, SAP or spoke SDP)
- **ip-protocol-num** field, which when used in AQP matches allows more precise control of match criteria, e.g. to specify port or IP address matches specifically for either TCP or for UDP.

AQP entries with match criteria that exclusively use any combination of ASO characteristic and values, direction of traffic, and AA subscriber define default policies. All other AQP entries define application aware policies. Both default and application aware policies. Until a flow's application is identified only default policies can be applied.

3.2.2.4.2 AQP Actions

An AQP action consists of the following action types. Multiple actions are supported for each rule entry (unlike ip-filters):

- Dual or single-bucket bandwidth rate limit policer

- Drop (discard)
- Error drop
- Flow count limit policer
- Flow setup rate limit policer
- Fragment drop
- HTTP enrichment
- HTTP error redirect
- HTTP notification
- HTTP redirect
- Source mirror for an existing mirror service
- Remark QoS (one or a combination of discard priority, forwarding class name, DSCP). When applied, ingress marked FC and discard priority is overwritten by AA ISA and the new values are used during egress processing (for example, egress queueing or egress policy DSCP remarking). For MPLS class-based forwarding, ingress-marked FC is still used to select an egress tunnel.
- None (monitor and report only)
- Session filter
- URL-Filter (ICAP Category Based URL Filtering)
- GTP filter
- SCTP filter
- TCP MSS adjust
- TCP validate

Any flow diverted to an ISA group is evaluated against all entries of an AQP defined for that group at flow creation (default policy entries), application identification completion (all entries), and an AA policy change (all flows against all entries as a background task). Any given flow can match multiple entries, in which case multiple actions will be selected based on the AQP entry's order (lowest number entry, highest priority) up to a limit of:

- 1 drop action
- Any combination of (applied only if no drop action is selected):
 - Up to 1 mirror action;
 - up to 1 FC, 1 priority and 1 DSCP remark action;
 - up to 4 BW policers;
 - up to 12 flow policers.

AQP entries the IP flow matched, that would cause the above per-IP-flow limits to be exceeded are ignored (no actions from that rule are selected).

Examples of some policy entries may be:

- Limit the subscriber to 20 concurrent Peer To Peer (P2P) flows max.
- Rate limit upstream total P2P application group to 400 kb/s.
- Remark the voice application group to EF.

3.2.2.4.3 Application Assurance Policers

The rate limit (policer) policy actions provide the flow control mechanisms that enable rate limiting by application and/or AA subscribers.

There are six types of policers:

- Flow rate policer monitors a flow setup rate.
- Flow count limits control the number of concurrent active flows
- Single-rate bandwidth policers monitor bandwidth using a single rate and burst size parameters.
- Dual-rate bandwidth rate policers monitor bandwidth using CIR/PIR and CBS/MBS. These can only be used at the per-subscriber granularity.
- Time of day overrides the default policer values at the specified time of day.
- Congestion override policers apply when the subscriber is in a congestion state.

Once a policer is referred to by an AQP action for one traffic direction, the same policer cannot be referred to in the other direction. This also implies that AQP rules with policer actions must specify a traffic direction other than the “both” direction.

[Table 16](#) illustrates a policer's hardware rate steps for AA ISA.

Table 16 **Policer's Hardware Rate Steps for AA ISA**

Hardware Rate Steps	Rate Range (Rate Step x 0 to Rate Step x 127 and max)
0.5 Gbytes/s	0 to 64 Gbytes/s
100 Mb/s	0 to 12.7Gbytes/s
50 Mb/sec	0 to 6.4 Gbytes/s
10 Mb/sec	0 to 1.3 Gbytes/s
5 Mb/sec	0 to 635 Mb/sec
1 Mb/s	0 to 127 Mb/s

Table 16 **Policer's Hardware Rate Steps for AA ISA (Continued)**

Hardware Rate Steps	Rate Range (Rate Step x 0 to Rate Step x 127 and max)
500 kb/s	0 to 64 Mb/s
100 kb/s	0 to 12.7 Mb/s
50 kb/s	0 to 6.4 Mb/s
10 kb/s	0 to 1.2Mb/s
8 kb/s	0 to 1 Mb/s
1 Kb/sec	0 to 127 Kb/sec

Policers are unidirectional and are named with these attributes:

- Policer name
- Policer type: single or dual bucket bandwidth, flow rate limit, flow count limit.
- Granularity: select per-subscriber, system-wide, or Access-Network-Location (ANL)
- Parameters for flow setup rate (flows per second rate)
- Parameters for flow count (maximum number of flows)
- Rate parameters for single-rate bandwidth policer (PIR)
- Parameters for two-rate bandwidth policer (CIR, PIR)
- PIR and CIR adaptation rules (min, max, closest)
- Burst size (CBS and MBS)
- Conformant action: allow (mark as in-profile)
- Non-conformant action: discard, or mark with options being in profile and out of profile

Policers allow temporary over subscription of rates to enable new sessions to be added to traffic that may already be running at peak rate. Existing flows are impacted with discards to allow TCP backoff of existing flows, while preventing full capacity from blocking new flows.

Policers can be based on an AQP rule configuration to allow per-app-group, per-AA subscriber total, per AA profile policy per application, and per system per app-group enforcement.

Policers are applied with two levels of hierarchy (granularity):

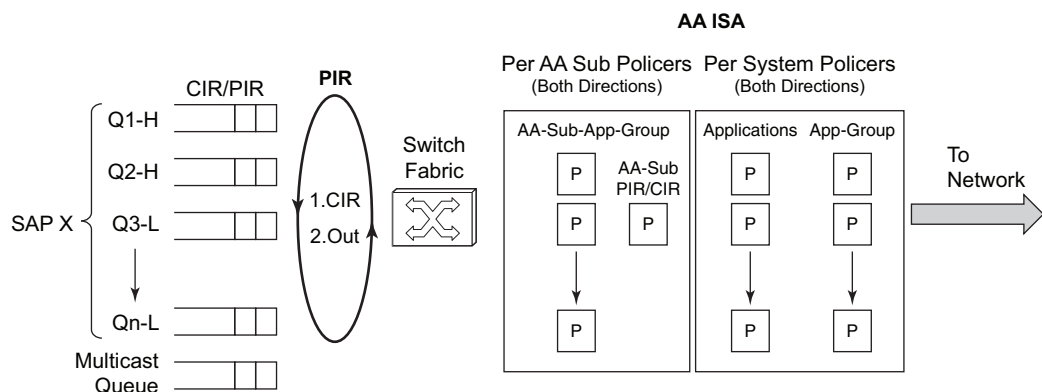
- Per individual AA subscriber

- Per-AA subscriber per app group/application or protocol rate
- Per-AA subscriber per application rate limit for a small selection of applications
- Per-AA subscriber PIR/CIR. This allows the AA ISA to emulate IOM ingress policers in from-sub direction.
- Per system (AA ISA or a group of AA subscribers)
 - Total protocol/application rate
 - Total app group rate
- Per ANL
 - Per-ANL per application group/application or protocol rate

Flows may be subject to multiple policers in each direction (from-subscriber-to-network or from network-to-subscriber).

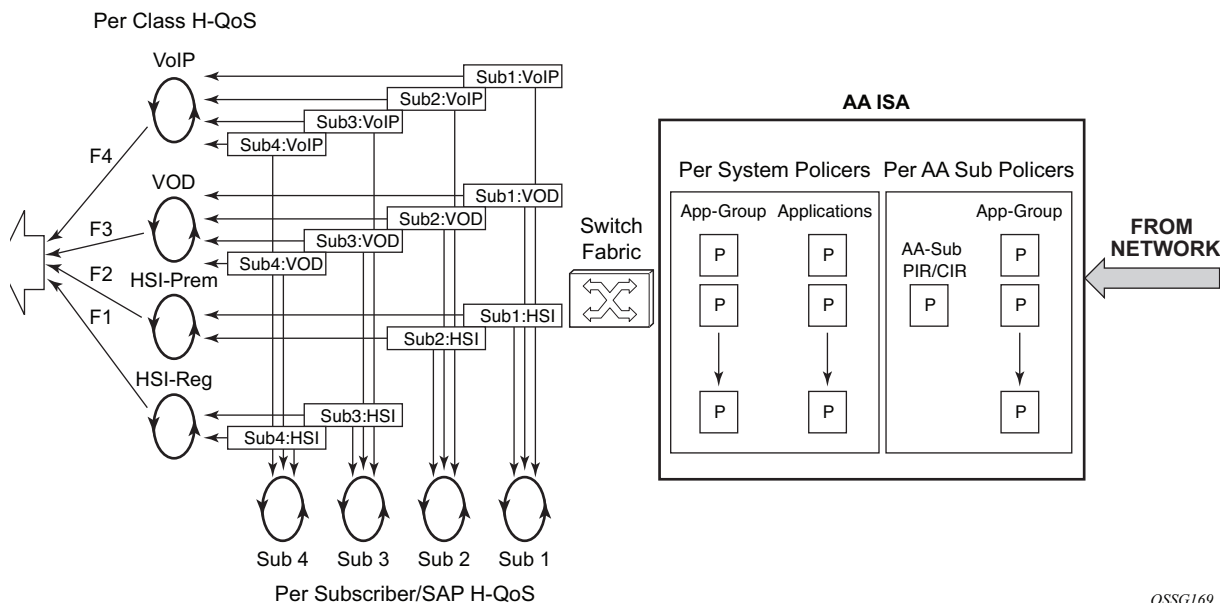
In [Figure 24](#), Application Assurance policers are applied after ingress SAP policers. Configuration of the SAP ingress policers can be set to disable ingress policing or to set PIR/CIR values such that AA ISA ingress PIR/CIR will be invoked first. This enables application aware discard decisions, ingress policing at SAP ingress is application blind. However, this is a design/implementation guideline that is not enforced by the node.

Figure 24 From-AA Subscriber Application-Aware Bandwidth Policing



OSSG166

In the to-AA subscriber direction ([Figure 25](#)), traffic hits the AA ISA policers before the SAP egress queuing and scheduling. This allows application aware flow, AA subscriber and node traffic policies to be implemented before the Internet traffic is mixed with the other services at node egress. AA ISA policers may remark out-of-profile traffic which allows preferential discard at an IOM egress congestion point only upon congestion.

Figure 25 To-AA Subscriber Application-Aware Bandwidth Policing

3.2.2.4.4 Time of Day Policing Adjustments

Time-of-day changes to Application Assurance policing rates are supported through the use of time-of-day override in the policers, up to eight overrides. Up to eight overrides can be configured per policers each using either a daily or weekly time-range. The adjusted policing limits are applied immediately to any pre-existing or new flows.

3.2.2.4.5 Congestion Override Policing

As part of Dynamic Experience Management (DEM), congested Access Network Locations (ANLs) can, if configured, trigger a policing override to the per-subscriber's bandwidth policers. When a subscriber is declared to be in a congestion state, the per-sub congestion policer rates are triggered. This overrides any pre-existing per-sub policer rates, including time-of-day policer rates. These per-sub congestion policer rates are applied for the duration of time that the subscriber is in a congestion state. Once the subscriber's state is changed to uncongested, the per-sub congestion policer rates are no longer applied to the subscriber's traffic. The adjusted policing limits are applied immediately to any pre-existing or new flows of the subscriber.

The per-sub congestion override policers are only applicable to bandwidth policers, both single and dual leaky buckets. They are not applicable to per-sub flow count or flow rate policers.

To configure the per-subscriber bandwidth policer override rates, use the following commands:

- **config>app-assure>group>policer>congestion-override**
- **config>app-assure>group>policer>congestion-override>cbs**
- **config>app-assure>group>policer>congestion-override>mbs**
- **config>app-assure>group>policer>congestion-override>pir**
- **config>app-assure>group>policer>congestion-override>cib**

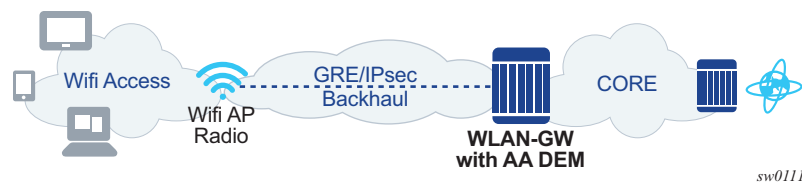
3.2.2.4.6 Dynamic Experience Management

Dynamic Experience Management (DEM) is a Wireless LAN Gateway (WLAN GW) capability that monitors user plane traffic to build a network-wide view of congestion on the subscriber, application, and access point radio levels. DEM enables making real-time decisions and dynamic actions, such as rate limiting or blocking of certain applications. It provides a managed, optimal user experience within the actual, overall network capabilities.

In situations of high network load and congestion, application Quality of Experience (QoE) degrades due to restricted resources across the network (for example, in radio or transport). In this context, operators cannot differentiate background traffic from real-time traffic efficiently and dynamically. This differentiation is especially important for delay-sensitive applications such as video.

In Radio Access Networks (RAN), the network congestion points are typically located in the access point WiFi radio. See [Figure 26](#).

Figure 26 WiFi Network Congestion at AP Radio



Increased penetration of WiFi-enabled devices (for example, mobile handsets, tablets, laptops, and TVs) and widespread use of streaming video results in frequent data plane congestion events in WiFi networks. This congestion results in service degradation for WiFi subscribers attached to congested access points and creates challenges in implementing fair usage policies to manage network congestion in the access network.

DEM provides the capability of managing WiFi access congestion points at the WLGW to provide some level of QoS guarantees to different applications, which otherwise poses challenges as the loading of the different access points at any point in time is different, both in quantity (Bandwidth) and application types (for example, video, web, or mail).

Intelligent Network Congestion Control

DEM technology is an implementation of intelligent congestion control. If congestion is predicted or detected, the DEM gateway automatically scales back the less delay-sensitive traffic and gives priority to more delay-sensitive applications. Applications are managed to their respective resource needs to provide the best QoE. Over The Top (OTT) applications and users are managed to their respective resource needs and configured preferences.

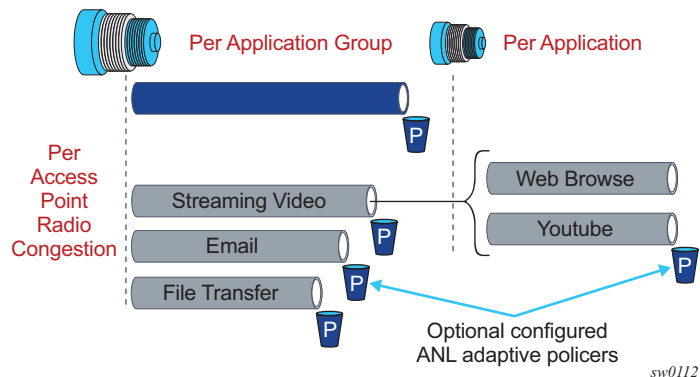
A DEM-GW builds on AA Layer 3 to Layer 7 DPI capabilities to detect applications per AA subscriber as well as per congestion point. It allows the DEM-GW AA to take intelligent actions when congestion occurs in the access network.

Multi-Point Congestion Enforcement

The DEM technology allows the DEM GW to detect congestion within the access network.

If congestion is detected at any point, DEM-GW can employ policies per application, per application group, or per subscriber to limit the impact of low-priority traffic on QoE-sensitive applications. See [Figure 27](#).

Figure 27 DEM-GW Multi-point Congestion Control



A DEM-GW is integrated directly into the WLGW using AA. The DEM-GW models the congestion points, called Access Network Location (ANLs), that it learns from the WLGW subscriber attributes, and manages them accordingly to achieve the configured QoE/QoS target.

The DEM-GW achieves congestion control by:

- running DPI to classify flows into applications, including encrypted traffic
- dynamically learning access network congestion points and estimating their maximum capacity:
 - through real-time detection, sniffing, measurements and profiling
 - continuous monitoring of UEs locations and associating them to the right access point radio congestion points
- QoE enforcement:
 - efficient access point radio congestion detection, localization and management provided via configurable adaptive policers

The DEM-GW actively runs intelligent congestion control. It relies on location information relayed by WLGW sub management for Access Point MAC and VLAN.

For AP congestion detection, the DEM-GW runs an algorithm-based on measurements of Round Trip Time (RTT) to determine congestion state.

The DEM-GW uses location-awareness of all UEs to apply traffic management at specific impacted access sites, while un-restricting users during times of non-congestion. This ensures different applications within an AP radio get fair share of available resources, while controlling low-value traffic during times of congestion.

The inherited subscriber or application awareness at the DEM-GW (SSG/PGW/GGSN), when integrated with AA application detection and control, results in entitlement-based enforcements of specific applications for specified users or UEs, allowing the operators to provide differentiated services.

The end-to-end DEM solution can involve PCRF for opt-in policy control and off-line reporting platforms to facilitate some additional value-add use-cases.

Access-Network-Location Policers

DEM-GW employs adaptive bandwidth policer variants of AA single leaky bucket bandwidth policers, called Access-Network-Location policers. These policers are used exclusively with DEM-GW congestion points (WLGW AP radio). They are similar to existing single bucket policers, but differ in the following aspects.

- The policer rate is configured using a ratio (/%) instead of absolute rates.
- The ratios are applied against the total estimated measured capacity of the congestion point to derive the actual policer's rate. For example, for measured capacity at congestion time of 1.5Mbps, or a configured policer rate of 30%, the actual policer rate applied: $1.5 \times 30\% = 0.5$ Mbps.
- Adaptive policers are applied only in the downstream traffic direction.
- Adaptive policers run only while the associated ANL is in congestion state. No action is taken when there is no congestion.

These policers are invoked using existing AQP mechanisms that match configured parameters such as apps or app-groups and execute the configured actions.

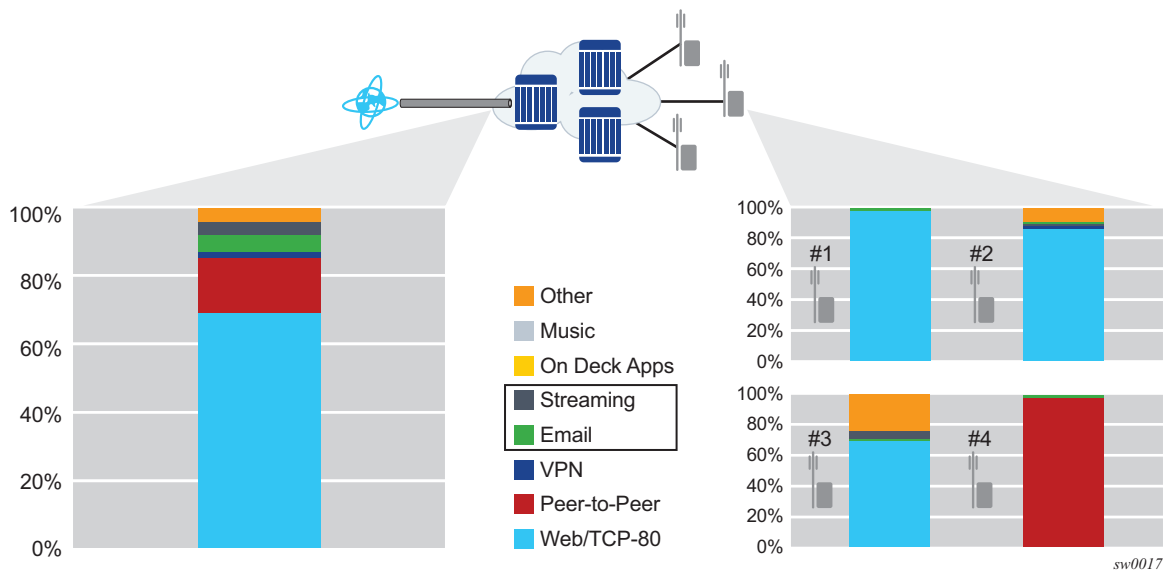
Adaptive-policers are used to throttle traffic going through access point radios during congestion state. Multiple adapt-policers can be configured per congestion point-type (type =MAC+VLAN). For example:

- adapt-policer 1,rate=20(%), backhaul links — called from AQP entry with “email” app-group match condition
- adapt-policer 2,rate=10(%), backhaul links — called from AQP entry with OTT video app-group match condition
- adapt-policer 3,rate=0(%), backhaul links — called from AQP entry with p2p app-group match condition (this effectively drops p2p traffic during congestion)

Location Based Analytics

Location based analytics provides the operator with an accurate view of the subscriber's location (ANL) and application usage for a specified location in WiFi networks for the purpose of data-mining. See [Figure 28](#).

Figure 28 Access Point Radio per Application Reporting



To provide an accurate reporting of the subscriber location via analytics tools such as the Network Services Platform, AA exports location information and congestion status in both volume and comprehensive cflowd reports. The off-line cflowd collector then allows per ANL (Access Point and AP radio) per application or application groups statistics.

3.2.2.4.7 Application Assurance HTTP Redirect

AA HTTP Policy Redirect

With AA ISA HTTP policy based redirect feature, when HTTP flows are blocked, the user is directed to a web portal that displays relevant messages to indicate why the HTTP traffic is blocked, such as: time of day policy to block youtube.com, top-up request, and so on.

Without HTTP policy redirect, when HTTP flows are blocked, the subscriber application retries and before it times-out.

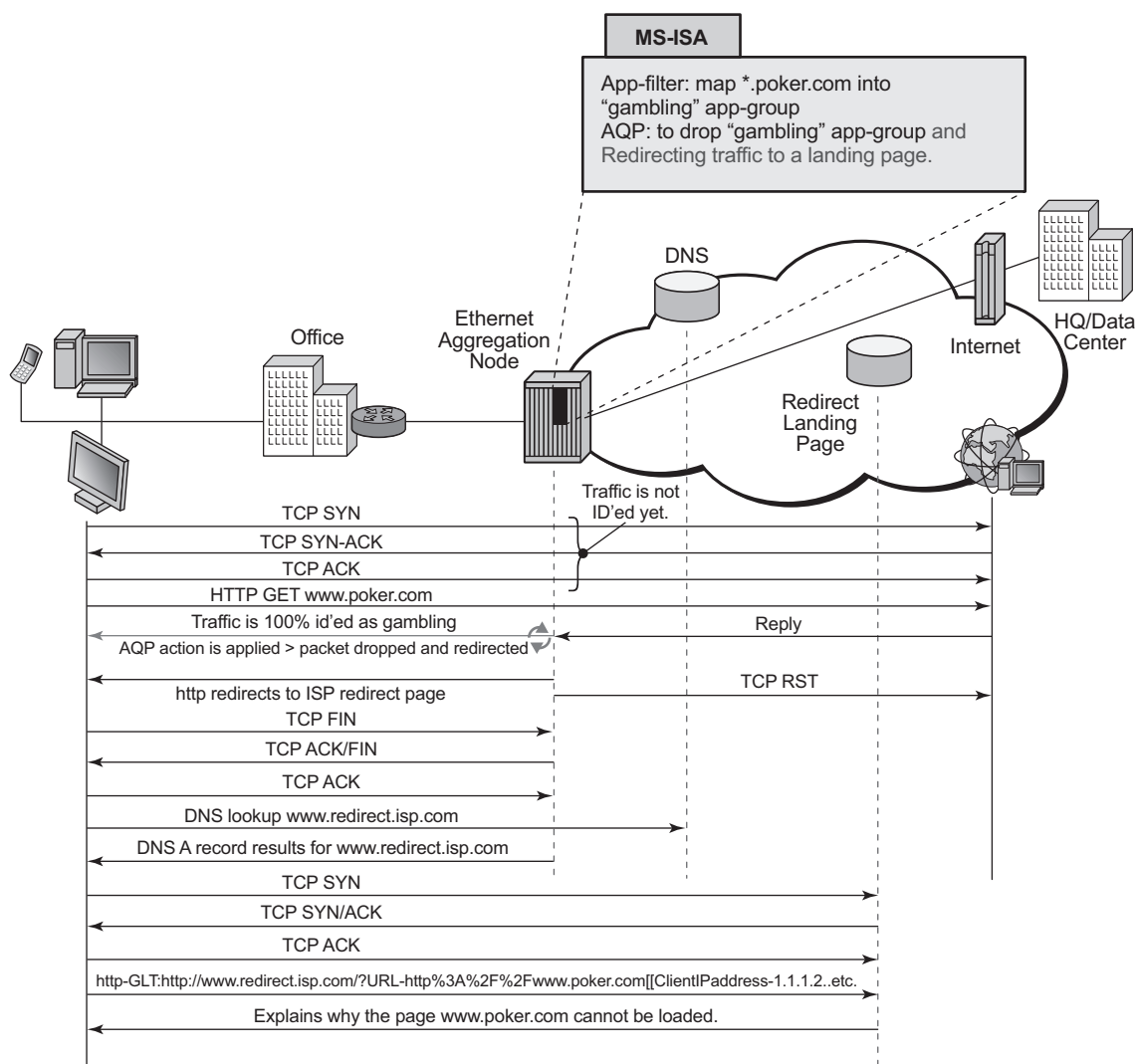
AA ISA provides full customer control to configure an AQP action that redirects traffic that matches the AQP match criteria. Hence, the HTTP redirect service can be applied at any level (application, application group, specific subscribers, specific source IP addresses) or any other AQP match criteria.

To illustrate, say the operator configures `www.poker.com` as a “gambling” app-group.

The operator configures AA_ISA to drop and redirect all HTTP traffic classified under “gambling” app-group to `www.redirect.isp.com`. When a client/subscriber initiates an HTTP GET for `www.poker.com`, traffic to `poker.com` is dropped at the AA ISA. AA ISA issues a redirect to the client. [in the redirect, information about the user are encoded in the PATH message, such as `www.poker.com`, sub-ID, sub-type, reason for redirect (=AQP drop action) AA application name]. Client, unaware of the drop, responds to the redirect.

Redirect landing page explains to the user why the page at `www.poker.com` is not accessible. See [Figure 29](#).

Figure 29 HTTP Redirect Due To URL Block



al_0186

AA ISA allows the operator to configure HTTP redirect policies. An HTTP redirect policy contains, most importantly, the HTTP host to be used for the redirect. Within the AQP actions, such policies can be linked (like policers). Redirect takes place only if the AQP configured matching criteria is met and the HTTP flow is dropped (due to other AQP actions, such as "drop", flow-count/rate policers). The redirect only applies to HTTP traffic. Non-HTTP flows (even if the conditions above are met) are not redirected (no redirect for RTSP traffic).

The HTTP redirect policy includes an option for TCP-client-reset. This is used to improve the end-user experience when TCP traffic that cannot be HTTP redirected is blocked. Resetting the client TCP session avoids the client waiting for tcp session timeout. The ISA will initiate a TCP reset towards the client if the AA policy results in an http-redirect with packet drop but the HTTP redirect cannot be delivered. Scenarios for this include blocked HTTPs (TLS) sessions, blocking of non-HTTP traffic, and blocking of existing flows after a policy re-evaluate of an existing subscriber. A mid-session policy change to redirect & block traffic for a sub will cause a TCP reset of existing non-http tcp sessions when the next packet for those sessions arrives. For example, when the packet is dropped.

AA HTTP 404 Redirect

HTTP status code-based redirect feature provides error resolution and search technology that enhances the Internet experience for end customers while generating new revenue stream for the ISP.

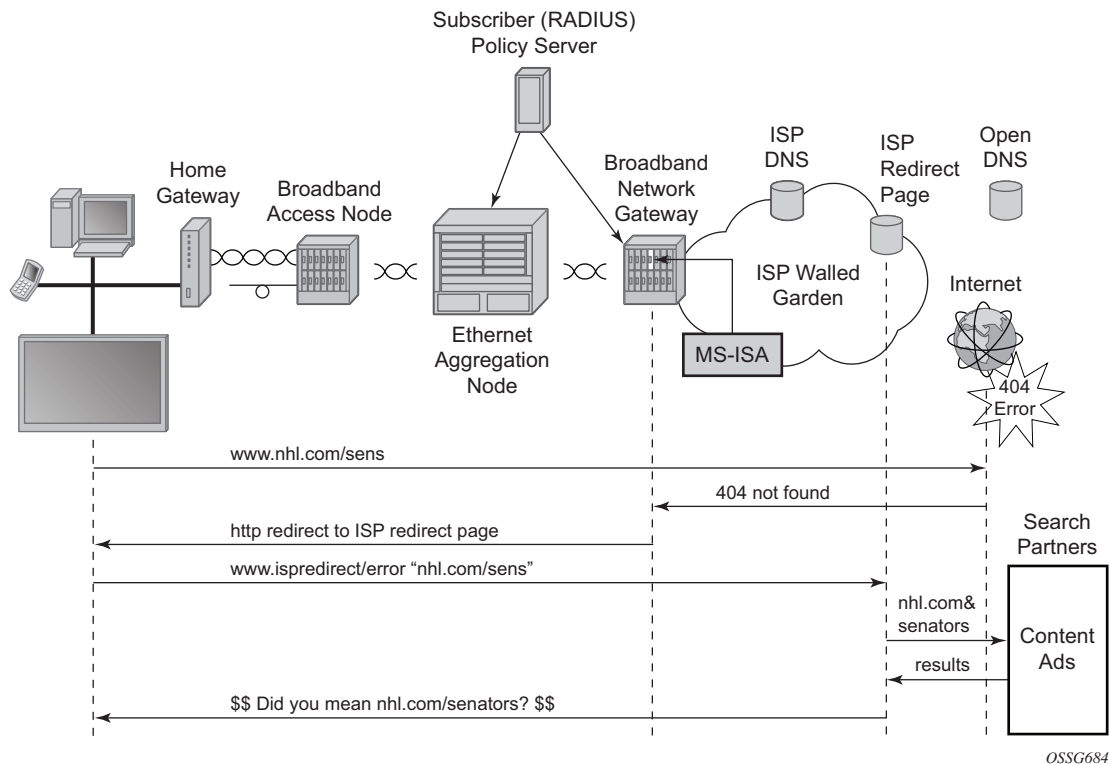
Nokia's AA ISA HTTP status code-based redirect feature, along with its partners Barefruit or Xercole, replaces unhelpful DNS and HTTP error messages with relevant alternatives, giving the user a search solution rather than a no direction. Customers benefit from an improved surfing experience as they are served relevant results that can help them find what they were looking for. The ISP, on the other hand, receives a share of the search revenue.

Every time an end-user clicks on a broken link (Page Not Found), an error page displays. Frequently, a search provider produces results, through a browser plug-in, for that user. This generates revenue for the search provider if the user clicks on a paid link.

With AA ISA HTTP status code-based redirect feature, the user sees high-quality, relevant search results. In addition, instead of the search provider receiving all of the revenue, the ISP is paid every time a user clicks on a sponsored link.

AA ISA provides full customer control to configure an AQP action that redirects traffic that matches the AQP match criteria ([Figure 30](#)). Hence, the HTTP redirect service can be applied at any level (application, application group, specific subscribers, specific source IP addresses) or any other AQP match criteria.

Figure 30 AQP Actions



HTTP headers are intercepted by AA ISA on the return path from the requested web site. If the HTTP status code is a non custom 404, then the response is replaced with JavaScript that redirects the client to the Contextual Analysis Servers (Barefruit server). This redirect contains details of the original URI that gave rise to the 404 error.

The operator can configure AA ISA HTTP 404 redirect to use either Barefruit or Xerocole partner contextual analysis servers. A redirect policy can be defined once at the AA group level (similar to policers), and then referenced as many times as needed in AQP actions. The system allows a maximum of one HTTP 404 redirect policy per AA group.

3.2.2.4.8 ICAP - Large Scale Category-based URL Filtering

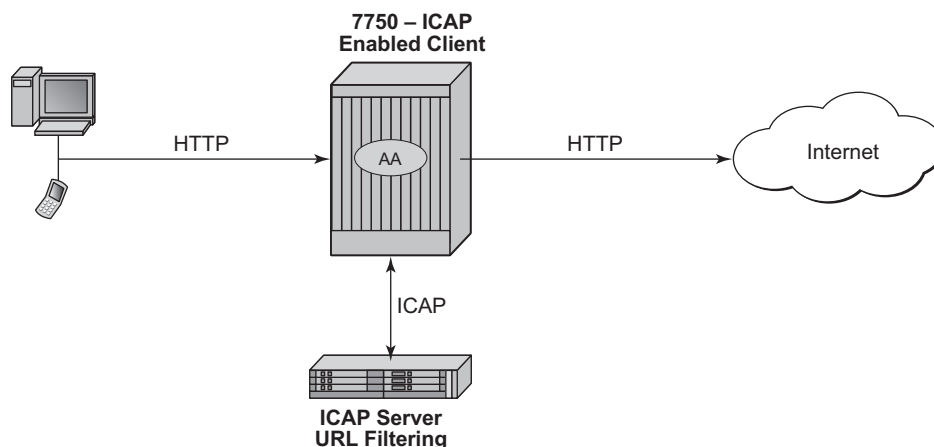
ICAP and the use of the AA-interface is only supported on the 7750 SR. Large scale URL filtering is a common content filtering requirement from broadband, mobile, and business VPN operators that allows them to solve various use cases such as:

- Category based URL filtering: typically offered as an opt-in service by broadband or mobile operators to protect the subscribers from accessing selected category of URLs, such as, gambling, drugs, pornography, racism and so on
- Managed URL filtering service for Business VPN to prevent employee from accessing specific content.

Application Assurance provides both a cost efficient and best of breed content filtering solution to solve these use cases by enabling off-line dedicated web filtering servers through the Internet Content Adaptation Protocol (ICAP). Using application assurance the operator does not need to deploy costly inline filtering appliances or a limited client software solution requiring maintenance and updates for a growing number of computing devices and operating systems (for example, laptop, smartphone, smartTV, tablets).

A high level packet flow diagram of the solution is shown in [Figure 31](#). The AA ISA is the ICAP client and performs inline Layer 7 packet processing functions while the ICAP application server is used for URL filtering off-line, thus the application server does not need to be inserted in the data flow:

Figure 31 ICAP High Level Flow Diagram



al_0185

The 7750 SR uses the Application Assurance capabilities to extract the URL from the subscriber's HTTP/HTTPS request and send an ICAP rating request to the ICAP server along with the subscriber-id information. The ICAP server can then return an accept or redirect response based on various criteria such as subscriber profile, URL categories, whitelist, blacklist, time of the day.

The ICAP response received by the 7750 SR ICAP client is used to either accept, redirect, or block the flow.

In order to handle the instance where an Internet server's reply arrives before the ICAP server's response, AA blocks traffic from the Internet server until the response from the ICAP server is received. This ensures that the appropriate action is always applied to the Internet traffic.

- Each HTTP request within a TCP flows are sent to the ICAP server for rating.
- HTTPs (SSL/TLS) ICAP URL-Filtering is limited to the domain name information.
- HTTPS Redirection can only be performed if the Client Hello message contains an SNI, in order to match the filter and proceed with the redirect action.

3.2.2.4.9 Local URL-List Filtering

Service providers may need to apply network wide URL filtering policies to prevent subscribers from accessing illegal content in the following context:

- Court order URL takedown
- Child pornography related content
- Government mandated URL takedown list

Operators can use AA to comply with these regulatory requirements typically driven by government or court order to control the access to specific URLs hosting illegal content. In the context of child protection the operator may be required or incited to provide this filtering.

Local url-list filtering is applied network-wide to all subscribers. This solution provides a cost-efficient method by storing the list of URLs to be filtered on the system compact flash. Therefore, using the AA-ISA ICAP functionality along with an external server is not necessary.

The ISA-AA url-filter local url-list filtering policy provides URL control capability using a list of URLs contained in a file stored on one of the system's compact flash cards. The router uses the Application Assurance capabilities to extract the URL from the subscriber's HTTP request and compares it to the list of URLs contained in this local file. If a match is found the subscriber flow is redirected to a preconfigured web server landing page typically describing why the access to this resource was denied.

The system supports both unencrypted and OpenSSL 3DES encrypted file formats to protect the content of the list.

Operators can specify the size of the URL list to be filtered. The size can be set to either standard or extended. Configuring the specified url-list as extended provides support for filtering on a larger number of URLs.

URL-List Update

The system supports a flexible mechanism to upgrade a local url-list automatically using either CRON or the NSP NFM-P to comply with the regulatory requirements in terms of list upgrade frequency.

HTTP/HTTPS

Each HTTP request within a TCP flow is filtered by the AA ISA. For HTTPS traffic, the system extracts the domain name information contained in the SSL/TLS server name.

File Format

The following characters are considered invalid and result in a failure to load the url-list:

- non-printable ASCII characters other than \n and \r
- space characters in the URL

When specifying a URL, do not include schema such as https:// or ftp://. The schema http:// is allowed but is not necessary.

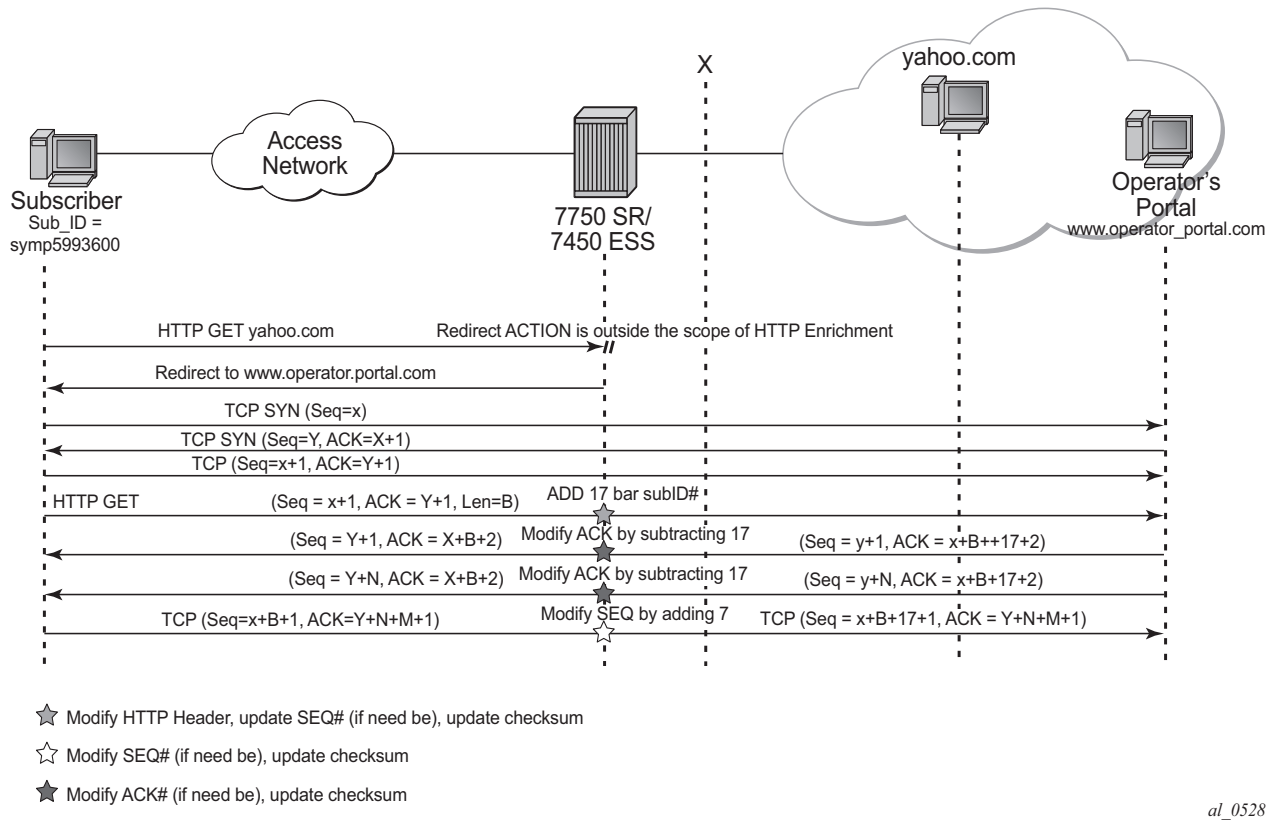
The following is an example of url-list file content.

```
# Comment line for domain1 URL not using http:// schema
www.domain1.com/URI1
# Comment line for domain2 URL using http:// schema
http://domain2.com/URI2
```


3.2.2.4.10 HTTP Header Enrichment

AA ISA supports modifications of the HTTP header for traffic going to specific user configured sites (URLs/IPs); in order to add Network based information, such as subscriber ID to the HTTP header. These sites use this information to authenticate the user and/or present the user with user-specific information and services.

Figure 32 HTTP Enrichment



In [Figure 32](#), the operator configures the AA ISA to insert the subscriber ID into the HTTP header for all the HTTP traffic destined to the operator portal (designated by server IP and/or HTTP host name). Traffic going to other destinations, such as yahoo.com, does not get enriched. To support this, AA introduces a new AQP action called **HTTP_enrich** that allows the operator to enrich traffic that satisfies the AQP-matching conditions.

The operator can configure multiple HTTP enrichment policies that get applied to traffic going to different destinations. For example, HTTP traffic destined to “xyz.com”, gets the user’s IP inserted into the header, while traffic going to “billing.xyz.com” gets enriched with subscriber ID and user’s IP address.

AA ISA supports insertion of one or more of the following parameters/fields into the HTTP header: User's IP@, subscriber ID and configurable static string fields. The text preceding the inserted field is fully configurable. For example, sub-ID = 1243534666 or x-sub-ID = 1243534666.

AA supports enrichment of all HTTP methods, such as GET, POST, and so on. AA enriches HTTP traffic without having to terminate the TCP session (for example, it does not act as a proxy). In this way, AA enrichment function does not intervene with other TCP acceleration functions or appliances that could be deployed by the operator.

For configured enriched fields, operators can optionally configure AA ISA to perform MD5 hashing, RC4 encryption, and anti-spoofing.

Encryption can be performed either by configuring an encryption key, which is used to encrypt the header values using the RC4 algorithm, or by installing a certificate and configuring header enrichment to use that certificate. In the case of certificate-based header enrichment, the system uses the key contained in the HTTP header and performs encryption using the RSA algorithm. A maximum of 20 certificate profiles per group are supported.

Anti-spoofing, if enabled, ensures that only the fields enriched by AA are valid. Anti-spoofing is applicable only to the subscriber ID field.

AA statistics reflect post header enrichment packet sizes.

AA HTTP enrichment functionality has the following caveats.

- To handle the case of TCP retransmission, AA ISA implements an enrichment window of size = 5. If a retransmission of a packet occurs outside the last five enriched packets, no enrichment takes place.
- Corrupted packets, AA ISA-cut-through and out-of-order fragments are not enriched
- Out-of-sequence packets are not enriched. For example, if AA –ISA receives out-of-sequence HTTP requests: REQ2,REQ1,REQ3; only REQ2 and REQ3 can be enriched
- No enrichment takes place if, by enriching, the resulting packet size will exceed the configured MTU size. AA ISA does not perform fragmentation.
- The length of an encrypted header is directly analogous to the length of the encryption key. If a 2048-bit key is used, the encrypted header becomes 512 bytes long. Operators must be cautious when defining the key length and selecting which fields will be encrypted and enriched to ensure that the configured MTU size is not exceeded.
- AA ISA does not support header enrichment for WAP1.x, RTSP or SIP headers.
- AA ISA does not support header enrichment for L2 services.

- AA TCP performance measurements cannot co-exist with HTTP enrichment. Enriched flows are ineligible for TCP performance sampling. If a flow is selected for TCP performance measurements and is later enriched, then TCP performance measurements cease to continue.
- Enrichment can be applied as an action to any AQP entry, subject to the following conditions.
 - The matching conditions for the AQPs cannot include a specific HTTP protocol (such as, protocol eq HTTP_video). In other words, applications that require a specific HTTP protocol type (such as video or Flash) are not considered for enrichment.
 - Within the same AQP entry, the enrichment action cannot co-exist with any other AQP action (such as mark or police).
 - The AQP hit counter is not updated based on executing an HTTP enrichment action of an AQP.

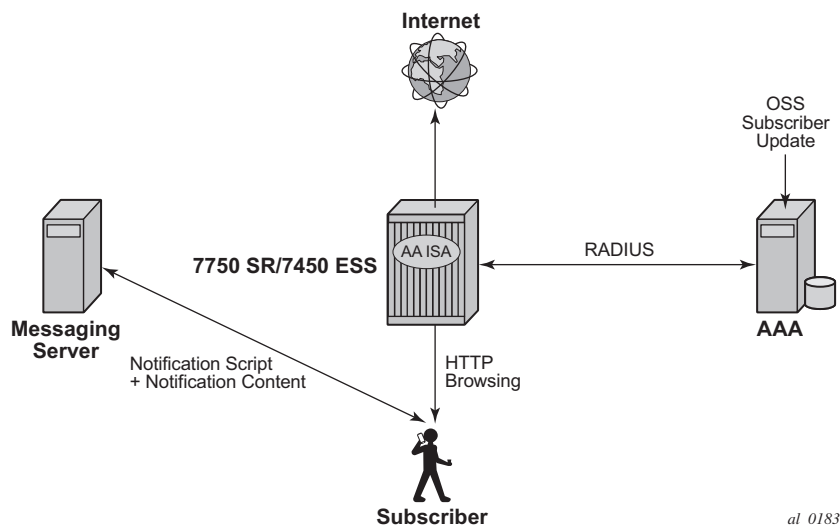
3.2.2.4.11 HTTP In Browser Notification

The AA ISA HTTP notification policy-based feature enables the operator to send in browser notification messages to their subscribers. The notification format can either be an overlay, a web banner, or a splash page, which makes HTTP notification less disruptive than standard HTTP redirection for the subscriber; both the original content and the notification message can be displayed at the same time while browsing.

There is a wide range of notification use cases in Broadband and WiFi networks to use this functionality such as fair use policy threshold warning, marketing and monetization messages, late bill payment notice, copyright infringement notice and operational outages.

The solution is based on two primary components, the AA ISA responsible for specific packet manipulation and a messaging server. The messaging server controls the message format and its content while the AA ISA modifies selected HTTP flows so that the subscriber transparently downloads a script located on the messaging server. This script is then executed by the web browser to display the notification message. The AA ISA only select specific HTTP request flows meeting the criteria of a web browser session compatible with in browser notification messages.

A high level view of the typical network elements involved in HTTP in browser notifications are describe in [Figure 33](#):

Figure 33 HTTP in Browser Notification - High Level

The AA ISA provides full subscriber control to configure an AQP action enabling HTTP notification policy based on specific app-profiles attributes (ASO characteristics), application, or application group. The operator can dynamically modify the subscriber policy from the policy manager to enable or disable HTTP notification during the lifetime of the subscriber.

Notification Interval

The notification can be configured to be displayed either once during the lifetime of the subscriber or at configured minimum interval (in minutes). When an interval in minutes is selected, the subscriber continues to receive notifications messages while browsing.

Success Verification

The system identifies successful and failed notifications. In the event the notification is not successful, the system automatically retries notifying the subscriber at the next flow that meets the criteria of a web browser session.

HTTP Notification Example

To illustrate how HTTP notification works, the steps below describe a typical usage quota notification example with a subscriber reaching its monthly quota:

- AAA identifies that a particular subscriber is now over its quota.
- A Radius CoA message is sent from the AAA to the 7750 SR to modify the subscriber app-profile in order to enable HTTP notification.

- The AA ISA modifies the subscriber profile and enable HTTP notification for this subscriber.
- The notification message is displayed in the subscriber web browser while browsing (in the form of an overlay or web banner). The content of the notification includes a link to the operator web portal to acknowledge the reception of the overage notification.
- Until the subscriber clicks on the acknowledgment link, the AA ISA will continue to execute the same policy so that notification messages are displayed in the subscriber web browser at the configured interval.
- Once the subscriber has clicked on the link provided in the notification message, the provider OSS system updates the AAA which then sends a new CoA message to the 7750 SR in order to modify the subscriber app-profile.
- The AA ISA modifies the subscriber app-profile and disables HTTP notifications for this subscriber.

HTTP Notification Customization through Radius VSA

The operator can customize the notification message per subscriber through the use a new radius VSA returned either at the subscriber creation time or within a CoA. This new VSA is a string appended automatically at the end of the script-url request made by the subscriber towards the messaging server, and it is not interpreted by the AA ISA. When received by the messaging server, it can be used to return specific content to the subscriber.

As an example, the HTTP Notification can be customized using the RADIUS VSA to display location based information, and the messaging server can use this data to display content based on the desired location:

- Alc-AA-Sub-Http-Url-Param RADIUS VSA: location=SohoStation
- Configured Script-URL: `http://10.1.1.1/notification.js`
- Subscriber HTTP request to the messaging server:
`http://10.1.1.1/notification.js?subId=<aa-subscriber-id>&VSA=&location=Soho Station`

3.2.2.5 Application Assurance Firewall

The Application Assurance firewall (FW) feature extends AA ISA application level analysis to provide an in-line integrated stateful service that protects subscribers from malicious security attacks. Using the AA stateful packet filtering feature combined with AA Layer 7 classifications and control empowers operators with advanced, next generation firewall functionalities that integrated are within. AA stateful firewall and application firewall run on the AA ISA. In a stateful inspection,

the AA FW does not only inspect packets at Layers 3 — 7, but also monitors and keeps track of the connection's state. If the operator configures a “deny” action within a session filter then the matching packets (matching both the AQP and associated session filter match conditions) are dropped and no flow session state/context is created.

AA FW can be used in all deployments of AA ISA:

- BNG (ESM)
- WLAN Gateway (ESM or DSM)
- Transit-subscriber
- Business AA.

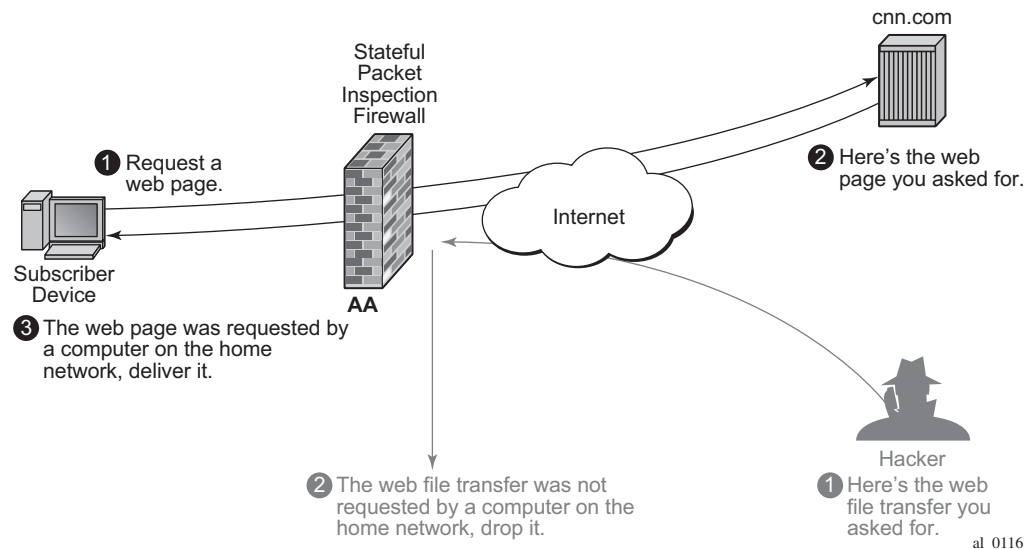
AA FW enabled solution provides:

- [Stateful /Stateless Packet Filtering and Inspection with Application-Level Gateway \(ALG\) Support](#)
- Security Gateway — [SeGW Firewall Protection](#) S1-MME (SCTP), S1-U (GTP-U) and OAM traffic protection.

Stateful /Stateless Packet Filtering and Inspection with Application-Level Gateway (ALG) Support

Stateful flow processing and inspection utilizes IP Layers 3/4 header information to build a state of the flow within AA ISA. Layer 7 inspection is used in order to provide ALG support. Stateful flow/session processing takes note of the originator of the session and hence can allow traffic to be initiated from the subscriber while denying, if configured, traffic originating from the network. Packets received from the network are inspected against the session filter and only those that are part of a subscriber-initiated-session are allowed.

Figure 34 Stateful Firewall



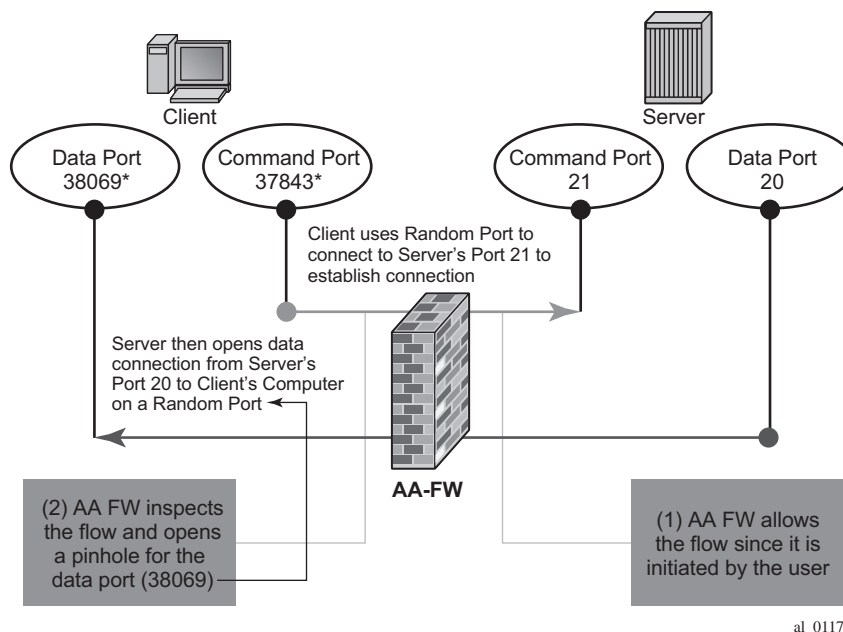
Stateless packet filtering does not take note of session initiator and hence, it discards or allows packets independent of the any previous packets. Stateless packet filtering can be performed in the system using IOM ACLs.

AA FW inspection of packets at Layer 7 offers Application Layer Gateway functionality for the following applications:

- rtsp
- sip
- h323 (IPv4 only)
- googletalkvoice
- ftp
- tftp
- pptp
- citrix
- sybase
- msexchange
- skinny
- ares
- bittorrent
- dns

- irc
- mailru
- qvod
- R commands
- sc2
- socks
- vudu
- winmx
- xunlei

Figure 35 Application Layer Gateway Support



These applications make use of control channels and flows that spun other flows. AA FW inspects the payload of these control flows so that it can open a pinhole for the associated required flows.

3.2.2.5.1 Denial of Service (DoS) Protection

DoS attacks work by consuming network and system resources, making them unavailable for legitimate network applications. Network flooding attacks, malformed packets, and port scans are examples of such DoS attacks.

The aim of AA FW DoS protection is to protect subscribers and prevent any abuse of network resources.

Using AA FW stateful session filters, operators can protect their subscribers from any port scan scheme by configuring the session filters to disallow any traffic that is initiated from the network.

Furthermore, AA ISA provides configurable flow policers. These policers, once configured prevent all sort of flooding attacks (for example, ICMP PING flooding, UDP flooding, SYN Flood Attack). These policers provide protection at multiple levels; per system per application/application groups and per subscriber per applications/applications groups. AA ISA flow policers has two flavors; flow setup rate policers and flow count policers. Flow setup rate policers limit the number of new flows, while flow count policers limit the total number of active flows.

To protect hosts and network resources, AA_FW validates/checks the following parameters, if any fails, it declares the packet to be invalid (/Errored):

- IP layer Validation:
 - IP version is not 4 nor 6
 - Checksum error (IPv4)
 - Header length check
 - Packet length check
 - TTL/Hop limit (not equal to zero) check
 - fragment offset check (teardrop and ping of death protection)
- class D/E (>=224.0.0.0)
- BCAST 255.255.255.255 (multicast source address)
- 127.x.x.x (invalid source address)
- invalid subnet (subnet, 0) [unless /31 point-to-point interface]
- invalid subnet multicast (subnet, -1) unless /31 point-to-point interface
 - IPv4 destination address checks:
- BCAST 255.255.255.255, 0.x.x.x, 127.x.x.x
 - IPv6_source address check
- multicast source address (FFxx:xxxx:.....:xxxx)
 - IPv6_destination address check
- invalid destination address (=:)
- TCP/UDP validation:
 - header checksum
 - Source or destination ports (not equal to zero) check
(only dest port is checked for UDP)

– Invalid TCP flags:

- TCP FIN Only: only the FIN flag set
- TCP No Flags: no flags are set
- TCP FIN RST: both FIN and RST are set
- TCP SYN URG: both SYN and URG are set
- TCP SYN RST: both SYN and RST are set
- TCP SYN FIN: both SYN and FIN are set
- Validates that the first packet of a TCP flow does not contain RST or FIN flags

The above complements ESM enhanced security features, such as IP (or mac) anti-spoofing protection (for example, protecting against “LAND attack”) and network protocols DoS protections. The combination provides a world class carrier grade FW function.

3.2.2.5.2 TCP Validation

Operators can configure AA AQP actions to monitor TCP packet exchanges and ensure that they follow TCP handshake procedures. AA drops packets that do not conform to these procedures. AA FW checks for corrupted TCP packets and invalid TCP flag settings for the different TCP session states.

For example, if the SACK Permitted or MSS option is detected, but the calculated option length is incorrect, AA flags the packet as malformed and drops it. TCP sessions that start without a SYN and packets received after a FIN are discarded as well.

Furthermore, if strict **tcp-validation** is configured, AA checks and drops TCP packets with invalid sequence or acknowledgment numbers.

Drops due to TCP validation policies are recorded under permit-deny statistics. Therefore, TCAs can be configured against these statistics. Optionally, the operator can also capture TCP validation drop activity by enabling event logging.

3.2.2.5.3 Policy Partitioned AA FW

AA FW can provide up to 128 virtual/partitioned FWs, each with its own FW policies. This is achieved through the use of AA-Partitions. Different VPNs can have different FW policies/rules.

3.2.2.5.4 Configuring AA FW

AA ISA AQPs are enhanced with few new AQP actions that provide session filtering functionality. As is the case of AQPs, these have partition level scope. This allows different FW policies to be implemented by utilizing AA partitions concepts within the same AA ISA group. Hence, multiple virtual AA FW instances can be realized. There is no need for multiple physical instances of FWs to implement different FW policies.

The AA FW stateful session filter consists of multiple entries (similar to ACLs) with a **match** and **action** per entry. Actions are **deny** or **permit**. A **deny** action results in packets discarded without creating a session /flow context. **match** conditions include IP 5 tuples info. An overall default action is also configurable, in case of a no match to any session filter entry.

AQPs with session filter actions, need to have, as a matching condition, traffic direction, ASOs and/or subscriber name. It cannot have any references to applications and/or application groups.

AA FW offers, in addition to session-filter actions, a variety of AQP actions to that are aimed to allow or deny: errored/malformed packets, fragmented packets and/or first packet out-of-order fragments and overload traffic.

Statistics are incremented when packets are dropped by a session filter. These are accounted against:

- protocol = denied by default policy,
- application= unknown,
- application group = unknown.

A session-filter hit-count counter is maintained by AA ISA and can be viewed via CLI. There is no current support for export of session-filter entry hit counters via XML to SAM.

3.2.2.5.5 AA FW Logging

AA ISA can be configured, per AQP or per session filter, to log events related to how the packets are processed (either allowed or denied). AA supports event logging locally on the node or remotely via syslog. AA ISA FW logs contain the following information:

- Group partition
- Timestamp
- 5-tuple

- Direction
- Subscriber info (if available)
- Log source/type (session-filter or AQP)
- Action (allow/drop)
- Session-filter specific
 - Session-filter name
 - Session-filter entry
- AQP specific
 - Drop reason
 - Fragment offset (if applicable)
 - Fragment ID (if applicable)
 - TCP validation policy (if applicable)
- If an out of order fragment triggers the log, then whatever 5-tuple information is available is included.

For AQPs, only **drop** events are captured in the log. The logs do not capture drops due to flow policers.

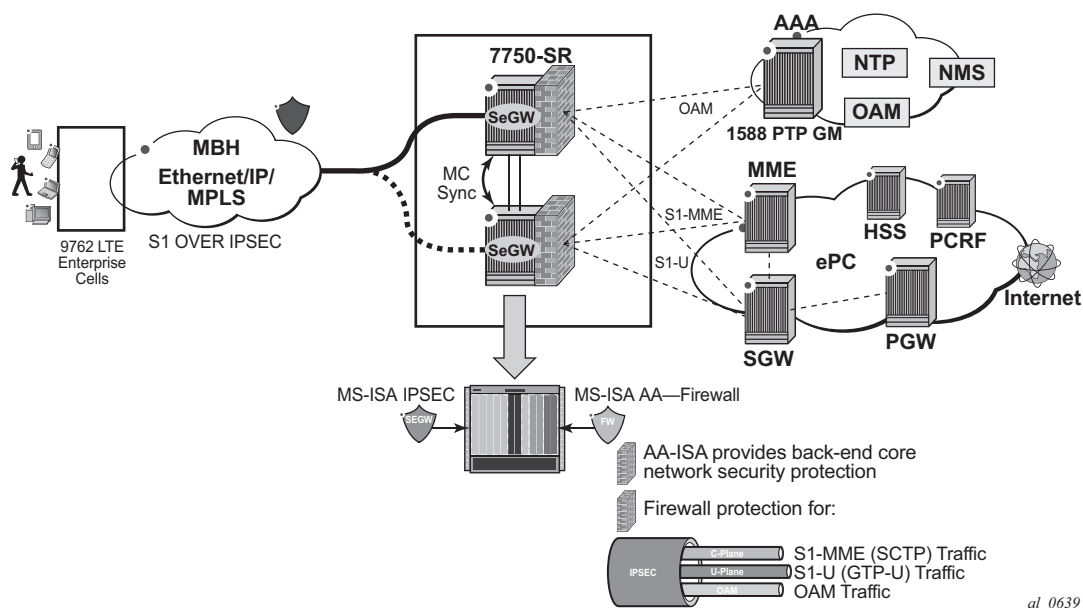
The operator can configure up to one event log per partition. For offline logging via syslog, the operator needs to configure the IP address of the syslog server and the VLAN ID to be used to connect to the server.

3.2.2.5.6 SeGW Firewall Protection

The 7750 SR SeGW with Application Assurance Firewall (AA FW) deployed in 3G/4G/Femto access networks provides the operator with back-end core network security protection. AA FW provides protection for:

1. S1-MME (SCTP) traffic
2. S1- U (GTP-U) traffic
3. OAM traffic

Figure 36 SeGW Firewall Deployment



SAPs on the private side of Tunnel ISA are diverted to AA for firewall protection. If per eNB/ Femto Access Point (FAP) control is desired, then AA auto-configures/instantiate subscribers based on the “seen-ip” transit-AA subscriber model (no RADIUS interaction is required). This auto-creates a subscriber per eNB/FAP. Alternatively, AA applies firewall rules to the diverted SAP (for all eNBs/FAPs) at the aggregate level (for all eNBs/FAPs).

One AA ISA is supported per Tunnel-ISA group. Therefore, all private side SAPs that are diverted to AA for Firewalling service go to the same AA ISA module with no need to load balance the traffic into different AA ISAs. If the capacity of one AA ISA is not sufficient, then the IPsec tunnel group is split into two (or more) groups. Each group is served by an AA ISA.

OAM Traffic Protection

The aim of AA Firewall protection is to protect and prevent any abuse of OAM network resources (such as NMS).

Network flooding attacks, malformed packets and port scans are examples of such attacks that can be carried out using a compromised eNB/Femto Access Points (FAP).

Ports Scan attacks: Using AA FW stateful session filters, operators can allow traffic only on certain IP addresses and port numbers.

1. **Ports Scan Attacks:** Using AA FW stateful session filters, operators can allow traffic only on certain IP addresses and port numbers.
 - For example, operator can configure AA to only allow traffic that is initiated by NMS towards the FAPs. Hence, a compromised FAP cannot initiate an attack on NMS infrastructure.
 - Operator can limit the type of traffic allowed based on L3 — L7 classification. Operator can allow only HTTP with a certain URL/domain, DNS, PTP, FTP (independent of the port number used) and block all other traffic.
2. **Flood Attacks:** The operator can limit the type of traffic allowed based on Layer 3 — Layer 7 classification. The operator can allow only HTTP with a certain URL/domain, DNS, PTP, FTP. The AA ISA provides configurable flow policers that can act on FW permitted sessions. These policers, once configured prevent all sort of flooding attacks, such as ICMP PING flooding, UDP flooding, SYN Flood Attack, and so on, of the port number used) and block all other traffic.
 - These policers provide protection at multiple levels; per system per application/application groups and per FAP (or per NMS) per applications/applications groups.
 - There are three types of AA ISA policers:
 - Flow setup rate policers to limit the number of new flows.
 - Flow count policers to limit the total number of active flows.
 - Bandwidth policers to limit the total OAM bandwidth allowed by a given FAP towards NMS.
3. **Malformed Packets Attacks:** In order to protect Hosts and network resources, AA FW performs validation on IP packets, at the IP layer and TCP/UDP layer, to ensure that the packets are valid. Invalid packets are discarded (a configurable option). This provides protection against well-known attacks such as LAND attack. See [SeGW Firewall Service](#) for a complete description. AA allows the operator to optionally drop fragmented or out-of-order fragmented IP packets.

In addition, for OAM traffic, all AA functionalities including Layer 7 analytics and control as well as Application Layer Gateway (ALG) are supported.

For more details on OAM Traffic protection, refer to the [Stateful /Stateless Packet Filtering and Inspection with Application-Level Gateway \(ALG\) Support](#) and [Denial of Service \(DoS\) Protection](#) sections.

S1- MME (SCTP) Firewall

Network flooding attacks, malformed packets and port scans are examples of DoS attacks that can be carried out using a compromised eNB/FAP. AA FW provides inspection of SCTP (the protocol used to communicate to MME). Such inspection includes checking for SCTP protocol Id, source/destination ports, PPID, SCTP chunk checking and malformed SCTP packet (such as checksum validation).

SCTP chunk checking includes checking for:

- Invalid length values. Frames with invalid length value are dropped regardless of the chunk type.
- Data chunks with length value that is too small to accommodate PPID. Such frames are dropped as invalid/badly formed.
- Data chunks with length value that is too large for chunk. Such frames are dropped as invalid/badly-formed.

For S1-MME traffic, the operator can configure various AA actions:

- Drop packets with invalid checksum, src/dest IP and/or port numbers (malformed Packet protection) by appropriately configuring session filters and /or **error-drop [event-log <event-log-name>] AQP action** command.
- PPID Filtering, using SCTP-Filter command
- Rate limit the amount of S1-MME traffic (flooding protection) in terms of Bandwidth (bits/sec), using AA bandwidth policers.
- Limit the number of concurrent SCTP flows (flooding protection) using AA flow count policers.
- Limit the SCTP flow setup rate (flows/sec) to protect against DoS flooding using AA flow rate policers.
- Drop fragmented packets or drop out of order fragmented packets using the **fragment-drop {all | out-of-order} AQP action** command.

The actions above can be applied per eNB/FAP IP address and/or per MME (to control aggregate traffic per MME).

SCTP PPID Filtering

AA allows the operator to configure PPID filters that contain a list of PPIDs to allow or deny.

```
config>app-assure>group <aa-group-id>[:<partition>]
    sctp-filter <sctp-filter-name> [create]
        description <description-string>
        no description
```

```

event-log <event-log-name>
no event-log
ppid-range min <min-ppid> max <max-ppid>    //[0..4294967295]
no ppid-range
ppid
    default-action {permit | deny}
    entry <entry-id> value <ppid-value> action {permit | deny}
        //<entry-id> : [1..255]
            <ppid-value>      : [0..4294967295]D | [256 chars max]
            <permit | deny> : permit | deny
    no value <entry-id>
no sctp-filter <sctp-filter-name>

```

The filter can then be used within an AQP action.

AA identifies DATA chunks within SCTP payloads (for example, as first, nth or last chunk) and filters according to the configured PPID filter. If any chunk PPID matches a PPID on the configured blocked PPID list, the whole SCTP packet is dropped.

SCTP packets without DATA chunks are not impacted or accounted for by an SCTP Filter.

For IP fragmentation, and in the case where the operator did not configure AA ISA to drop “all fragmented traffic”, only the first IP fragment is inspected and subject to the PPID filtering. Any action applied to the first fragment is also applied to the remaining fragments. Out-of-order fragments appearing before the first fragment receive the default action (for example, drop action of “out-of-order-Frag”).

S1-U GTP Traffic Protection

The 7750 SR SeGW with AA FW provides protection of SGW/SGSN infrastructure against an attack from a compromised eNB/FAP. AA FW supports:

1. Protection against malformed GTP packets attack:

For GTP-v1 traffic carried over UDP port number port 2152, AA performs various packet sanity checks, such as:

- UDP destination port is 2152
- Version: GTP-U should always be version 1.
- Protocol Type bit should be 1
- Invalid/Missing Mandatory Header Fields
- Invalid Optional/Spare Header Fields
- Invalid/Missing Header Extensions
- Invalid Length

For S1-U interface, only GTP-v1 is supported. No support for GTP-v2 (as there is no signaling on S1-U interface).

Details of the various GTP sanity checks that are performed for different GTP-U message types are shown in [Table 17](#):

Table 17 GTP-U Message Types

Payload Size	Encapsulated Data Checks	IE Checks	Header Extension Checks	Optional HEADER Check	GTP Mandatory Header Checks					
				If E, S or PN =1	Length	TEID	Spare	PT	version	
>0	PayloadSize is assumed to be the size of the remainder of the packet, unless the packet is fragmented. No checking of the encapsulated data	No checks	Valid types = Service Class Indicator & • PDCP PDU Number Extension size= 4*# of extensions	OptionalSize = 8 If E=0, ExtSize = 0	Optional Size + ExtensionSize + Payload Size	<>0	0	1	1	G-PDU (Encapsulated Data Delivery) – Message Type 255
	No payload after the IEs	Only private extensions are allowed.	No external header allowed.	No optional headers allowed.	IE Size	0	0	1		Echo Request – Message Type 1

Table 17 **GTP-U Message Types (Continued)**

Payload Size	Encapsulated Data Checks	IE Checks	Header Extension Checks	Optional HEADER Check	GTP Mandatory Header Checks					
				If E, S or PN = 1	Length	TEID	Spare	PT	version	
	No payload after the IEs	Recovery ID is present Private extensions allowed.	No external header allowed.	No optional headers allowed.	IE Size	0	0	1	1	Echo Response – Message Type 2
	No payload after the IEs	Extension Header Type List IE is present Private extensions allowed No checking on the extension header value	No external header allowed.	No optional headers allowed.	IE Size	0	0	0	1	Supported Extension Headers Notification - Message Type 31

Table 17 GTP-U Message Types (Continued)

Payload Size	Encapsulated Data Checks	IE Checks	Header Extension Checks	Optional HEADER Check	GTP Mandatory Header Checks					
				If E, S or PN =1	Length	TEID	Spare	PT	version	
	No payload after the IEs	TEID IE & GTP-U Peer Address IE are present IE type and length are verified Private extensions allowed	Only the UDP Port Extension Header is valid	Option Size = 8	Optional Size + ExtensionSize + IESize	<>0	0	1	1	Error Indication – Message Type 26
	No payload after the IEs	Only Private extensions are allowed	no valid external header allowed.	Option alSize = 8 IF E = 0, ExtSize = 0	IE Size	<>0	0	1	1	End Marker – Message Type 254

To enable GTP packet sanity checks, the operator must configure:

```
config>app-assure>group <aa-group-id>[:<partition>]
```

Once the **gtp** command is issued for a partition, AA treats traffic with UDP destination port number 2152 as GTP. It applies the different GTP level firewall functions as configured by the operator. However, it does not look beyond the GTP header for further inner L3-L7 packet classifications and actions. For example, Ipfix record for GTP traffic contains the 5 tuples of the GTP-u tunnel (eNB, SGW IPs and port numbers, and so on, no TEID).

2. Protection against unsupported GTP messages
3. AA allows the operator to configure a GTP filter to indicate which GTP message types are to be allowed/denied as well as the maximum allowed GTP message length:

```
config>app-assure>group <aa-group-id>[:<partition>]>gtp
  gtp-filter <gtp-filter-name> [create]
    max-payload-length <bytes> // [0..65535]
    message-type
    default-action {permit|deny}
    entry <entry-id> value <gtp-message-value> action {permit|deny}
```

4. There are approximately 67 valid message names to enter in the above GTP filter. Both names and numbers are accepted as input (for user convenience), but the CLI info will always show the name:

echo-request, echo-response, error-indication, g-pdu, end-marker and supported-extension-headers-notification.

5. Once a GTP filter is configured, it can then be included as an AQP action:

```
config>app-assure>group <aa-group-id>[:<partition>]> policy
  app-qos-policy
    entry <entry-id> [create]
      action
        gtp-filter <gtp-filter-name>
```

6. Extensive GTP header sanity checks (included in [Table 17](#)) that are based on different GTP message types are only performed when these GTP messages are permitted by the GTP filter. If no GTP filter is configured, then no extensive GTP-U header checks are performed. In other words, if the operator wants to allow all GTP-U packets and perform all GTP header sanity checks, then the operator needs to configure a GTP filter with default action of **permit** and no values, such as:

```
config>app-assure>group 1:100> gtp
  gtp-filter "allow-all" create
    message-type
    default-action permit
```

7. Protection against flooding attack:

AA can be configured to drop all fragments and/or out of order fragments, using AQP action: **fragment-drop {all | out-of-order}**

8. In the case that the IP **fragment-drop** command is not set, then the following conditions apply to the way AA inspects GTP traffic:

- Permit/deny decisions are entirely based on the first fragment. The first fragment contains the entire GTP header in almost all of the cases.
- Max packet length check is not done across fragments. Only the first fragment length is checked. In other words, AA ISA may permit a packet that is larger than the max packet allowed if it is fragmented, with the first fragment smaller than the configured maximum packet size allowed.
- First fragmented packet is discarded (and logged), as well as subsequent fragments:
 - If the first packet is too small to contain the mandatory header (12 bytes, ending with the TEID).
 - If the mandatory header indicates there should be an optional header, and the fragment is too small to contain the optional header (mandatory + optional = 16 bytes).

3.2.3 Service Monitoring and Debugging

Operators can use AA-specific tools in addition to system tools that allow them to monitor, adjust, debug AA services. The following are examples of some of the available functions:

- Display and monitor AA ISA group status and statistics (AA ISA status and capacity planning/monitoring).
- Clear AA ISA group statistics (clears all system and per-AA subscriber statistics).
- Special study mode for real-time monitoring of AA subscriber traffic (ESM or transit subscriber, SAP or spoke SDP).
- Display per AQP entry statistics for number of hits (flow matching the entry) and conflicts (actions ignored due to per-flow-action-limit exceeded).
- Mirror (all or any subset of traffic seen by an AA ISA group).
- Display all the per-ISA statistics from the aa-performance record, for examining resource loading of each ISA
- Display the top active AA subscribers per ISA by bytes, packets or flows, for traffic in each direction

3.2.4 CPU Utilization

The ISA show status command displays per ISA CPU utilization by main tasks, to provide insight into what aspects of load may be loading the ISA. These are split into 2 main areas:

- Management CPU, which includes all tasks related to communication between the CPM and the ISA, with the following usage percentage reported:
 - System — Various infrastructure and overhead work
 - Management — Managing AA policy, AA subscriber and trap configurations and handling tools requests
 - Statistics — Collecting and reporting statistics and Cflowd reporting
 - Idle
- Datapath CPUs, which includes all tasks related to datapath packet and flow processing on the ISA, with the following usage percentage reported:
 - System — Various infrastructure and overhead work
 - Packet processing — Receiving, associating with flows, applying application QoS policy and transmitting
 - Application ID — Using protocol signatures and other techniques to identify application/app-group and determine the application QoS policy

3.2.5 CLI Batch: Begin, Commit and Abort Commands

The Application Assurance uses CLI batch capability in policy definition. To start editing a policy, a begin command must be executed. To finish editing either abort (discard all changes) or commit (accept all changes) needs to be executed. CLI batch state is preserved on an HA activity switch.

To enter the mode to create or edit policies, the **begin** keyword must be entered at the prompt. Other editing commands include:

- The **commit** command saves changes made to policies during a session. The newly committed policy takes effect immediately for all new flows. Existing flows will transition onto the new policy shortly after the commit.
- The **abort** command discards changes that have been made to policies during a session.

To allow flexible order for policy editing, the **policy>commit** function cross references policy components to verify, among others:

- Whether all ASO characteristics have a default value and are defined in the app-profile.
- Checks whether limits are adhered.

3.3 Configuring Application Assurance with CLI

This section provides information to configure Application Assurance entities using the command line interface. It is assumed that the user is familiar with basic configuration of policies.

3.3.1 Provisioning AA ISA MDA

The following illustrates syntax to provision AA ISA and configure ingress IOM QoS parameters. (The egress IOM QoS is configured in the **config>isa>application-assurance-grp>qos** context.)

CLI Syntax:

```
config>card>mda mda-slot
mda-type isa-aa
network
    ingress
        pool
            slope-policy slope-policy-name
            resv-cbs percent-or-default
            queue-policy network-queue-policy-name
```

The following output displays an AA ISA configuration example.

```
*A:cpm-a>config>app-assure# show mda 1/1
=====
MDA 1/1
=====
Slot  Mda   Provisioned      Equipped          Admin   Operational
      Mda   Mda-type         Mda-type          State   State
-----
1     1     isa-aa           isa-ms up         up
=====
*A:cpm-a>config>app-assure#

*A:cpm-a>config>card# info
-----
card-type iom3-xp-c
mda 1
mda-type isa-aa
exit
-----
*A:cpm-a>config>card#
```

3.3.2 Configuring an AA ISA Group

To enable AA on the router:

- Create an AA ISA group.
- Assign active and optional backup AA ISAs to an AA ISA group.
- Select the forwarding classes to divert.
- Enable the group.
- Optionally:
 - Enable group policy partitioning
 - Configure capacity cost threshold values
 - Configure the number of transit prefix IP policies
 - Configure IOM egress queues to the MS-ISA
 - Enable overload cut through and configure the high and low watermarks values
 - Configure performance statistics accounting

The following example illustrates AA ISA group configuration with:

- Primary AA ISA and warm redundancy provided by the backup AA ISA.
- “fail-to-wire” behavior configured on group failure.
- BE forwarding class selected for divert.
- Default IOM QoS for logical ISA egress ports. The ISA ingress QoS is configured as part of ISA provisioning (**config>card>mda>network>ingress>qos**).

The following commands illustrate AA ISA group configuration context.

CLI Syntax:

```

config>isa>application-assurance-group isa-aa-group-id
    [aa-sub-scale {residential | vpn}] [create]
    backup mda-id
    description description
    divert-fc fc-name
    no fail-to-open
    isa-capacity-cost-high-threshold threshold
    isa-capacity-cost-low-threshold threshold
    partitions
    primary mda-id
    qos
        egress
            from-subscriber
                pool [pool-name]
                resv-cbs percent-or-default
                slope-policy slope-policy-name
  
```

```

port-scheduler-policy port-scheduler-policy-
name
queue-policy network-queue-policy-name
to-subscriber
    pool [pool-name]
        resv-cbs percent-or-default
        slope-policy slope-policy-name
port-scheduler-policy port-scheduler-
policy-name
queue-policy network-queue-policy-name
[no] shutdown

```

The following output displays an AA ISA group configuration example.

```

A:ALU-A>config>isa>aa-grp# info detail
-----
no description
primary 1/2
backup 2/2
no fail-to-open
isa-capacity-cost-high-threshold 4294967295
isa-capacity-cost-low-threshold 0
no partitions
divert-fc be
qos
    egress
        from-subscriber
            pool
                slope-policy "default"
                resv-cbs default
            exit
            queue-policy "default"
            no port-scheduler-policy
        exit
    to-subscriber
        pool
            slope-policy "default"
            resv-cbs default
        exit
        queue-policy "default"
        no port-scheduler-policy
    exit
exit
no shutdown
-----
A:ALU-A>config>isa>aa-grp#

```

3.3.2.1 Configuring Watermark Parameters

Use the following CLI syntax to configure thresholds for logs and traps when under high consumption of the flow table. The flow table has a limited size and these thresholds can be established to alert the user that the table is approaching capacity. These flow table watermarks represent number of flow contexts allocated on the ISA, which will be slightly higher than the actual number of existing flows at the point when the watermark is reached.

The low threshold is used while the high threshold is used as an alarm.

CLI Syntax:

```
config>application-assurance
      flow-table-high-wmark high-watermark
      flow-table-low-wmark low-watermark
```

3.3.3 Configuring a Group Policy

3.3.3.1 Beginning and Committing a Policy Configuration

To enter the mode to create or edit Application Assurance policies, you must enter the **begin** keyword at the **config>app-assure>group>policy** prompt. The **commit** command saves changes made to policies during a session. Changes do not take effect in the system until they have performed the commit function. The **abort** command discards changes that have been made to policies during a session.

The following error message displays when creating or modifying a policy without entering **begin** first.

```
A:ALA-B>config>app-assure>group>policy#
MINOR: AA #1005 Invalid Set - Cannot proceed with changes when in non-edit mode
```

There are no default policy options. All parameters must be explicitly configured.

Use the following CLI syntax to begin a policy configuration.

CLI Syntax:

```
config>app-assure# group group-id
policy
begin
```

Use the following CLI syntax to commit a policy configuration.

CLI Syntax:

```
config>app-assure# group group-id
policy
```

commit

3.3.3.2 Aborting a Policy Configuration

Use the following CLI syntax to abort a policy configuration.

CLI Syntax: config>app-assure# group *group-id*
policy
abort

3.3.3.3 Configuring an IP Prefix List

An operator can use IP lists to define a list of IP addresses (along with any masks). This list can be later referenced in AQPs, application filters and/or session-filters.

Use the following CLI syntax to configure an application filter entry.

CLI Syntax: config>aa>group>policy>app-assurance>group <aa-group-id>[:<partition>]
ip-prefix-list <prefix-list-name> [create]
no ip-prefix-list <prefix-list-name>
description <description>
no description
prefix <address/mask> [name <prefix-name>]
no prefix <address/mask>

```
*A:Dut-A>config>app-assure>group# ip-prefix-list AllowedLan1Hosts create
*A:Dut-A>config>app-assure>group>pfx>$ description "allowed hosts"
*A:Dut-A>config>app-assure>group>pfx>$ prefix 10.10.8.2/32
*A:Dut-A>config>app-assure>group>pfx>$ prefix 10.10.8.180/32
*A:Dut-A>config>app-assure>group>pfx>$ prefix 10.10.8.231/32
*A:Dut-A>config>app-assure>group>pfx>$ exit
*A:Dut-A>config>app-assure>group#
```

```
*A:Dut-A>config>app-assure>group# ip-prefix-list "AllowedLan1Hosts"
*A:Dut-A>config>app-assure>group>pfx># info
-----
description "allowed hosts"
prefix 10.10.8.2/32
prefix 10.10.8.180/32
prefix 10.10.8.231/32
-----
*A:Dut-A>config>app-assure>group>pfx>#
```

3.3.3.4 Configuring AA Session Filters

Session filters can be configured to allow stateful firewall use-cases. Refer to [AA Group Commands](#) for syntax and CLI descriptions.

CLI Syntax:

```
*A:Dut-A>config>app-assure>group# session-filter
  <session-filter-name> [create]
  default-action {permit | deny} [event-log <event-log-
    name>]
  description <description-string>
  entry <entry-id> [create]
    action {permit | deny} [event-log <event-log-
      name>]
    match
      dst-ip <ip-address>
      dst-ip ip-prefix-list <ip-prefix-list-
        name>
      no dst-ip
      dst-port {eq | gt | lt} <port-num>
      dst-port range <start-port-num> <end-
        port-num>
      dst-port port-list <port-list-name>
      no dst-port
      ip-protocol-num <ip-protocol-number>
      no ip-protocol-num
      src-ip <ip-address>
      no src-ip
      src-ip ip-prefix-list <ip-prefix-list>
      src-port {eq | gt | lt} <port-num>
      src-port range <start-port-num> <end-
        port-num>
      src-port port-list <port-list-name>
      no src-port
```

```
*A:Dut-A>config>app-assure>group# session-filter " denyUnsolicitedwMgntCntrl" create
  description "S-FW opted-in sub - allow ISP access"
  default-action deny event-log "FW_log"
  entry 10 create
    description "allow ICMP access from ISP LAN#1"
    match
      ip-protocol-num icmp
      src-ip 10.10.8.0/24
    exit
    action permit
  exit
  entry 30 create
    description "allow all TCP (e.g. FTP/telnet)access from ISP LAN#2"
    match
      ip-protocol-num tcp
      src-ip 192.168.0.0/24
    exit
```

```

        action permit
    entry 40 create
        description "allow TCP on port 80 /HTTP access from a IP List on ISP LAN#1"
        match
            ip-protocol-num tcp
            src-ip ip-prefix-list AllowedLAN1Hosts
            dst-port eq 80
        exit
        action permit

    exit

*A:Dut-A>config>app-assure>group>sess-fltr$ info
-----
        description "S-FW opted-in sub . allow ISP access"
        default-action deny event-log "FW_Log"
        entry 10 create
            description "allow ICMP access from ISP LAN#1"
            match
                ip-protocol-num icmp
                src-ip 10.10.8.0/24
            exit
            action permit
        exit
        entry 20 create
            description "allow ICMP access from ISP LAN#2"
            action deny
        exit
        entry 30 create
            description "allow all TCP (e.g. FTP/
telnet)access from ISP LAN#2"
            match
                ip-protocol-num tcp
                src-ip 192.168.0.0/24
            exit
            action permit
        exit
        entry 40 create
            description "allow TCP on port 80 /
HTTP access from a IP List on
ISP LAN#1"
            match
                ip-protocol-num tcp
                src-ip ip-prefix-list "AllowedLan1Hosts"
                dst-port eq 80
            exit
            action permit
        exit

-----

*A:Dut-A>config>app-assure>group>sess-fltr$

*A:Dut-A>config>app-assure>group>policy>eqp>
    entry 110 create
        description "FW for managed opted-in subs"
        match

```

```

        traffic-direction network-to-subscriber
    exit
    action
        session-filter " denyUnsolicitedwMgmtCntrl "
        fragment-drop all event-log "FW_log"
        error-drop event-log "FW_log"
        overload-drop

    exit
exit

*A:Dut-A>config>app-assure>group>policy>aqp>entry# info
-----
        description "FW for managed opted-in subs."
        match
            traffic-direction network-to-subscriber
        exit
        action
            session-filter "denyUnsolicitedwMgmtCntrl"
            fragment-drop all event-log "FW_log"
            error-drop event-log "FW_log"
            overload-drop

        exit
        no shutdown
-----
*A:Dut-A>config>app-assure>group>policy>aqp>entry#

```

3.3.3.5 Configuring an Application Group

An operator can configure an application group to group multiple application into a single application assurance entity by referencing those applications in the group created.

Use the following CLI syntax to configure an application group.

CLI Syntax: `config>app-assure>group>policy# app-group application-group-name [create]`
 `description description`

The following example displays an application group configuration.

```

*A:ALA-48>config>app-assure>group>policy# app-group "Peer to Peer" create
*A:ALA-48>config>app-assure>group>policy>app-grp# info
-----
        description "Peer to Peer file sharing applications"
-----
*A:ALA-48>config>app-assure>group>policy>app-grp#

```


3.3.3.6 Configuring an Application

An operator can configure an application to group multiple protocols, clients or network applications into a single Application Assurance application by referencing it later in the created application filters as display in other sections of this guide.

Use the following CLI syntax to configure an application.

CLI Syntax:

```
config>app-assure>group>policy# application application-name [create]
app-group app-group-name
description description
```

The following example displays an application configuration.

```
*A:ALA-48>config>app-assure>group>policy# application "SQL" create
*A:ALA-48>config>app-assure>group>policy>app# info
-----
description "SQL protocols"
app-group "Business Critical Applications"
-----
*A:ALA-48>config>app-assure>group>policy>app#
```

3.3.3.7 Configuring an Application Filter

An operator can use an application filter to define applications based on ALU protocol signatures and a set of configurable parameters like IP flow setup direction, IP protocol number, server IP address and server TCP/UDP port. An application filter references an application configured as previously shown.

Use the following CLI syntax to configure an application filter entry.

CLI Syntax:

```
config>app-assure>group>policy# app-filter
entry entry-id [create]
application application-name
description description-string
expression expr-index expr-type {eq | neq} expr-string
flow-setup-direction {subscriber-to-network |
network-to-subscriber | both}
http-match-all-requests
ip-protocol-num {eq | neq} protocol-id
network-address {eq | neq} ip-address
network-address {eq | neq} ip-prefix-list ip-prefix-list-name
protocol {eq | neq} protocol-signature-name
server-address {eq | neq} ip-address
```

```

server-address {eq | neq} dns-ip-cache dns-ip-cache-name
server-address {eq | neq} ip-prefix-list ip-prefix-list-name
server-port {eq | neq | gt | lt} server-port-number
server-port {eq | neq} range start-port-num end-port-num
server-port {eq} {port-num | range start-port-num end-port-num} first-packet-trusted | first-packet-validate}
no shutdown

```

The following example displays an application filter configuration.

```

*A:ALA-48>config>app-assure>group>policy>app-filter# entry 30 create
*A:ALA-48>config>app-assure>group>policy>app-filter>entry# info
-----
description "DNS traffic to local server on expected port #5
3"
protocol eq "dns"
flow-setup-direction subscriber-to-network
ip-protocol-num eq *
server-address eq 192.0.2.0/32
server-port eq 53
application "DNS_Local"
no shutdown
-----
*A:ALA-48>config>app-assure>group>policy>app-filter>entry#

```

3.3.3.8 Configuring an Application Profile

Use the following CLI syntax to configure an application profile.

CLI Syntax:

```

config>app-assure>group>policy# app-profile app-profile-name [create]
characteristic characteristic-name value value-name
description description-string
[no] aa-sub-suppressible
divert

```

The following example displays an application profile configuration.

```

*A:ALA-48>config>app-assure>group>policy# app-profile "Super" create
*A:ALA-48>config>app-assure>group>policy>app-prof# info
-----
description "Super User Application Profile"
divert
characteristic "Server" value "Prioritize"
characteristic "ServiceBw" value "SuperUser"

```

```
characteristic "Teleworker" value "Yes"
characteristic "VideoBoost" value "Priority"
-----
*A:ALA-48>config>app-assure>group>policy>app-prof#
```

3.3.3.9 Configuring Suppressible App-Profile with SRRP

For information about SRRP, refer to the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*.

In the context of an ESM SRRP deployment, the operator can define at the app-profile level if the subscriber will be diverted to the ISA-AA card per SRRP group interface. This can be useful to reduce the total number of ISA cards required in the event of a switch-over from a primary to backup SRRP node when AA is used as a value-add service for selected subscribers.

To configure the network for suppressible app-profiles in the context of SRRP the operator needs to:

- Enable the capability to suppress AA subscribers on a given SRRP group interface, typically by selecting backup SRRP group interfaces.
- ESM subscribers with a valid app-profile are diverted to AA by default, to suppress selected group of subscribers using AA for optional value-add services. The operator then specifies which app-profile will be suppressed and therefore not diverted to AA.

Use the following CLI syntax to enable the capability to suppress ESM subscribers from a backup SRRP group interface:

CLI Syntax:

```
config>service>vprn>sub-if>grp-if# suppress-aa-sub
[create]
characteristic characteristic-name value value-name
description description-string
[no] aa-sub-suppressible
divert
```

The following example displays an application profile configuration used for premium subscribers, this type of subscriber will always be diverted to Application Assurance, it is also the default configuration:

```
7750>config>app-assure>group>policy# info
-----
app-profile "Premium" create
characteristic "Parental-Control" eq "Yes"
divert
exit
-----
```

The following example displays an application profile configuration for best effort / value-add subscribers not diverted to Application Assurance on the SRRP group interface configured with “suppress-aa-sub”:

```
7750>config>app-assure>group>policy# info
-----
      app-profile "1-default" create
      divert
      aa-sub-suppressible
      exit
-----
```

3.3.3.10 Configuring Application Service Options

Use the following CLI syntax to configure application service options.

CLI Syntax: config>app-assure>group>policy# app-service-options
 characteristic *characteristic-name* [create]
 default-value *value-name*
 value *value-name*

The following example displays an application service options configuration.

```
*A:ALA-48>config>app-assure>group>policy>aso# info
-----
      characteristic "Server" create
      value "Block"
      value "Permit"
      value "Prioritize"
      default-value "Block"
      exit
      characteristic "ServiceBw" create
      value "Lite_128k"
      value "Power_5M"
      value "Reg_1M"
      value "SuperUser"
      default-value "Reg_1M"
      exit
      characteristic "Teleworker" create
      value "No"
      value "Yes"
      default-value "No"
      exit
      characteristic "VideoBoost" create
      value "No"
      value "Priority"
      default-value "No"
      exit
-----
*A:ALA-48>config>app-assure>group>policy>aso#
```

3.3.3.11 Configuring a Policer

Use the following CLI syntax to configure a policer.

CLI Syntax:

```
config>app-assure>group>policy# policer policer-name
    type type granularity granularity create
    action {priority-mark | permit-deny}
    adaptation-rule pir adaptation-rule
    description description-string
    mbs maximum burst size
    rate pir-rate
    tod-override tod-override-id [create]
```

The following example displays an Application Assurance policer configuration.

```
*A:ALA-48>config>app-assure>group# policer "RegDown_Policer" type dual-bucket-
bandwidth granularity subscriber create

*A:ALA-48>config>app-assure>group>policer# info
-----
description "Control the downstream aggregate bandwidth for Regular
1Mbps subscribers"
rate 1000 cir 500
mbs 100
cbs 50
-----
*A:ALA-48>config>app-assure>group>policer#
```

3.3.3.12 Configuring an Application QoS Policy

Use the following CLI syntax to configure an application QoS policy.

CLI Syntax:

```
config>app-assure>group>policy# app-qos-policy
entry entry-id [create]
    action
        bandwidth-policer policer-name
        drop
        error-drop [event-log event-log-name]
        flow-count-limit policer-name
        flow-rate-limit policer-name
        fragment-drop {all | out-of-order} [event-log
            event-log-name]
        http-error-redirect redirect-name
        mirror-source [all-inclusive] mirror-service-
            id
        overload-drop [event-log event-log-name]
        remark
```

```

        dscp in-profile dscp-name out-profile
            dscp-name
        fc fc-name
        priority priority-level
    url-filter url-filter-name characteristic
        characteristic-name
    description description-string
    match
        aa-sub sap {eq | neq} sap-id
        aa-sub esm {eq | neq} sub-ident-string
        aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
        app-group {eq | neq} application-group-name
        application {eq | neq} application-name
        characteristic characteristic-name {eq} value-
            name
        dscp {eq | neq} dscp-name
        dst-ip {eq | neq} ip-address[/mask]
        dst-ip {eq | neq} ip-prefix-list ip-prefix-
            list-name
        dst-port {eq | neq} port-num
        dst-port {eq | neq} range start-port-num end-
            port-num
        src-ip {eq | neq} ip-address[/mask]
        src-ip {eq | neq} ip-prefix-list ip-prefix-
            list-name
        src-port {eq | neq} port-num
        src-port {eq | neq} range start-port-num end-
            port-num
        traffic-direction {subscriber-to-network |
            network-to-subscriber | both}
    no shutdown

```

The following example displays an application QoS policy configuration.

```

*A:ALA-48>config>app-assure>group>policy>aqp# entry 20 create
-----
s"
        description "Limit downstream bandwidth to Reg_1M subscriber
match
    traffic-direction network-to-subscriber
    characteristic "ServiceBw" eq "Reg_1M"
exit
action
    bandwidth-policer "RegDown_Policer"
exit
no shutdown
-----
*A:ALA-48>config>app-assure>group>policy>aqp#

```

The following example display an AQP entry configuration to mirror all positively identified only P2P traffic (AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled.

```
A:ALA-48>config>app-assure>group>policy>aqp#
-----
entry 100 create
match
  app-group eq P2P
  characteristic aa-sub-mirror eq enabled
exit
action
  # mirror to an existing mirror service id
  mirror-source 100
exit
no shutdown
exit
-----
A:ALA-48>config>app-assure>group>policy>aqp#
```

The following example displays an AQP entry to mirror all P2P traffic (all positively identified P2P traffic and any unidentified traffic that may or may not be P2P - AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled (the order is significant):

```
A:ALA-48>config>app-assure>group>policy>aqp>entry#
-----
entry 100 create
match
  app-group eq P2P
  characteristic aa-sub-mirror value enabled
exit
action
  mirror-source all-inclusive 100
exit
no shutdown
exit
-----
A:ALA-48>config>app-assure>group>policy>aqp#
```

3.3.3.13 Configuring an Application and DNS IP Cache for URL Content Charging Strengthening

In the context of URL content charging, also known as zero rating, the DNS IP cache (**dns-ip-cache** command) feature ensures that only legitimate traffic is classified in a given application and charging-group. Subscribers' DNS responses matching a list of domain names used for content charging populate the DNS IP cache. The system can then be configured to create app-filters matching HTTP or HTTPS expressions

as well as the IP cache ensuring that traffic is properly classified. If the operator utilizes proxies in their network, they may also configure a maximum of 8 IP addresses which match the IP addresses of the proxies used. Traffic whose destination IP address matches one of the configured proxies will be assumed to be legitimate traffic.

To configure the system for URL content charging strengthening with a dns-ip-cache the operator needs to:

- Create an application of interest and its related app-filter's URL expressions. This application is typically mapped into a charging-group.
- Create a **dns-ip-cache**. Configure parameters so the IP cache is populated by the domain names from the application mapped to the zero rating charging group and specify which DNS server IP addresses the IP cache will listen from.
- Configure a AQP to enable the dns-ip-cache.
- Optionally, configure static IP addresses matching the IP addresses of the trusted proxies

Use the following CLI syntax to create a dns-ip-cache:

CLI Syntax:

```
config>app-assure>group#
dns-ip-cache dns-ip-cache-name [create]
    dns-match
        description <description-string>
        no description
        domain <domain-name> expression <expression>
        no domain <domain-name>
        server-address <server-address> [name <server-name>]
        no server-address <server-address>
    ip-cache
        size <cache-size>
        high-watermark <percent>
        low-watermark <percent>
        [no] static-address <static-ip-address>
    [no] shutdown
```

The following example displays a configuration for a **dns-ip-cache** configured to snoop DNS responses for two different domains “*.domain1.com” and “*.domain2.com” which are zero rated or charged specifically by the operator. The configuration only uses DNS responses from the DNS server addresses configured within the **dns-match** to populate the **ip-cache**:

```
7750>config>app-assure>group# info
-----
dns-ip-cache "dns-ip-cache1" create
    description "DNS IP Cache #1"
```



```
dns-match
  domain "Sponsor#1-Domain#1" expression "*.domain1.com$"
  domain "Sponsor#1-Domain#2" expression "*.domain2.com$"
  server-address 10.8.4.4 name "CompanyName"
  server-address 10.8.8.8 name "CompanyName"
  server-address 192.168.100.11 name "OperatorX-DNS1"
  server-address 192.168.100.12 name "OperatorX-DNS2"
exit
ip-cache
  size 1000
  high-wmark 90
  low-wmark 80
exit
no shutdown
exit
```

The domains configured in the dns-ip-cache must match the app-filter expressions for the applications zero rated or charged specifically by the operator. The following example displays the charging-group **Zero Rated** and application **Sponsor Content #1** configuration:

```
7750>config>app-assure>group>policy# info
-----
charging-group "Zero Rated" create
  description "Zero Rated Content"
  export-id 10
exit
app-group "Web" create
exit
application "Sponsor Content #1" create
  description "Application#1 - Content Zero Rated"
  app-group "Web"
  charging-group "Zero Rated"
exit
app-filter
  entry 100 create
    expression 1 http-host eq "*.sponsor1-domain1.com$"
    server-address eq dns-ip-cache "dns-ip-cache1"
    application "Sponsor Content #1"
    no shutdown
  exit
  entry 110 create
    expression 1 http-host eq "*.domain2.com$"
    server-address eq dns-ip-cache "dns-ip-cache1"
    application "Sponsor Content #1"
    no shutdown
  exit
exit
```

The following example displays the AQP entry to enable the **dns-ip-cache** to snoop DNS responses; this can be optionally based on ASO characteristics:

```
A:7750>config>app-assure>group>policy>aqp# entry 100 create
match
```

```

        characteristic "dns-ip-cache" eq "yes"
    exit
    action
        action dns-ip-cache "dns-ip-cache1"
    exit
    no shutdown

```

3.3.3.14 Configuring an HTTP Error Redirect

Use the following CLI syntax to configure an HTTP error redirect policy:

CLI Syntax:

```

config>app-assure>group>
http-error-redirect redirect-name create
no http-error-redirect redirect_name
description description-string
no description
error-code error-code [custom-msg-size custom-msg-size]
no error-code error-code
http-host http-host // eg. www.demo.barefruit.com
no http-host
participant-id participant-id // 32-char string used by
    template 1
no participant-id
no] shutdown
template template-id // {1, 2} one for Barefruit, 2=
    Xerocole
no template

```

The following example displays an Application Assurance HTTP redirect configuration.

```

*A:ALA-48>config>app-assure>group# http-error-redirect "redirect-404" create
description "redirect policy of 404 to Barefruit servers"
error-code 404
http-host
    att.barefruit.com
participant-id att-ISP
template 1

*A:ALA-48>config>app-assure>group> http-error-redirect# redirect-404 info
-----
description "redirect policy of 404 to Barefruit servers"
template 1
http-host "att.barefruit.com"
participant-id "att-ISP"

error-code 404

*A:ALA-48>config>app-assure>group>http-error-redirect#

```

3.3.3.15 Configuring HTTP Header Enrichment

Use the following CLI syntax to configure an HTTP header Enrichment policy:

CLI Syntax:

```
config>app-assure>group> http-enrich <http_enrich_name>
[create]
[no] description <description-string>
[no] shutdown
[no] field <field_name> name <header_name>
    // Where "Field name" can be:
    // subscriber-ip: Header name for subscriber IP
    // subscriber-id: Header name for the subscriber ID
    // static-string: Header name for inserted string
[no] http-enrich <http_enrich_name>
```

The following example displays an Application Assurance HTTP header enrichment configuration.

```
*A:BNG>config>app-assure>group# http-enrich enrich_example create
*A:BNG>config>app-assure>group>http-enrich$ description "enrich HTTP headers with
subscriber IP and subscriber ID"
*A:BNG>config>app-assure>group>http-enrich$ field "static-string" name "x-string"
*A:BNG>config>app-assure>group>http-enrich$ field "static-string" static-string
"orange"
*A:BNG>config>app-assure>group>http-enrich$ field "subscriber-id" name "x-subID"
*A:BNG>config>app-assure>group>http-enrich$ field "subscriber-id" anti-spoof
*A:BNG>config>app-assure>group>http-enrich$ field "subscriber-ip" name x-subIP
*A:BNG>config>app-assure>group>http-enrich$ field "subscriber-
ip" encode type md5 key
"secret10"
-----
*A:BNG>config>app-assure>group>http-enrich$ info
-----
        field "static-string"
            name "x-string"
            static-string "orange"
        exit
        field "subscriber-id"
            name "x-subID"
            anti-spoof
        exit
        field "subscriber-ip"
            name "x-subIP"
            encode type md5 key
            "bF0sZZDNT8DbZoVJHD1vrYr5mJaEggEqWbSvPhgIcPW6hym0sc080." hash2
        exit
-----
*A:BNG>config>app-assure>group>http-enrich$
```

In addition, the following **show** routine displays various HTTP enrichment-related statistics:

```
show application-assurance group 1 http-enrich "MyTemplate"
```

```

=====
Application Assurance Group 1 HTTP Enrichment "MyTemplate"
=====
Description   : (Not Specified)
Admin Status  : Up
AQP Referenced: No

-----
Name           Field           Enabled
           Features
-----
subscriber-ip   MyField         M
subscriber-id   Sub-ID         AC
-----
                                     A=anti-spoof,C=encode-cert,M=encode-
md5,R=encode-rc4

-----
Group          Enriched          Not Enriched
-----
1              0                  0
-----
Total          0                  0
-----
=====

```

3.3.3.16 Configuring an HTTP Redirect Policy

Use the following CLI syntax to configure an HTTP redirect policy:

CLI Syntax:

```

config>app-assure>group# http-redirect redirect-name
[create]
    description <description-string>
    no description
    template <template-id>
    redirect-url URL // redirect URL e.g. www.isp.com/
    redirect.html
    no redirect-url
    [no] shutdown
no http-redirect <redirect-name>

```

The following example displays an AA HTTP redirect configuration.

```

*A:ALA-48>config>app-assure>group# http-redirect "redirect1" create
    description "redirect policy for blocked http content traffic without url
parameters"
    template 3
    redirect-url http://www.isp.com/redirect.html
    no shutdown

```

The following example displays an Application Assurance **http-redirect** configuration using macro substitution to append url parameters within the redirect url:

```
*A:ALA-48>config>app-assure>group# http-redirect "redirect2" create
    description "redirect policy for blocked http content traffic with url parameters"
    "
        template 5
        redirect-url "http://www.isp.com/
redirect.html?requestedurl=$URL&subscriberid=$SUB&subscriberip=$IP&routerid=$RTRID&vsa=$URLPRM"
        no shutdown
```

The following example displays AQP entry to block all http gaming traffic (AppGroup BlockedContent) and perform redirect:

```
A:ALA-48>config>app-assure>group>policy>aqp>entry#
-----
    entry 100 create
        match
            app-group eq BlockedContent
        exit
        action
            drop
            http-redirect redirectgaming
        exit
    no shutdown
    exit
-----
A:ALA-48>config>app-assure>group>policy>aqp#
```

3.3.3.17 Configuring a Captive Redirect HTTP Redirect Policy

The traditional HTTP redirect policy is used to redirect flows on the HTTP response packet, meaning the TCP three-way handshake and the original HTTP request are allowed by the 7750 SR to the Internet before the subscriber is redirected. The captive redirect HTTP redirect policy is used to redirect flows without sending any traffic to the Internet unless it matches a configurable whitelist by terminating TCP sessions in the ISA-AA cards, in which case HTTP flows are redirected to a predefined redirect URL while non-HTTP TCP flows are TCP reset.

3.3.3.17.1 Captive-Redirect and HTTPS Flows Redirection

The captive redirect HTTP redirect policy can be optionally configured to redirect HTTPS sessions in addition to HTTP to a pre-defined redirect landing page, typically the captive-portal URL in the context of a WiFi network.

This capability is particularly useful when the router is used to provide a captive-portal type of access, as it allows the operator to improve the user experience by redirecting the subscriber's web browser sessions to the desired captive-portal landing page when the user first connects to the network using HTTPS instead of HTTP.

This capability is particularly useful when the router is used to provide a captive-portal type of access, as it allows the operator to improve the user experience by redirecting the subscriber's web browser sessions to the desired captive-portal landing page when the user first connects to the network using HTTPS instead of HTTP.

Prior to the introduction of this feature, users opening their web browsers to an HTTPS URL when first connecting to a new Wi-Fi network and expecting to be redirected to a captive portal were instead presented with an error page automatically generated by the web browser since the session was dropped or reset by the network, thus ultimately preventing the user from connecting. Most non-technical users connecting to a captive-portal network may not know the difference between HTTP and HTTPS when it comes to login/redirection, and a number of subscribers may not connect or may get frustrated trying multiple different links prior to a successful Wi-Fi authentication.

When the system is configured for **captive-redirect redirect-https** it will terminate transport layer security (TLS) TCP sessions in the ISA-AA cards and return a self-signed certificate back to the user. Upon the user acceptance of the security warning generated by the web browser, the web session will then automatically be redirected to the configured captive-portal landing page.

Captive redirect policy supports redirection for HTTP, HTTPS, HTTP2, SPDY, and TCP Fast Open connections.

A session-filter is used to define the criteria for permitting or redirecting flows using the captive redirect HTTP redirect policy. Typically the operator needs to permit UDP on port 53 for DNS and they can optionally permit other content based on IP address, port number, IP prefix list, or DNS IP cache thus allowing specific on-net or off-net applications through the captive redirect policy.

To configure the system for captive redirect HTTP redirect the operator needs to:

- Create an http-redirect policy. If the ISA group aa-sub-scale mode is configured for residential or VPN, then configure the http-redirect policy for captive-redirect and associate the appropriate VLAN id AA Interface (an aa-interface routable within the subscriber's service must be created for each ISA-AA card in the system). If the ISA group aa-sub-scale mode is configured for DSM, then there is no need to associate the http-redirect policy to a VLAN id and no need to create an AA Interface.

- Create a session filter policy to allow at the minimum UDP on port 53. Additional traffic can be whitelisted based on a statically defined IP prefix list or a dynamic DNS IP cache policy. The redirect landing page should be configured using IP prefixes.
- The last action of the session filter should be set to http-redirect the remaining flows using a predefined captive redirect HTTP redirect policy.

Use the following CLI syntax to create a captive redirect HTTP redirect policy:

CLI Syntax:

```
config>app-assure>group# http-redirect <redirect-name>
[create]
    captive-redirect
        vlan-id <service-port-vlan-id>
        no vlan-id
    description <description-string>
    no description
    [no] redirect-https
    redirect-url <redirect-url>
    no redirect-url
    [no] shutdown
    [no] tcp-client-reset
    template <template-id>
    no template
no http-redirect <redirect-name>
```

The following example displays a typical configuration for a session filter user in the context of captive redirect:

```
A:7750# configure application-assurance group 1:1 create
A:7750>config>app-assure>group# info
-----
session-filter "wifi-unauthenticated" create
default-action deny
entry 5 create
    match
        ip-protocol-num udp
        dst-port eq 53
    exit
    action permit
exit
entry 10 create
    match
        dst-ip dns-ip-cache "whitelist"
    exit
    action permit
exit
entry 15 create
    description "Allow traffic to the redirect landing page server"
    match
        ip-protocol-num tcp
        dst-port eq 80
        dst-ip 172.16.70.100/32
```

```

        exit
        action permit
    exit
    entry 20 create
        match
            ip-protocol-num tcp
        exit
        action http-redirect "redirect-portal"
    exit
exit
-----

```

The following example displays a typical configuration for the AA interface used by the captive redirect HTTP redirect policy for ESM Subscribers (DSM does not require the configuration of the AA Interface):

```

A:7750# configure service ies 1 customer 1 create
A:7750>config>service>ies# info
-----
    aa-interface "aa-if-captive-redirect-isa_1-2" create
        description "AA Interface for ISA-AA card 1/2"
        address 172.16.3.1/31
        sap 1/2/aa-svc:20 create
            no shutdown
        exit
        no shutdown
    exit
-----

```

The following example displays a typical configuration for the HTTP redirect policy for ESM Subscribers (DSM does not require the configuration of the VLAN ID):

```

A:7750# configure application-assurance group 1
A:7750>config>app-assure>group>http-redir# info
-----
    template 5
    tcp-client-reset
    redirect-https
    redirect-url "http://172.16.70.100/Redirect/redirect-portal.html?RequestedURL=$URL"
    captive-redirect
        vlan-id 20
    exit
    no shutdown
-----

```

3.3.3.18 Configuring ICAP URL Filtering

To configure the system for ICAP URL Filtering, the operator needs to:

- Create an aa-interface and assign an ip address to each AA ISA within an IES or VPRN service. This routed interface is then used by the system to establish TCP communication with the ICAP server.
- Create an http-redirect policy (used by the url-filter to redirect HTTP or HTTPS traffic).
- Create a url-filter, configure the icap server ip-address, redirect-policy, and default action.
- Verify that the aa-interfaces and url-filter are operationally up.

Use the following CLI syntax to configure the aa-interfaces for each AA ISA:

CLI Syntax:

```
config>service>vprn# aa-interface <aa-if-name> [create]
config>service>vprn>aa-if# aa-interface interface <ip-
  int-name> [create]
description <description-string>
no description
address <ipv4_subnet/31>
no address
    sap <card/mda/aa-svc:vlan> [create]
        description <description-string>
        no description
        egress
            [no] filter
            [no] qos
        exit
        ingress
            [no] qos
        exit
        [no] shutdown
    exit
```

The following example displays an AA interface created for the ISA card 1/2 using IP address 172.16.2.1/31:

```
A:7750>config>service>ies# info
-----
aa-interface "aa-if1" create
address 172.16.2.1/31
sap 1/2/aa-svc:10 create
egress
    filter ip 10
exit
no shutdown
exit
no shutdown
exit
```

In the example above, 172.16.2.1 is used by the IOM side of the interface while the ISA itself is automatically assigned 172.16.2.0 based on the /31 subnet.

Recommendations:

- More than one aa-interface can be configured per AA ISA card, however, the operator needs to use the same service vlan across all these interfaces for a given url-filter object.
- Configure an egress ip filter under the sap towards the ISA AA interface to only allow selected ip addresses or subnet (subnet examples: icap servers, network management).

Use the following CLI syntax to configure the url-filter:

CLI Syntax:

```
config>app-assure>group#
url-filter <url-filter-name> [create]
    default-action {allow | block-all | block-http-
        redirect <redirect-name>}
    no default-action
    http-redirect <http-redirect-name>
    no http-redirect
    http-request-filtering {all | first}
    icap
        custom-x-header <x-header-name>
        [no] custom-x-header
    vlan-id <service-port-vlan-id>
    no vlan-id
    server <ip-address[:port]> [create]
        description <description-string>
        no description
        [no] shutdown
    no server <ip-address[:port]>
no url-filter <url-filter-name>
```

The following example displays a url-filter configuration:

```
*A:7750>config>app-assure>group# url-filter "filter1" create
    default-action block-http-redirect "http-redirect-portal"
    icap
        vlan-id 10
        server 172.16.1.101 create
        no shutdown
    exit
exit
no shutdown
```

The following example displays the AQP entry to enable icap url-filtering for opted-in subscribers based on ASO characteristics:

```
A:7750>config>app-assure>group>policy>aqp# entry 100 create
    match
        characteristic "url-filter" eq "yes"
    exit
```

```
action
    url-filter "filter1"
exit
no shutdown
```

Optionally the operator can add a custom-x-header to the ICAP request in order for the ICAP server to filter traffic based on this new x-header value instead of filtering based on subscriber names. This is done by defining a new ASO characteristic for the different ICAP filtering service packages used in the network and referring the characteristic name in the url-filter AQP action.

The following example displays a url-filter configuration with the custom-x-header field added to the ICAP request:

```
A:7750>config>app-assure>group# url-filter "filter1" create
default-action block-http-redirect "http-redirect-portal"
http-redirect "http-redirect-portal"
icap
    custom-x-header "Filtering-Policy"
    vlan-id 10
    server 172.16.1.101 create
        no shutdown
    exit
exit
no shutdown
```

The following example displays the App-Service-Option characteristic used to define the type of filtering policy available:

```
A:7750>config>app-assure>group>policy>aso# info
-----
characteristic "url-filter-policy" create
    value "filtering-policy-1" #less than 10 years old
    value "filtering-policy-2" # less than 16 years old
    value "mcdonalds"
    value "none"
    value "starbucks"
    default-value "none"
exit
-----
```

The following example displays the App-Qos-Policy action required to add the appropriate ASO value to the ICAP custom-x-header custom field:

```
A:7750>config>app-assure>group>policy>aqp# entry 100 create
match
    characteristic "url-filter" eq "yes"
exit
action
    url-filter "filter1" characteristic "url-filter-policy"
exit
no shutdown
```

3.3.3.19 Configuring Local URL-List Filtering

To configure the system for local URL-list filtering, the operator needs to:

- Create a URL-list policy referencing a valid file located on the compact flash
- Create a url-filter policy for local-filtering by referencing this URL-list
- Create an AQP to apply this url-filter policy

Use the following CLI syntax to create a URL-list:

CLI Syntax:

```
config>app-assure>group# url-list <url-list-name>
[create]
description <description-string>
no description
decrypt-key <key | hash-key | hash2-key> [hash | hash2]
no decrypt-key
file <file-url>
no file
[no] shutdown
size <url-list-size>
[standard | extended] - Default : standard
```

The decryption key is optional, if the decryption key is not specified the system will assume that the file is not encrypted. To encrypt a file in Linux using the supported encryption format use the following command:

```
Linux# openssl des3 -nosalt -in <input-file.txt> -out <output.enc>
```

The following example displays a URL-list configuration:

```
A:7750>config>app-assure>group# url-list url-list1 create
-----
description "Local List for URL Filtering"
decrypt-key ".i84/PluS0lMG0Qkae7mAV2Oj10n726Z" hash2
file "cf3:\url-list1.enc"
no shutdown
-----
```

Use the following CLI syntax to create a url-filter policy for local-filtering:

CLI Syntax:

```
config>app-assure>group# url-filter <url-filter-name>
[create]
url-filter <url-filter-name> [create]
description <description-string>
no description
```

```
default-action {allow | block-all | block-http-redirect  
  <redirect-name>}  
no default-action  
[no] http-redirect <redirect-name>  
http-request-filtering {all | first}  
local-filtering  
[no] url-list <url-list-name>  
[no] shutdown
```

The following example displays a url-filter configured for local-filtering:

```
A:7750>config>app-assure>group# url-filter "url-blacklist1" create  
A:7750>config>app-assure>group>url-filter# info  
-----  
default-action allow  
http-redirect "http-redirect-portal"  
local-filtering  
  url-list "url-list1"  
exit  
no shutdown  
-----
```

The default action should always be configured to “allow” when the url-filter is configured for local-filtering. The default-action in this context represents the action the system will take in case the local-list file is not accessible; this scenario may happen if the source file was corrupted or if the compact flash card was not accessible.

The following example displays the AQP entry to enable ICAP url-filtering for opted-in subscribers based on ASO characteristics:

```
A:7750>config>app-assure>group>policy>aqp# entry 100 create  
match  
  characteristic "child-protection" eq "yes"  
exit  
action  
  url-filter "url-blacklist1"  
exit  
no shutdown
```

3.3.3.20 Configuring HTTP Notification

Use the following CLI syntax to configure an HTTP Notification policy.

CLI Syntax:

```
config>app-assure>group#  
http-notification <http-notification-name> [create]  
  description <description-string>  
  no description  
  script-url <script-url-name>
```

```

no script-url
interval {one-time | <minimum-interval>}
template <template-id>
no template
[no] shutdown
no http-notification <http-notification-name>

```

The following example displays an HTTP notification policy configured with a minimum interval of 5 minutes:

```

A:7750>config>app-assure>group# http-notification "in-browser-notification" create
A:7750>config>app-assure>group>http-notif# info
-----
description "In Browser Notification Example"
template 1
script-url "http://10.1.1.1/In-Browser-Notification/script.js"
interval 5
no shutdown
-----

```

The operator then needs to enable the http-match-all-req feature for any HTTP request sent the messaging server domain which will be used to monitor HTTP notification success/failures. This is done by creating a new application and enabling http-match-all-req within the app-filter.

```

A:7750>config>app-assure>group>policy# application "IBN Messaging Server" create
A:7750>config>app-assure>group>policy>app$ app-group "Web"

A:7750>config>app-assure>group>policy# app-filter entry 100 create
A:7750>config>app-assure>group>policy>app-filter>entry$ info
-----
expression 1 http-host eq "^10.1.1.1$"
http-match-all-req
application "IBN Messaging Server"
no shutdown
-----

```

The following examples displays the AQP entry required to match this policy based on an ASO characteristic:

```

A:7750>config>app-assure>group>policy>aqp# info
-----
entry 200 create
match
characteristic "in-browser-notification" eq "yes"
exit
action
http-notification "in-browser-notification"
exit
no shutdown
exit
-----

```

3.3.4 Configuring AA Volume Accounting and Statistics

A network operator can configure AA volume statistic collection and accounting on both AA ISA system and subscriber levels.

The following commands illustrate the configuration of statistics collection and accounting policy on an AA group/partition aggregate level (without subscriber context).

CLI Syntax: `config>app-assure>group>statistics>app-group
accounting-policy act-policy-id
collect-stats`

CLI Syntax: `config>app-assure>group>statistics>application
accounting-policy act-policy-id
collect-stats`

CLI Syntax: `config>app-assure>group>statistics>protocol
accounting-policy act-policy-id
collect-stats`

These commands illustrate the configuration of statistics collection and accounting policy for each AA subscriber in the system.

CLI Syntax: `config>app-assure>group>statistics>aa-sub
accounting-policy acct-policy-id
aggregate-stats
app-group app-group-name export-using export-method
[export-method... (upto 2 max)]
application application-name export-using export-method
[export-method... (upto 2 max)]
charging-group charging-group-name export-using export-
method [export-method... (upto 2 max)]
collect-stats
exclude-tcp-retrans
max-throughput-stats
protocol protocol-name export-using export-method
radius-accounting-policy rad-acct-plcy-name`

These commands illustrate configuration of special study mode for a subset of AA subscribers (configured) to collect all protocol and/or application statistics with an AA subscriber context.

CLI Syntax: `config>app-assure>group>statistics# aa-sub-study
{application | protocol}
accounting-policy acct-policy-id
collect-stats`

For details on accounting policy configuration (including among others AA record type selection and customized AA subscriber record configuration) refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.

The following output illustrates per AA-subscriber statistics configuration that elects statistic collection for a small subset of all application groups, applications, protocols:

```
*A:ALU-40>config>app-assure>group>statistics>aa-sub# info
```

```
-----
accounting-policy 4
collect-stats
app-group "File Transfer"
app-group "Infrastructure"
app-group "Instant Messaging"
app-group "Local Content"
app-group "Mail"
app-group "MultiMedia"
app-group "Business_Critical"
app-group "Peer to Peer"
app-group "Premium Partner"
app-group "Remote Connectivity"
app-group "Tunneling"
app-group "Unknown"
app-group "VoIP"
app-group "Web"
app-group "Intranet"
application "BitTorrent"
application "eLearning"
application "GRE"
application "H323"
application "TLS"
application "HTTP"
application "HTTPS"
application "HTTPS_Server"
application "HTTP_Audio"
application "HTTP_Video"
application "eMail_Business"
application "eMail_Other"
application "Oracle"
application "Skype"
application "SAP"
application "SIP"
application "SMTP"
application "SQL_Alltypes"
application "TFTP"
protocol "bittorrent"
protocol "dns"
protocol "sap"
protocol "skype"
-----
```

```
*A:ALU-40>config>app-assure>group>statistics>aa-sub#
```


3.3.4.1 Configuring Cflowd Collector

The following output displays an Application Assurance cflowd collector configuration example:

```
Example: *A:ALA-48# configure application-assurance group 1
            cflowd collector 192.168.131.149:55000 create
            *A:ALA-48>config>app-
              assure>group>cflowd>collector$description
              "cflowd_collector_NewYork"
            *A:ALA-48>config>app-assure>group>cflowd>collector# no
              shutdown
            *A:ALA-48>config>app-assure>group>cflowd>collector#
              exit

            *A:ALA-48>config>app-assure>group>cflowd# info
            -----
              collector 192.168.131.149:55000 create
              description "cflowd_collector_NewYork"
              no shutdown
            -----
            *A:ALA-48>config>app-assure>group>cflowd#
```

3.3.4.2 Configuring AA Volume, TCP and RTP Performance Reporting

```
CLI Syntax: config>app-assure>group isa-aa-group-id
              cflowd
              collector ip-address[:port] [create]
              no collector ip-address[:port]
              description description-string
              no description
                  [no] shutdown
              rtp-performance
                  flow-rate sample-rate
                  no flow-rate
                  flow-rate2 sample-rate2
                  no flow-rate2
              tcp-performance
                  flow-rate sample-rate
                  no flow-rate
                  flow-rate2 sample-rate2
                  no flow-rate2
              template-retransmit seconds
              no template-retransmit
                  [no] shutdown
              volume
```

```

rate sample-rate
no rate
[no] shutdown

```

CLI Syntax:

```

config>application-assurance
group isa-aa-group-id[:partition [create]]
no group isa-aa-group-id[:partition
    cflowd
        volume
            [no] shutdown
        rtp-performance
            [no] app-group app-group-name [flow-rate |
                flow-rate 2]
            [no] application application-name [flow-
                rate | flow-rate 2]
            [no] shutdown
        tcp-performance
            [no] app-group app-group-name [flow-rate |
                flow-rate 2]
            [no] application application-name [flow-
                rate | flow-rate 2]
            [no] shutdown

```

The default is **flow-rate**.

The following example shows a configuration that:

- Enables per-flow volume stats for group 1, partition 1 and configures sampling rate to 1/1000.
- Enables per-flow TCP performance stats for web_traffic application within group 1, partition 1 and configures TCP sampling rate to 1/500.
- Enables per-flow TCP performance stats for citrix_traffic application within group 1, partition 1 using TCP sampling rate2 to 1/100.
- Enables per-flow RTP A/V performance stats for voip_traffic application within group 1, partition 1 and configures rtp sampling rate to 1/10.

```

*A:ALA-48# configure application-assurance group 1 cflowd
*A:ALA-48>config>app-assure>group>cflowd# volume rate 1000
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance flow-rate 500
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance flow-rate2 100
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance flow-rate 10
*A:ALA-48>config>app-assure>group>cflowd# no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
-----
collector 192.168.131.149:55000 create
description "cflowd_collector_NewYork"
exit
volume
    rate 1000

```

```

        exit
        tcp-performance
            flow-rate 500
            flow-rate 100
        rtp-performance
            flow-rate 10
        exit
        no shutdown
    -----
    *A:ALA-48>config>app-assure>group>cflowd#

    *A:ALA-48# configure application-assurance group 1:1 cflowd
    *A:ALA-48>config>app-assure>group>cflowd#
    *A:ALA-48>config>app-assure>group>cflowd# volume no shutdown
    *A:ALA-48>config>app-assure>group>cflowd# tcp-performance application "web_traffic"
    *A:ALA-48>config>app-assure>group>cflowd# tcp-
    performance application "citrix" [flow-
    rate2]
    *A:ALA-48>config>app-assure>group>cflowd# tcp-performance no shutdown
    *A:ALA-48>config>app-assure>group>cflowd# rtp-
    performance application "voip_traffic"
    *A:ALA-48>config>app-assure>group>cflowd# rtp-performance no shutdown
    *A:ALA-48>config>app-assure>group>cflowd# info
    -----
        volume
            no shutdown exit
        rtp-performance no shutdown
            application "voip_traffic"
        tcp-performance
            no shutdown
            application "web_traffic"
            application "citrix" flow-rate2
        exit
    
```


3.4 Application Assurance Command Reference

- [Application Assurance Command Reference](#)
- [Command Descriptions](#)

3.4.1 Application Assurance Command Reference

- [Hardware Commands](#)
- [Admin Commands](#)
- [ISA Commands](#)
- [Application Assurance Commands](#)
- [AA Interface Commands](#)
- [Persistence Commands](#)

3.4.1.1 Hardware Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide* for hardware command descriptions.

3.4.1.2 Admin Commands

```
admin
  — application-assurance
    — group aa-group-id
      — url-list url-list-name upgrade
    — upgrade
```

3.4.1.3 ISA Commands

```
config
  — isa
    — application-assurance-group application-assurance-group-index [create] [aa-sub-scale sub-scale]
    — no application-assurance-group application-assurance-group-index
      — [no backup mda-id]
      — description description-string
```

- **no description**
- [no] **divert-fc** *fc-name*
- [no] **fail-to-open**
- [no] **http-enrich-maximum**
- **isa-capacity-cost-high-threshold** *threshold*
- **no isa-capacity-cost-high-threshold**
- **isa-capacity-cost-low-threshold** *threshold*
- **no isa-capacity-cost-low-threshold**
- [no] **isa-overload-cut-through**
- **minimum-isa-generation** *min-isa-generation*
- **overload-sub-quarantine**
 - [no] **shutdown**
- [no] **partitions**
- [no] **primary** *mda-id*
- **qos**
 - **egress**
 - **from-subscriber**
 - **pool** *[pool-name]*
 - **no pool**
 - **resv-cbs** *percent-or-default*
 - **no resv-cbs**
 - **slope-policy** *slope-policy-name*
 - **no slope-policy**
 - **port-scheduler-policy** *port-scheduler-policy-name*
 - **no port-scheduler-policy**
 - **queue-policy** *network-queue-policy-name*
 - **no queue-policy**
 - **wa-shared-high-wmark** *percent*
 - **no wa-shared-high-wmark**
 - **wa-shared-low-wmark** *percent*
 - **no wa-shared-low-wmark**
 - **to-subscriber**
 - **pool** *[pool-name]*
 - **no pool**
 - **resv-cbs** *percent-or-default*
 - **no resv-cbs**
 - **slope-policy** *slope-policy-name*
 - **no slope-policy**
 - **port-scheduler-policy** *port-scheduler-policy-name*
 - **no port-scheduler-policy**
 - **queue-policy** *network-queue-policy-name*
 - **no queue-policy**
 - **wa-shared-high-wmark** *percent*
 - **no wa-shared-high-wmark**
 - **wa-shared-low-wmark** *percent*
 - **no wa-shared-low-wmark**
- **shared-resources**
 - **tcp-adv-func**
- [no] **shutdown**
- **statistics**
 - **performance**
 - **accounting-policy** *acct-policy-id*
 - **no accounting-policy**
 - [no] **collect-stats**

- **transit-prefix-ipv4-entries** *entries*
- **no transit-prefix-ipv4-entries**
- **transit-prefix-ipv4-remote-entries** *entries*
- **no transit-prefix-ipv4-remote-entries**
- **transit-prefix-ipv6-entries** *entries*
- **no transit-prefix-ipv6-entries**
- **transit-prefix-ipv6-remote-entries** *entries*
- **no transit-prefix-ipv6-remote-entries**

3.4.1.4 Application Assurance Commands

- [AA Commands](#)
- [AA Group Commands](#)

3.4.1.4.1 AA Commands

```

config
  — application-assurance
    — arp arpld [create]
    — no arp arpld
      — description description-string
      — no description
      — master-selection-mode mode
      — peer ip-address
      — no peer
      — peer-endpoint sap sap-id encap-type {dot1q | null | qinq}
      — peer-endpoint spoke-sdp sdp-id:vc-id
      — no peer-endpoint
      — priority value
      — no priority
      — [no] shutdown
    — bit-rate-high-wmark high-watermark
    — bit-rate-low-wmark low-watermark
    — no bit-rate-low-wmark
    — datapath-cpu-high-wmark high-watermark
    — datapath-cpu-high-wmark max
    — datapath-cpu-low-wmark low-watermark
    — flow-setup-high-wmark high-watermark
    — flow-setup-low-wmark low-watermark
    — no flow-setup-low-wmark
    — flow-table-high-wmark high-watermark
    — no flow-table-high-wmark
    — flow-table-low-wmark low-watermark
    — no flow-table-low-wmark
    — packet-rate-high-wmark high-watermark
    — packet-rate-low-wmark low-watermark
    — no packet-rate-low-wmark
    — protocol protocol-name

```

- [no] **shutdown**
- **radius-accounting-policy** *rad-acct-plcy-name* [create]
- no **radius-accounting-policy** *rad-acct-plcy-name*
 - **description** *description-string*
 - no **description**
 - **interim-update-interval** *minutes*
 - no **interim-update-interval**
- **radius-accounting-server**
 - **access-algorithm** {direct | round-robin}
 - **retry** *count*
 - **router** *router-instance*
 - **router service-name** *service-name*
 - no **router**
 - **server** *server-index* **address** *ip-address* **secret** *key* [hash | hash2] [port *port*] [create]
 - no **server** *server-index*
 - **source-address** *ip-address*
 - no **source-address**
 - **timeout** *seconds*
- **significant-change** *delta*
- no **significant-change**

3.4.1.4.2 AA Group Commands

- ```
config
— application-assurance
 — group aa-group-id[:partition-id] [create]
 — no group aa-group-id:partition-id
 — [no] aa-sub-remote
 — access-network-location
 — source source-type level level
 — no source source-type
 — rtt-threshold threshold
 — no rtt-threshold
 — rtt-threshold-tolerance tolerance
 — no rtt-threshold-tolerance
 — [no] aqp-initial-lookup
 — certificate-profile cert-profile-name [create]
 — no certificate-profile cert-profile-name
 — certificate certificate-file
 — no certificate
 — description description-string
 — no description
 — [no] shutdown
 — cflowd
 — collector ip-address[:port] [create]
 — no collector ip-address[:port]
 — description description-string
 — no description
 — [no] shutdown
 — comprehensive
```



---

```

— app-group app-group-name [rate]
— no app-group app-group-name
— application application-name [rate]
— no application application-name
— flow-rate sample-rate
— no flow-rate
— flow-rate2 sample-rate
— no flow-rate2
— [no] shutdown
— direct-export
— collector collector-id [create]
— no collector collector-id
— [no] address ip-address [:port]
— [no] shutdown
— description description-string
— no description
— vlan-id service-port-vlan-id
— no vlan-id
— export-override mode
— no export-override
— prefix prefix-string
— no prefix
— rtp-performance
— app-group app-group-name [rate]
— no app-group app-group-name
— application application-name [rate]
— no application application-name
— flow-rate sample-rate
— no flow-rate
— flow-rate2 sample-rate
— no flow-rate2
— [no] shutdown
— [no] shutdown
— tcp-performance
— app-group app-group-name [rate]
— no app-group app-group-name
— application application-name [rate]
— application application-name
— flow-rate sample-rate
— no flow-rate
— flow-rate2 sample-rate
— no flow-rate2
— [no] shutdown
— template-retransmit seconds
— no template-retransmit
— volume
— rate sample-rate
— no rate
— [no] shutdown
— description description-string
— no description
— [no] disable-deferred-billing
— dns-ip-cache dns-ip-cache-name [create]
— no dns-ip-cache dns-ip-cache-name

```

---

```

— description description-string
— no description
— dns-match
 — domain domain-name expression expression
 — no domain domain-name
 — server-address server-address [name server-name]
 — no server-address server-address
— ip-cache
 — high-wmark percent
 — low-wmark percent
 — size cache-size
 — [no] static-address static-ip-address
— [no] shutdown
— event-log event-log-name [create]
— no event-log event-log-name
 — buffer-type buffer-type
 — max-entries max-entries
 — [no] shutdown
 — syslog
 — address ip-address
 — no address
 — description description-string
 — no description
 — facility syslog-facility
 — port port
 — severity syslog-severity
 — vlan-id service-port-vlan-id
 — no vlan-id
— gtp
 — event-log event-log-name
 — no event-log
 — gtp-filter gtp-filter-name [create]
 — no gtp-filter gtp-filter-name
 — description description-string
 — no description
 — event-log event-log-name
 — no event-log
 — max-payload-length bytes
 — no max-payload-length
 — message-type
 — default-action {permit | deny}
 — entry entry-id value gtp-message-value action {permit | deny}
 — no entry entry-id
 — mode mode
 — [no] shutdown
— http-enrich http-enrich-name [create]
— no http-enrich http-enrich-name
 — description description-string
 — no description
 — [no] field field-name
 — [no] anti-spoof
 — encode type type key key

```

---

```

— encode type type key hash-key hash
— encode type type key hash2-key hash2
— encode type type cert-profile cert-profile-name
— no encode
— name header-name
— static-string string
— no static-string
— [no] shutdown
— [no] tls-extension
— extension-id extension-id
— no extension-id
— [no] subtype tls extension subtype
— encode type type key key | hash-key | hash2-key [hash
 | hash2]
— no encode
— http-error-redirect redirect-name [create]
— no http-error-redirect redirect-name
— description description-string
— no description
— error-code error-code [custom-msg-size custom-msg-size]
— no error-code error-code
— http-host http-host
— no http-host
— participant-id participant-id
— no participant-id
— [no] shutdown
— template template-id
— no template
— [no] http-match-all-requests
— http-notification http-notification [create]
— no http-notification http-notification
— description description-string
— no description
— interval minimum-interval
— interval one-time
— script-url script-url-name
— no script-url
— [no] shutdown
— template template-id
— no template
— http-redirect redirect-name [create]
— no http-redirect redirect-name
— captive-redirect
— vlan-id service-port-vlan-id
— no vlan-id
— description description-string
— no description
— [no] redirect-https
— redirect-url redirect-url
— no redirect-url
— [no] shutdown
— [no] tcp-client-reset
— template template-id
— no template

```

- 
- [no] **http-x-online-host**
  - **ip-prefix-list** *ip-prefix-list-name* [create]
  - no **ip-prefix-list** *ip-prefix-list-name*
    - **description** *description-string*
    - no **description**
    - **prefix** *ip-prefix/ip-prefix-length* [name *prefix-name*]
    - no **prefix** *ip-prefix/ip-prefix-length*
  - **policer** *policer-name* **type** *type* **granularity** *granularity* [create]
  - **policer** *policer-name*
  - no **policer** *policer-name*
    - **action** {*priority-mark* | *permit-deny*}
    - **adaptation-rule** **pir** {*max* | *min* | *closest*} [*cir* {*max* | *min* | *closest*}]
    - no **adaptation-rule**
    - **cbs** *committed-burst-size*
    - no **cbs**
    - **congestion-override**
      - **cbs** *congested-cbs*
      - no **cbs**
      - **cir** *congested-cir*
      - no **cir**
      - **mbs** *congested-mbs*
      - no **mbs**
      - **pir** *congested-pir*
      - no **pir**
    - **description** *description-string*
    - no **description**
    - **flow-count** *flow-count*
    - no **flow-count**
    - [no] **gtp-traffic**
    - **mbs** *maximum-burst-size*
    - no **mbs**
    - **rate** *pir-rate* [*cir* *cir-rate*]
    - no **rate**
    - **rate-percentage** *rate-percentage*
    - no **rate-percentage**
    - **tod-override** *tod-override-id* [create]
    - no **tod-override** *tod-override-id*
      - **cbs** *committed-burst-size*
      - no **cbs**
      - **description** *description-string*
      - no **description**
      - **flow-count** *flow-count*
      - no **flow-count**
      - **mbs** *maximum-burst-size*
      - no **mbs**
      - **rate** *pir-rate* [*cir* *cir-rate*]
      - no **rate**
      - [no] **shutdown**
      - **time-range** **daily** **start** *start-time* **end** *end-time* [on *day* [*day*]]
      - **time-range** **weekly** **start** *start-time* **end** *end-time*
      - no **time-range**
  - **policy**
    - **abort**
    - **app-filter**

- **entry** *entry-id* [**create**]
- **no entry** *entry-id*
  - **application** *application-name*
  - **description** *description-string*
  - **no description**
  - **expression** *expr-index* *expr-type* {**eq** | **neq**} *expr-string*
  - **no expression** *expr-index*
  - **flow-setup-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}
  - [**no**] **http-match-all-requests**
  - **http-port** {**eq** | **neq**} *port-num*
  - **http-port** {**eq** | **neq**} **port-list** *port-list-name*
  - **no http-port**
  - **ip-protocol-num** {**eq** | **neq**} *protocol-id*
  - **no ip-protocol-num**
  - **network-address** {**eq** | **neq**} *ip-address*
  - **network-address** {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
  - **no network-address**
  - **protocol** {**eq** | **neq**} *protocol-name*
  - **no protocol**
  - **server-address** {**eq** | **neq**} *ip-address*
  - **server-address** {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
  - **server-address** {**eq** | **neq**} **dns-ip-cache** *dns-ip-cache-name*
  - **no server-address**
  - **server-port** {**eq** | **neq** | **gt** | **lt**} *port-num*
  - **server-port** {**eq** | **neq**} **range** *start-port-num* *end-port-num*
  - **server-port** {**eq**} {*port-num* | **range** *start-port-num* *end-port-num*} {**first-packet-trusted** | **first-packet-validate**}
  - **server-port** {**eq** | **neq**} **port-list** *port-list-name*
  - **server-port** {**eq**} **port-list** *port-list-name* {**first-packet-trusted** | **first-packet-validate**}
  - **no server-port**
  - [**no**] **shutdown**
- **app-group** *application-group-name* [**create**]
- **no app-group** *application-group-name*
  - **charging-group** *charging-group-name*
  - **no charging-group**
  - **description** *description*
  - **no description**
  - **export-id** *export-id*
  - **no export-id**
- **app-profile** *app-profile-name* [**create**]
- **no app-profile** *app-profile-name*
  - [**no**] **aa-sub-suppressible**
  - **capacity-cost** *cost*
  - **no capacity-cost**
  - **characteristic** *characteristic-name* **value** *value-name*
  - **no characteristic** *characteristic-name*
  - **description** *description-string*

- **no description**
- **[no] divert**
- **app-qos-policy**
  - **entry** *entry-id* **[create]**
  - **no entry** *entry-id*
  - **action**
    - **bandwidth-policer** *policer-name*
    - **no bandwidth-policer**
    - **dns-ip-cache** *dns-ip-cache-name*
    - **no dns-ip-cache**
    - **[no] drop**
    - **error-drop** **[event-log** *event-log-name* **]**
    - **no error-drop**
    - **flow-count-limit** *policer-name* **[event-log** *event-log-name* **]**
    - **no flow-count-limit**
    - **flow-rate-limit** *policer-name* **[event-log** *event-log-name* **]**
    - **no flow-rate-limit**
    - **fragment-drop** **{all | out-of-order}** **[event-log** *event-log-name* **]**
    - **no fragment-drop**
    - **gtp-filter** *gtp-filter-name*
    - **no gtp-filter**
    - **http-enrich** *http-enrich-name*
    - **no http-enrich**
    - **http-error-redirect** *redirect-name*
    - **no http-error-redirect**
    - **http-notification** *http-notification*
    - **no http-notification**
    - **http-redirect** *redirect-name* **flow-type** *flow-type*
    - **no http-redirect**
    - **mirror-source** **[all-inclusive]** *mirror-service-id*
    - **no mirror-source**
    - **overload-drop** **[event-log** *event-log-name* **]**
    - **no overload-drop**
    - **remark**
      - **dscp in-profile** *dscp-name* **out-profile** *dscp-name*
      - **no dscp**
      - **fc** *fc-name*
      - **no fc**
      - **priority** *priority-level*
      - **no priority**
    - **sctp-filter** *sctp-filter-name*
    - **no sctp-filter**
    - **session-filter** *session-filter-name*
    - **no session-filter**
    - **tcp-mss-adjust** *segment-size*
    - **no tcp-mss-adjust**
    - **tcp-validate** *tcp-validate-name*
    - **no tcp-validate**
    - **[no] tls-enrich**

- **url-filter** *url-filter-name* [**characteristic** *characteristic-name*]
- **no url-filter**
- **description** *description-string*
- **no description**
- **match**
  - **aa-sub** **esm** {**eq** | **neq**} *sub-ident-string*
  - **aa-sub** **esm-mac** {**eq** | **neq**} *esm-mac-name*
  - **aa-sub** **sap** {**eq** | **neq**} *sap-id*
  - **aa-sub** **spoke-sdp** {**eq** | **neq**} *sdp-id:vc-id*
  - **aa-sub** **transit** {**eq** | **neq**} *transit-aasub-name*
  - **no aa-sub**
  - **app-group** {**eq** | **neq**} *application-group-name*
  - **no app-group**
  - **application** {**eq** | **neq**} *application-name*
  - **no application**
  - **characteristic** *characteristic-name* **eq** *value-name*
  - **no characteristic** *characteristic-name*
  - **charging-group** {**eq** | **neq**} *charging-group-name*
  - **no charging-group**
  - **dscp** {**eq** | **neq**} *dscp-name*
  - **no dscp**
  - **dst-ip** {**eq** | **neq**} *ip-address*
  - **dst-ip** {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
  - **no dst-ip**
  - **dst-port** {**eq** | **neq**} *port-num*
  - **dst-port** {**eq** | **neq**} **port-list** *port-list-name*
  - **dst-port** {**eq** | **neq**} **range** *start-port-num end-port-num*
  - **no dst-port**
  - **ip-protocol-num** {**eq** | **neq**} *protocol-id*
  - **no ip-protocol-num**
  - **src-ip** {**eq** | **neq**} *ip-address*
  - **src-ip** {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
  - **no src-ip**
  - **src-port** {**eq** | **neq**} *port-num*
  - **src-port** {**eq** | **neq**} **port-list** *port-list-name*
  - **src-port** {**eq** | **neq**} **range** *start-port-num end-port-num*
  - **no src-port**
  - **traffic-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}
- **[no] shutdown**
- **app-service-options**
  - **characteristic** *characteristic-name* [**create**]
  - **no characteristic** *characteristic-name*
    - **default-value** *value-name*
    - **no default-value**
    - **[no] value** *value-name*
- **application** *application-name* [**create**]
- **no application** *application-name*
  - **app-group** *app-group-name*
  - **charging-group** *charging-group-name*

---

```

 — no charging-group
 — description description-string
 — no description
 — export-id export-id
 — no export-id
— begin
— charging-group charging-group-name [create]
— no charging-group charging-group-name
 — description description-string
 — no description
 — export-id export-id
 — no export-id
 — notify-start-stop [flow-based]
 — no notify-start-stop
— commit
— custom-protocol custom-protocol-id ip-protocol-num protocol-id
 [create]
— custom-protocol custom-protocol-id
— no custom-protocol custom-protocol-id
 — description description-string
 — no description
 — expression expr-index eq expr-string offset payload-octet-
 offset direction direction
 — no expression expr-index
 — [no] shutdown
— default-charging-group charging-group-name
— no default-charging-group
— diff
— policy-override
 — policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-
 aasub-name} [create]
 — no policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-
 aasub-name}
 — characteristic characteristic-name value value-name
 — no characteristic characteristic-name
— port-list port-list-name [create]
— no port-list port-list-name
 — description description-string
 — no description
 — [no] port port-number
 — [no] port range start-port-num end-port-num
— sctp-filter sctp-filter-name [create]
— no sctp-filter sctp-filter-name
 — description description-string
 — no description
 — event-log event-log-name
 — no event-log
 — ppid
 — default-action {permit | deny}
 — entry entry-id value ppid-value action {permit | deny}
 — no entry entry-id
 — ppid-range min min-ppid max max-ppid
 — no ppid-range
— session-filter session-filter-name [create]

```



- **no session-filter** *session-filter-name*
  - **default-action** {**permit** | **deny**} [**event-log** *event-log-name*]
  - **description** *description-string*
  - **no description**
  - **entry** *entry-id* [**create**]
  - **no entry** *entry-id*
    - **action** {**permit** | **deny** | **tcp-strict-order**} [**event-log** *event-log-name*]
    - **action** **application** *application-name*
    - **action** **http-redirect** *http-redirect-name* [**event-log** *event-log-name*]
    - **action** **tcp-optimizer** *tcp-optimizer-name*
    - **description** *description-string*
    - **no description**
    - **match**
      - **dst-ip** *ip-address*
      - **dst-ip** **dns-ip-cache** *dns-ip-cache-name*
      - **dst-ip** **ip-prefix-list** *ip-prefix-list-name*
      - **no dst-ip**
      - **dst-port** {**eq** | **gt** | **lt**} *port-num*
      - **dst-port** **port-list** *port-list-name*
      - **dst-port** **range** *start-port-num end-port-num*
      - **no dst-port**
      - **ip-protocol-num** {*ip-protocol-number* | *protocol-name*}
      - **no ip-protocol-num**
      - **src-ip** *ip-address*
      - **src-ip** **ip-prefix-list** *ip-prefix-list*
      - **no src-ip**
      - **src-port** {**eq** | **gt** | **lt**} *port-num*
      - **src-port** **port-list** *port-list-name*
      - **src-port** **range** *start-port-num end-port-num*
      - **no src-port**
- **statistics**
  - **aa-admit-deny**
    - **accounting-policy** *acct-policy-id*
    - **no accounting-policy**
    - [no] **collect-stats**
    - [no] **gtp-filter-stats**
    - [no] **policer-stats**
    - [no] **policer-stats-resources**
    - [no] **sctp-filter-stats**
    - [no] **session-filter-stats**
    - [no] **tcp-validate-stats**
  - **aa-partition**
    - **accounting-policy** *acct-policy-id*
    - **no accounting-policy**
    - [no] **collect-stats**
    - [no] **traffic-type**
  - **aa-sub**
    - **accounting-policy** *acct-policy-id*
    - **no accounting-policy**
    - **aggregate-stats** **export-using** *export-method* [*export-method...*(up to 2 max)]

- **aggregate-stats** **no-export**
- **app-group** *app-group-name* **export-using** *export-method*  
[*export-method...*(up to 2 max)]
- **app-group** *app-group-name* **no-export**
- **no app-group** *app-group-name*
- **application** *application-name* **export-using** *export-method*
- **application** *application-name* **no-export**
- **no application** *application-name*
- **charging-group** *charging-group-name* **export-using** *export-method*  
*method* [*export-method...*(up to 2 max)]
- **charging-group** *charging-group-name* **no-export**
- **no charging-group** *charging-group-name*
- [no] **collect-stats**
- [no] **exclude-tcp-retrans**
- [no] **max-throughput-stats**
- [no] **protocol** *protocol-name* **export-using** *export-method*
- **radius-accounting-policy** *rad-acct-plcy-name*
- **no radius-accounting-policy**
- [no] **usage-monitoring**
- **aa-sub-study** *study-type*
  - **aa-sub** {*esm sub-ident-string* | **esm-mac** *esm-mac-name* | **sap**  
*sap-id* | **spoke-sdp** *sdp-id:vc-id* | **transit** *transit-aasub-name*}
  - **no aa-sub** {*esm sub-ident-string* | **sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id* | **transit** *transit-aasub-name*}
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [no] **collect-stats**
- **app-group**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [no] **collect-stats**
- **application**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [no] **collect-stats**
- **protocol**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [no] **collect-stats**
  - [no] **shutdown**
- **threshold-crossing-alert**
  - **error-drop** **direction** *direction* [**create**]
  - **no error-drop** **direction** *direction*
    - **high-wmark** *high-watermark* **low-wmark** *low-watermark*
  - **fragment-drop-all** **direction** *direction* [**create**]
  - **no fragment-drop-all** **direction** *direction*
    - **high-wmark** *high-watermark* **low-wmark** *low-watermark*
  - **fragment-drop-out-of-order** **direction** *direction* [**create**]
  - **no fragment-drop-out-of-order** **direction** *direction*
    - **high-wmark** *high-watermark* **low-wmark** *low-watermark*
  - **gtp-filter** *filter-name*
    - **max-payload-length** **direction** *direction* [**create**]
    - **no max-payload-length** **direction** *direction*

- **high-wmark** *high-watermark low-wmark low-watermark*
- **message-type**
  - **default-action** *direction direction [create]*
  - **no default-action** *direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
  - **entry** *entry-id direction direction [create]*
  - **no entry** *entry-id direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
  - **header-sanity** *direction direction [create]*
  - **no header-sanity** *direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
- **gtp-sanity-drop** *direction direction [create]*
- **no gtp-sanity-drop** *direction direction*
  - **high-wmark** *high-watermark low-wmark low-watermark*
- **overload-drop** *direction direction [create]*
- **no overload-drop** *direction direction*
  - **high-wmark** *high-watermark low-wmark low-watermark*
- **policer** *policer-name direction direction [create]*
- **no policer** *policer-name direction direction*
  - **high-wmark** *high-watermark low-wmark low-watermark*
- **sctp-filter** *sctp-filter-name*
  - **packet-sanity** *direction direction [create]*
  - **no packet-sanity** *direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
- **ppid**
  - **default-action** *direction direction [create]*
  - **no default-action** *direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
  - **entry** *entry-id direction direction [create]*
  - **no entry** *entry-id direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
  - **ppid-range** *direction direction [create]*
  - **no ppid-range** *direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
- **session-filter** *session-filter-name*
  - **default-action** *direction direction [create]*
  - **no default-action** *direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
  - **entry** *entry-id direction direction [create]*
  - **no entry** *entry-id direction direction*
    - **high-wmark** *high-watermark low-wmark low-watermark*
- **tcp-validate** *tcp-validate-name direction direction [create]*
- **no tcp-validate** *tcp-validate-name direction direction*
  - **high-wmark** *high-watermark low-wmark low-watermark*

---

```

— tcp-validate tcp-validate-name [create]
— no tcp-validate tcp-validate-name
 — description description-string
 — no description
 — event-log event-log-name [all]
 — no event-log
 — [no] strict
— transit-ip-policy ip-policy-id [create]
— no transit-ip-policy ip-policy-id
 — def-app-profile app-profile-name
 — no def-app-profile
 — description description-string
 — no description
 — [no] detect-seen-ip
 — dhcp
 — [no] shutdown
 — diameter
 — [no] application-policy name
 — [no] shutdown
 — ipv6-address-prefix-length IPv6-prefix-length
 — no ipv6-address-prefix-length
 — radius
 — authentication-policy name
 — no authentication-policy
 — seen-ip-radius-acct-policy rad-acct-plcy-name
 — no seen-ip-radius-acct-policy
 — [no] shutdown
 — static-aa-sub transit-aasub-name
 — static-aa-sub transit-aasub-name app-profile app-profile-name
 [create]
 — no static-aa-sub transit-aasub-name
 — [no] ip ip-address[/mask]
 — sub-ident-policy sub-ident-policy-name
 — no sub-ident-policy
 — transit-auto-create
 — [no] shutdown
— transit-prefix-policy prefix-policy-id [create]
— no transit-prefix-policy prefix-policy-id
 — description description-string
 — no description
 — entry entry-id [create]
 — entry entry-id
 — no entry entry-id
 — aa-sub transit-aasub-name
 — no aa-sub
 — match
 — aa-sub-ip ip-address[/mask]
 — no aa-sub-ip
 — network-ip ip-address[/mask]
 — no network-ip
 — static-aa-sub transit-aasub-name
 — static-aa-sub transit-aasub-name app-profile app-profile-name
 [create]
 — no static-aa-sub transit-aasub-name

```

- **static-remote-aa-sub** *transit-aasub-name*
- **static-remote-aa-sub** *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
- **no static-remote-aa-sub** *transit-aasub-name*
- **url-filter** *url-filter-name* [**create**]
- **no url-filter** *url-filter-name*
  - **default-action** **allow**
  - **default-action** **block-all**
  - **default-action** **block-http-redirect** *http-redirect-name*
  - **no default-action**
  - **description** *description-string*
  - **no description**
  - **http-redirect** *http-redirect-name*
  - **no http-redirect**
  - **http-request-filtering** **all** | **first**
  - **icap**
    - **custom-x-header** *custom-x-header-name*
    - **no custom-x-header**
    - **server** *ip-address[:port]* [**create**]
    - **no server** *ip-address[:port]*
      - **description** *description-string*
      - **no description**
      - **[no] shutdown**
    - **vlan-id** *service-port-vlan-id*
    - **no vlan-id**
  - **local-filtering**
    - **[no] url-list** *url-list-name*
- **[no] shutdown**
- **url-list** *url-list-name* [**create**]
- **no url-list** *url-list-name*
  - **decrypt-key** *key* | **hash-key** | **hash2-key** [*hash1* | *hash2*]
  - **no decrypt-key**
  - **description** *description-string*
  - **no description**
  - **file** *file-url*
  - **no file**
  - **[no] shutdown**
  - **size** *url-list-size*
- **wap1x**
  - **[no] shutdown**

### 3.4.1.5 AA Interface Commands

```

config
 — service
 — ies/vprn service-id
 — aa-interface aa-if-name [create]
 — no aa-interface aa-if-name
 — address {ip-address/mask | ip-address netmask}
 — no address [ip-address/mask | ip-address netmask]
 — description description-string

```

- **no description**
- **ip-mtu** *octets*
- **no ip-mtu**
- **sap** *sap-id* [**create**]
- **no sap** *sap-id*
  - **description** *long-description-string*
  - **no description**
  - **egress**
    - **filter ip** *ip-filter-id*
    - **no filter** [**ip** *ip-filter-id*]
    - **qos** *policy-id*
    - **no qos** [*policy-id*]
  - **ingress**
    - **qos** *policy-id*
    - **no qos** [*policy-id*]
  - [**no**] **shutdown**
- [**no**] **shutdown**

### 3.4.1.6 Persistence Commands

- ```

config
  — system
    — persistence
      — application-assurance
        — description description-string
        — no description
        — location flash-id
        — no location

```

3.4.2 Command Descriptions

- [Generic Commands](#)
- [Admin Commands](#)
- [Application Assurance Commands](#)
- [Group Commands](#)
- [Policer Commands](#)
- [Policy Commands](#)
- [Application Filter Commands](#)
- [Application Profile Commands](#)
- [Application QoS Policy Commands](#)
- [Application Service Options Commands](#)
- [Statistics Commands](#)

- [ISA Commands](#)

Application Assurance uses system components for some of its functionality. Refer to the following for details on:

- Configuration of Application Assurance Accounting policy including per accounting type record selection and customization of AA subscriber records.
- Configuration of AA ISA IOM QoS.

3.4.2.1 Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>app-assure>aarp config>app-assure>group config>app-assure>group>statistics>aa-sub config>app-assure>group>cflowd>collector config>app-assure>group>cflowd>dir-exp>collector config>app-assure>group>cflowd>group>cflowd config>app-assure>group>cflowd>group>cflowd>collector config>app-assure>group>cflowd>group>cflowd>volume config>app-assure>group>certificate-profile config>app-assure>group>dns-ip-cache config>app-assure>group>event-log>syslog config>app-assure>group>gtp>gtp-filter config>app-assure>group>http-enrich config>app-assure>group>http-error-redirect config>app-assure>group>http-notification config>app-assure>group>http-redirect config>app-assure>group>ip-prefix-list config>app-assure>group>policer config>app-assure>group>policer>tod-override config>app-assure>group>policy>app-filter>entry config>app-assure>group>policy>app-group config>app-assure>group>policy>application config>app-assure>group>policy>app-profile config>app-assure>group>policy>app-qos-policy>entry config>app-assure>group>policy>aqp>entry config>app-assure>group>policy>aqp>entry>action>url-filter config>app-assure>group>policy>charging-group config>app-assure>group>policy>custom-protocol config>app-assure>group>policy>transit-ip-policy

```
config>app-assure>group>port-list
config>app-assure>group>sctp-filter
config>app-assure>group>session-filter
config>app-assure>group>session-filter>entry
config>app-assure>group>tcp-validate
config>app-assure>group>tod-override
config>app-assure>group>transit-prefix-policy
config>app-assure>group>url-filter
config>app-assure>group>url-filter>icap>server
config>app-assure>group>url-list
config>app-assure>protocol
config>app-assure>rad-acct-plcy
config>isa
config>isa>aa-group
config>service>ies>aa-interface
config>service>vprn>aa-interface
config>system>persistence>application-assurance
```

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Parameters *string* — The description character string, up to 80 characters. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.

description

Syntax **description** *long-description-string*
no description

Context config>service>ies>aa-interface>sap
config>service>vprn>aa-interface>sap

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Parameters *string* — The description character string, up to 160 characters. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	<pre> config>app-assure>aarp config>app-assure>group>cflowd config>app-assure>group>cflowd>collector config>app-assure>group>cflowd>comprehensive config>app-assure>group>cflowd>rtp-performance config>app-assure>group>cflowd>tcp-performance config>app-assure>group>cflowd>volume config>app-assure>group>certificate-profile config>app-assure>group>dns-ip-cache config>app-assure>group>event-log config>app-assure>group>gtp config>app-assure>group>http-enrich config>app-assure>group>http-error-redirect config>app-assure>group>http-notification config>app-assure>group>http-redirect config>app-assure>group>policer>tod-override config>app-assure>group>policy>app-filter>entry config>app-assure>group>policy>app-qos-policy>entry config>app-assure>group>policy>custom-protocol config>app-assure>group>statistics>protocol config>app-assure>group>transit-ip-policy>dhcp config>app-assure>group>transit-ip-policy>radius config>app-assure>group>transit-ip-policy>transit-auto-create config>app-assure>group>url-filter config>app-assure>group>url-filter>icap>server config>app-assure>group>url-list config>app-assure>group>wap1x config>app-assure>protocol config>isa>aa-grp config>service>ies>aa-interface config>service>ies>aa-interface config>service>ies>aa-interface>sap config>service>vprn>aa-interface config>service>vprn>aa-interface>sap </pre>
Description	This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command. The shutdown command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

3.4.2.2 Admin Commands

application-assurance

Syntax	application-assurance
Context	admin
Description	This command enables the context to perform Application Assurance (AA) configuration operations.

upgrade

Syntax	upgrade
Context	admin>app-assure
Description	Use this command to load a new isa-aa.tim file as part of a router-independent signature upgrade. An AA ISA reboot is required.

3.4.2.3 Application Assurance Commands

aarp

Syntax	aarp aarpId [create] no aarp aarpId
Context	config>application-assurance
Description	This command defines an Application Assurance Redundancy Protocol (AARP) instance. This instance is paired with the same <i>aarpId</i> in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP. The no form of the command removes the instance from the configuration.
Parameters	<i>aarpId</i> — An integer that identifies an AARP instance. Values 1 to 65535 create — Keyword used to create the AARP instance.

master-selection-mode

Syntax	master-selection-mode <i>mode</i>		
Context	config>app-assure>aarp		
Description	This command configures the AARP mode of operation with the peer instance. The modes affect the AARP state machine behavior according to the desired behavior. Minimize-switchover will change AARP state based on Master ISA failure, and be non-revertive in that when the priority ISA returns a switch does not occur, which is optimal for AA flow identification. Inter-chassis efficiency mode considers both priority (revertive) and the endpoint status of the AARP instance and will switch activity in case of EP failure in order to avoid sending all the traffic over the ICL. The priority-based-balance mode will be revertive after a priority master returns to service, but excludes EP status. The master-selection-mode configuration must match on both peer AARP instances, or the AARP operational status will stay down.		
Default	master-selection-mode minimize-switchovers		
Parameters	<i>mode</i> — Specifies the AARP master selection mode. <table data-bbox="451 907 1377 1081"> <tr> <td>Values</td><td> minimize-switchovers — Optimal AA flow detection continuity by minimizing AARP switchovers. inter-chassis-efficiency — Minimizes inter-chassis traffic. priority-based-balance — AA load balance between AARP peers based on configured priority. </td></tr> </table>	Values	minimize-switchovers — Optimal AA flow detection continuity by minimizing AARP switchovers. inter-chassis-efficiency — Minimizes inter-chassis traffic. priority-based-balance — AA load balance between AARP peers based on configured priority.
Values	minimize-switchovers — Optimal AA flow detection continuity by minimizing AARP switchovers. inter-chassis-efficiency — Minimizes inter-chassis traffic. priority-based-balance — AA load balance between AARP peers based on configured priority.		

peer

Syntax	peer <i>ip-address</i> no peer
Context	config>app-assure>aarp
Description	This command defines the IP address of the peer router which must be a routable system IP address. If no peer is configured and the AARP is no shutdown, it is configured as a single node AARP instance. The no form of the command removes the IP address from the AARP instance.
Default	no peer
Parameters	<i>ip-address</i> — Specifies the IP address in the a.b.c.d format.

peer-endpoint

Syntax	peer-endpoint sap <i>sap-id</i> encap-type { dot1q null qinq } peer-endpoint spoke-sdp <i>sdp-id:vc-id</i> no peer-endpoint
Context	config>app-assure>aarp
Description	This command defines the peer endpoint ID of the SAP or spoke-SDP parent-aa-sub of the AARP peer. The no form of the command removes the peer endpoint from the AARP instance.
Default	no peer-endpoint
Parameters	<i>sap-id</i> — Specifies the physical port identifier portion of the SAP definition. <i>sdp-id:vc-id</i> — Specifies the spoke SDP ID and VC ID. Values 1 to 32767 1 to 4294967295 dot1q null qinq — Specifies the encapsulation type.

priority

Syntax	priority <i>value</i> no priority
Context	config>app-assure>aarp
Description	This command defines the priority for the AARP instance. The priority value is used to determine the master/backup upon initialization or re-balance. The no form of the command reverts to the default value.
Default	priority 100
Parameters	<i>value</i> — Specifies an integer that defines the priority of an AARP instance. Values 0 to 255

bit-rate-high-wmark

Syntax	bit-rate-high-wmark <i>high-watermark</i>
Context	config>application-assurance
Description	This command configures the high watermark for bit rate alarms.

Default	bit-rate-high-wmark max
Parameters	<i>high-watermark</i> — Specifies the high watermark for bit rate alarms, in Mb/s. The value must be larger than or equal to the low watermark value.
Values	1 to 40000, max (disabled)

bit-rate-low-wmark

Syntax	bit-rate-low-wmark <i>low-watermark</i> no bit-rate-low-wmark
Context	config>application-assurance
Description	This command configures the utilization of the flow records on the ISA-AA Group when the full alarm will be cleared by the agent.
Default	bit-rate-low-wmark 0
Parameters	<i>low-watermark</i> — Specifies the low watermark for bit rate alarms, in Mb/s. The value must be lower than or equal to the high watermark value.
Values	0 to 39999

datapath-cpu-high-wmark

Syntax	datapath-cpu-high-wmark <i>high-watermark</i> datapath-cpu-high-wmark max
Context	config>app-assure
Description	This command configures the system-wide high watermark threshold as a percentage of the per-ISA datapath core CPU utilization, where an alarm will be raised by the agent. CPU usage is the average usage across all datapath cores.
Default	datapath-cpu-high-wmark 95
Parameters	<i>high-watermark</i> — Specifies the high watermark for datapath CPU usage alarms.
Values	1 to 100
	max — Disables the high watermark for datapath CPU usage alarms

datapath-cpu-low-wmark

Syntax	datapath-cpu-low-wmark <i>low-watermark</i>
Context	config>app-assure

Description	This command configures the system-wide low watermark threshold as a percentage of the per-ISA datapath core CPU utilization, where an alarm will be raised by the agent. CPU usage is the average usage across all datapath cores.
Default	datapath-cpu-low-wmark 90
Parameters	<i>low-watermark</i> — Specifies the low watermark for datapath CPU usage alarms.
Values	1 to 100

packet-rate-high-wmark

Syntax	packet-rate-high-wmark <i>high-watermark</i>
Context	config>app-assure
Description	This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent.
Default	packet-rate-high-wmark max
Parameters	<i>high-watermark</i> — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the packet-rate-low-wmark value.
Values	1 to 59523808, max packets/sec (disabled)

packet-rate-low-wmark

Syntax	packet-rate-low-wmark <i>low-watermark</i> no packet-rate-low-wmark
Context	config>app-assure
Description	This command configures the system wide low watermark threshold for per-ISA throughput in packets/second when an high packet rate alarm will be cleared by the agent. The value must be less than or equal to the packet-rate-high-wmark parameter. The no form of the command sets the parameter to minimum (watermark disabled).
Default	packet-rate-low-wmark 0
Parameters	<i>low-watermark</i> — Specifies the low watermark for packet rate alarms. The value must be lower than or equal to the packet-rate-high-wmark value.
Values	0 to 59523807 packets/sec

flow-setup-high-wmark

Syntax	flow-setup-high-wmark <i>high-watermark</i>
Context	config>app-assure
Description	This command configures the system wide high watermark threshold for per-ISA throughput in packets/second when an alarm will be raised by the agent. The value must be larger than or equal to the packet-rate-low-wmark parameter.
Default	flow-setup-high-wmark max
Parameters	<i>high-watermark</i> — Specifies the high watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-low-wmark value. Values 1 to 800000, max flows/sec (disabled)

flow-setup-low-wmark

Syntax	flow-setup-low-wmark <i>low-watermark</i> no flow-setup-low-wmark
Context	config>app-assure
Description	This command configures the flow setup rate on the ISA-AA when a flow setup alarm will be raised by the agent.
Default	flow-setup-low-wmark 0
Parameters	<i>low-watermark</i> — Specifies the low watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-high-wmark value. Values 1 to 799999 flows/sec

application-assurance

Syntax	application-assurance
Context	config
Description	This command enables the context to perform Application Assurance (AA) configuration operations.

flow-table-high-wmark

Syntax	flow-table-high-wmark <i>high-watermark</i> no flow-table-high-wmark

Context	config>app-assure				
Description	This command configures the system-wide high watermark threshold as a percentage of the flow table size for the per-ISA utilization of the flow records when a full alarm will be raised by the agent.				
Default	flow-table-high-wmark 95				
Parameters	<i>high-watermark</i> — Specifies the high watermark for flow table full alarms, in percent. <table><tr><td>Values</td><td>0 to 100</td></tr><tr><td>Default</td><td>95</td></tr></table>	Values	0 to 100	Default	95
Values	0 to 100				
Default	95				

flow-table-low-wmark

Syntax	flow-table-low-wmark <i>low-watermark</i> no flow-table-low-wmark				
Context	config>app-assure				
Description	This command configures the system-wide low watermark threshold as a percentage of the flow table size for per-ISA. The value must be lower than or equal to the flow-table-high-wmark <i>high-watermark</i> parameter.				
Default	flow-table-low-wmark 90				
Parameters	<i>low-watermark</i> — Specifies the low watermark for flow table full alarms, in percent. <table><tr><td>Values</td><td>0 to 100</td></tr><tr><td>Default</td><td>90</td></tr></table>	Values	0 to 100	Default	90
Values	0 to 100				
Default	90				

protocol

Syntax	protocol <i>protocol-name</i>
Context	config>app-assure
Description	This command configures the shutdown of protocols system-wide.
Parameters	<i>protocol-name</i> — A string of up to 32 characters identifying a predefined protocol.

group

Syntax	group <i>aa-group-id[:partition-id]</i> [create] no group <i>aa-group-id:partition-id</i>
Context	config>app-assure

Description	This command configures and enables the context to configure an application assurance group and partition parameters.
Parameters	<i>aa-group-id</i> — Specifies a group of ISA MDAs. Values 1 to 255 <i>partition-id</i> — Specifies a partition within a group. Values 1 to 65535 create — Keyword used to create the partition in the group.

aa-sub-remote

Syntax	[no] aa-sub-remote
Context	config>app-assure>group
Description	This command specifies whether or not the from subscriber and to subscriber traffic direction is reversed for this group-partition.
Default	no aa-sub-remote

cflowd

Syntax	cflowd
Context	config>app-assure>group
Description	This command enables the context to configure cflowd parameters for the application assurance group.

certificate-profile

Syntax	certificate-profile <i>cert-prof-name</i> [create] no certificate-profile <i>cert-prof-name</i>
Context	config>app-assure>group
Description	This command creates a certificate profile to be used for certificate-based encryption in HTTP header enrichment. The no form of this command removes the certificate profile.
Parameters	<i>cert-profile-name</i> — Specifies the name of the profile, up to 32 characters.

certificate

Syntax	certificate <i>certificate-file</i> no certificate
Context	config>app-assure>group>certificate-profile
Description	This command indicated the file name of the certificate to be added to the profile. The no form of this command removes the certificate from the profile.
Default	no certificate
Parameters	<i>certificate-file</i> — Specifies the name of the certificate file, up to 95 characters.

disable-deferred-billing

Syntax	[no] disable-deferred-billing
Context	config>app-assure>group
Description	This command disables deferred billing.

dns-ip-cache

Syntax	dns-ip-cache <i>dns-ip-cache-name</i> [create] no dns-ip-cache <i>dns-ip-cache-name</i>
Context	config>app-assure>group
Description	This command configures a DNS IP cache used to snoop DNS requests generated by subscribers to populate a cache of IP addresses matching a specified list of domain names. In the context of URL content charging strengthening, it is also mandatory to specify a list of trusted DNS servers to populate the DNS IP cache.
Parameters	<i>dns-ip-cache-name</i> — Specifies the Application Assurance DNS IP cache name. create — Specifies a keyword used to create the DNS IP cache.

dns-match

Syntax	dns-match
Context	config>app-assure>group>dns-ip-cache
Description	This command enters the context to configure match parameters in the DNS IP cache.

domain

Syntax	domain <i>domain-name</i> expression <i>expression</i> no domain <i>domain-name</i>
Context	config>app-assure>group>dns-ip-cache>dns-match
Description	This command configures a domain expression to populate the DNS IP cache. Up to 32 domains can be configured.
Parameters	<i>domain-name</i> — Specifies the name of the domain expression entry. <i>expression</i> — Specifies a domain name expression string, up to 64 characters, used to define a pattern match. This domain expression uses the same syntax as the expressions used in app-filters.

server-address

Syntax	server-address <i>server-address</i> [name <i>server-name</i>] no server-address <i>server-address</i>
Context	config>app-assure>group>dns-ip-cache>dns-match
Description	This command configures a DNS server address. DNS responses from this DNS server are used to populate the dns-ip-cache. Up to 64 server addresses can be configured.
Parameters	<i>server-address</i> — Specifies the IPv4 or IPv6 address of the DNS.
	Values
	ipv4-address a.b.c.d[/mask] mask - [1 to 32]
	ipv6-address x:x:x:x:x:x:prefix-length x:x:x:x:x:d.d.d.d x - [0 to FFFF]H d - [0 to 255]D prefix-length [1 to 128]
	<i>server-name</i> — Specifies an optional server name for a given server address.

ip-cache

Syntax	ip-cache
Context	config>app-assure>group>dns-ip-cache
Description	This command configures the dns-ip-cache cache parameters.

high-wmark

Syntax	high-wmark <i>percent</i>
Context	config>app-assure>group>dns-ip-cache>ip-cache
Description	This command configures the high watermark value for the DNS IP cache. When the number of IP addresses stored in the cache crosses above this threshold, the system will generate a trap.
Default	high-wmark 90
Parameters	<i>percent</i> — Specifies the high watermark value, in percent
Values	0 to 100
Default	90

low-wmark

Syntax	low-wmark <i>percent</i>
Context	config>app-assure>group>dns-ip-cache>ip-cache
Description	This command configures the low watermark value for the dns-ip-cache. If the dns-ip-cache has previously crossed the high-watermark value, the system will clear the trap in case the number of IP addresses stored in the cache crosses below the low watermark value.
Default	low-wmark 80
Parameters	<i>percent</i> — Specifies the low watermark value, in percent.
Values	0 to 100
Default	80

size

Syntax	size <i>cache-size</i>
Context	config>app-assure>group>dns-ip-cache>ip-cache
Description	This command configures the maximum number of entries in the cache.
Default	size 10
Parameters	<i>cache-size</i> — Specifies the maximum number of IP addresses that can be stored in the cache.
Values	10 to 32000
Default	10

static-address

Syntax	[no] static-address { <i>ip-address</i> <i>ipv6-address</i> }
Context	config>app-assure>group>dns-ip-cache>ip-cache
Description	This command configures a static address in the cache.
Parameters	<i>ip-address</i> <i>ipv6-address</i> — Specifies a character string up to 64 characters.

collector

Syntax	collector <i>ip-address[:port]</i> [create] no collector <i>ip-address[:port]</i>
Context	config>app-assure>group>cflowd
Description	This command defines a flow data collector for cflowd data. The IP address of the flow collector must be specified. The UDP port number is an optional parameter. If it is not set, the default of 2055 is used.
Parameters	<i>ip-address</i> — Specifies the IP address of the flow data collector in dotted decimal notation. <i>port</i> — Specifies the UDP port of flow data collector. Values 1 to 65535 Default 2055 create — Keyword used to create the flow data collector.

comprehensive

Syntax	comprehensive
Context	config>app-assure>group>cflowd
Description	This command enables the context to configure cflowd comprehensive statistics output parameters.

direct-export

Syntax	direct-export
Context	config>app-assure>group>cflowd
Description	This command enables the context to perform configuration related to the export of AA cflowd records directly inband from AA instead of going through the CPM.

collector

Syntax	collector <i>collector-id</i> [create] no collector <i>collector-id</i>
Context	config>app-assure>group>cflowd>dir-exp
Description	This command configures the cflowd direct export collector. Only one collector can be configured.
Default	none
Parameters	<i>collector ID</i> — the ID of the Cflowd direct export collector Values 1 to 65535 create — keyword to create the collector

address

Syntax	[no] address <i>ip-address</i> [: <i>port</i>]
Context	config>app-assure>group>cflowd>dir-exp-coll
Description	This command configures cflowd direct export collector remote address. Two addresses can be configured for each “collector” for redundancy. AA sends the same records to both at the same time.
Default	No default ip-address. Default port is 4739.
Parameters	<i>ip-address</i> — a.b.c.d Values port: 1 to 65535

vlan-id

Syntax	vlan-id <i>service-port-vlan-id</i> no vlan-id
Context	config>app-assure>group>cflowd>dir-exp
Description	This command configures the VLAN ID on which the ISA-AA is expected to be emitting traffic.
Default	none
Parameters	<i>service-port-vlan-id</i> — Specifies the VLAN ID value. Values 1 to 4094

export-override

Syntax	export-override <i>mode</i> no export-override
Context	configure>application-assurance>group>cflowd
Description	This command configures the AA sub-type used in cflowd record export. The cflowd stats exported to the cflowd collector to look identical to when AA is on the type of system defined by the mode. The following cflowd export fields are affected: - cflowd export observation point (field 138), the mode will be derived from the export-override category that is selected. - cflowd export AA_Subscriber_Type (field 12) modified as configured, using existing field types. - cflowd interface name is used as the sub-ID field, optionally modified to use the export-override mode prefix as a global identifier. All AA cflowd record types are affected by export-override. To change any of the export-override and/or prefix, cflowd must be shutdown first. When the export-override is set back to default (no export-override) the prefix will also be set back to default. The no form of the command removes the export override.
Default	no export-override
Parameters	<i>mode</i> — The type of system emulated by stats export. Values mobile (mobile gateway mode, cflowd field 138 = 2)

prefix

Syntax	prefix <i>prefix-string</i> no prefix
Context	config>application-assurance>group>cflowd>export-override
Description	This command specifies the <i>prefix-string</i> associated with the export-override .
Parameters	<i>prefix-string</i> — Up to an 8 character string. If the 8 character prefix is "ABCDEFGG_" for a particular node, the cflowd export override would generate IPv4 interface names such as ABCDEFGG_255.255.255.255 or IPv6 as ABCDEFGG_2001:DB8:EF01:2345::/64. By default the prefix will be left blank.

rtp-performance

Syntax	rtp-performance
Context	config>app-assure>group>cflowd
Description	This command configures the cflowd RTP performance export.

event-log

Syntax	event-log <i>event-log-name</i> [create] no event-log <i>event-log-name</i>
Context	config>app-assure>group
Description	This command configures an event log.
Parameters	<i>event-log-name</i> — Specifies the name of the event log.

buffer-type

Syntax	buffer-type <i>buffer-type</i>		
Context	config>app-assure>group>evt-log		
Description	This command specifies the type of buffer to be used in the event log.		
Default	buffer-type linear		
Parameters	<i>buffer-type</i> — Specifies the type of event type. <table><tr><td>Values</td><td>linear — Specifies a linear buffer which once full will stop recording events until it is cleared circular — Specifies a circular buffer whereby older entries will be overwritten by newer entries syslog—Specifies that events are stored offline on a syslog host</td></tr></table>	Values	linear — Specifies a linear buffer which once full will stop recording events until it is cleared circular — Specifies a circular buffer whereby older entries will be overwritten by newer entries syslog —Specifies that events are stored offline on a syslog host
Values	linear — Specifies a linear buffer which once full will stop recording events until it is cleared circular — Specifies a circular buffer whereby older entries will be overwritten by newer entries syslog —Specifies that events are stored offline on a syslog host		

max-entries

Syntax	max-entries <i>max-entries</i> no shutdown
Context	config>app-assure>group>evt-log
Description	This command configures the number of entries in the buffer.
Default	max-entries 500

Parameters	<i>max-entries</i> — Specifies the maximum number of entries for the event log.
Values	1 to 100000
Default	500

syslog

Syntax	syslog
Context	config>app-assure>group>evt-log
Description	This command enables the context for configuring the target Syslog server.

address

Syntax	address <i>ip-address</i> no address
Context	config>app-assure>group>evt-log>syslog
Description	This command configures the target syslog host IP address.
Default	no address
Parameters	<i>ip-address</i> — Specifies the IP address of the target syslog host, either IPv4 or IPv6.
Values	ipv4-address a.b.c.d ipv6-address x:x:x:x:x:x:x:x x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

facility

Syntax	facility <i>syslog-facility</i>
Context	config>app-assure>group>evt-log>syslog
Description	This command configures the syslog facility. The syslog facility is an information field associated with a syslog message. It is defined by the syslog protocol and provides an indication of which part of the system originated the message.
Default	facility local7

Parameters	<i>syslog-facility</i> — Specifies the syslog facility keyword.
Values	kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

port

Syntax	port <i>port</i>
Context	config>app-assure>group>event-log>syslog
Description	This command specifies the UDP port used by application assurance to inject the syslog events inband.
Default	port 514
Parameters	<i>port</i> — Specifies the UDP port number.
Values	0 to 65535

severity

Syntax	severity <i>syslog-severity</i>
Context	config>app-assure>group>evt-log>syslog
Description	This command configures the syslog message severity level threshold.
Default	severity info
Parameters	<i>syslog-severity</i> — Specifies the severity level for the syslog message.
Values	emergency, alert, critical, error, warning, notice, info, debug

vlan-id

Syntax	vlan-id <i>service-port-vlan-id</i> no vlan-id
Context	config>app-assure>group>evt-log>syslog
Description	This command configures the service port VLAN ID to be used by application assurance to inject the syslog events inband. This VLAN ID needs also to be configured for application assurance interface.
Default	no vlan-id

Parameters *service-port-vlan-id* — Specifies the service port VLAN identifier.

Values 1 to 4094

app-group

Syntax **app-group** *app-group-name* [*rate*]
no app-group *app-group-name*

Context config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance
config>app-assure>group>cflowd>comprehensive

Description This command configures application groups to export performance records with cflowd.

The **no** form of the command removes the parameters from the configuration.

Parameters *app-group-name* — Specifies the application group name.

rate — Specifies which sampling flow rate to use; flow-rate or flow-rate2.

Values flow-rate, flow-rate2

Default flow-rate

application

Syntax **application** *application-name* [*rate*]
no application *application-name*

Context config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance
config>app-assure>group>cflowd>comprehensive

Description This command configures applications to export performance records with cflowd.

The **no** form of the command removes the parameters from the configuration.

Parameters *application-name* — Specifies the name defined for the application.

rate — Specifies which sampling flow rate to use; flow-rate or flow-rate2.

Values flow-rate, flow-rate2

Default flow-rate

flow-rate

Syntax **flow-rate** *sample-rate*

no flow-rate

Context	config>app-assure>group>cflowd>rtp-performance config>app-assure>group>cflowd>tcp-performance config>app-assure>group>cflowd>comprehensive
Description	This command specifies the per-flow sampling rate for the cflowd export of Application Assurance performance statistics. The no form of the command reverts to the default.
Default	no flow-rate
Parameters	<i>sample-rate</i> — Specifies the rate at which to sample flows that are eligible for TCP performance measurement. Values 1 to 1000

flow-rate2

Syntax	flow-rate2 <i>sample-rate</i> no flow-rate2
Context	config>app-assure>group>cflowd>rtp-performance config>app-assure>group>cflowd>tcp-performance config>app-assure>group>cflowd>comprehensive
Description	This command specifies the per-flow second sampling rate for the cflowd export of Application Assurance performance statistics. The no form of the command reverts to the default.
Default	no flow-rate2
Parameters	<i>sample-rate</i> — Specifies the rate at which to sample flows that are eligible for TCP and/or RTP performance measurement. Values 1 to 1000

template-retransmit

Syntax	template-retransmit <i>seconds</i> no template-retransmit
Context	config>app-assure>group>cflowd
Description	This command configures the period of time, in seconds, for the template to be retransmitted.
Default	template-retransmit 600

Parameters	<i>seconds</i> — Specifies the time period for the template to be retransmitted.
Values	10 to 600
Default	600

tcp-performance

Syntax	tcp-performance
Context	config>app-assure>group>cflowd
Description	This command enables the context to configure Cflowd TCP performance export parameters.

volume

Syntax	volume
Context	config>app-assure>group>cflowd
Description	This command configures the cflowd volume export.

rate

Syntax	rate <i>sample-rate</i> no rate
Context	config>app-assure>group>cflowd>volume
Description	This command configures the sampling rate of packets for the cflowd export of application assurance volume statistics. The no form of the command reverts to the default value.
Parameters	<i>sample-rate</i> — Specifies the rate at which to sample packets for the cflowd export of application assurance volume statistics. Values 1 to 10000

tls-extension

Syntax	[no] tls-extension
Context	config>app-assure>group>http-enrich
Description	This command enables the context to configure the TLS extension field name.

extension-id

Syntax	extension-id <i>extension-id</i> no extension-id
Context	config>app-assure>group>http-enrich>tls-extension
Description	This command configures an extension ID to be used for the customized extension. The no form of the command removes the extension ID.
Default	extension-id 17516
Parameters	<i>extension-id</i> — Specifies an extension ID Values 1 to 65535

subtype

Syntax	[no] subtype <i>tls extension subtype</i>
Context	config>app-assure>group>http-enrich>tls-extension
Description	This command configures a TLS subtype. The no form of the command removes the TLS subtype from the configuration.
Parameters	<i>tls extension subtype</i> — Specifies a TLS subtype, up to 32 characters

encode

Syntax	encode type <i>type</i> key <i>key</i> <i>hash-key</i> <i>hash2-key</i> [hash hash2] no encode
Context	config>app-assure>group>http-enrich>tls-extension>subtype
Description	This command configures how the HTTP header enrichment TLS extension TLS subtype will be encoded. The no form of the command removes the values from the configuration.
Parameters	<i>type</i> — Specifies the type of encoding that will be used on the field Values md5, rc4 <i>key</i> — Specifies the key associated with the encode method for the field name <i>hash-key</i> — Specifies the first hashed key <i>hash-key2</i> — Specifies the second hashed key

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

http-error-redirect

Syntax	http-error-redirect <i>redirect-name</i> [create] no http-error-redirect <i>redirect-name</i>
Context	config>app-assure>group
Description	This command configures an HTTP error redirect policy. The policy contains important information relevant to the redirect server. The no form of the command removes the redirect name from the group configuration.
Parameters	<i>redirect-name</i> — Specifies a string, up to 32 characters, that identifies the HTTP error redirect policy. create — Keyword to create the HTTP error redirect policy.

error-code

Syntax	error-code <i>error-code</i> [custom-msg-size <i>custom-msg-size</i>] no error-code <i>error-code</i>
Context	config>app-assure>group>http-error-redirect
Description	This command refers to which HTTP status codes a redirect action is applied. Only messages with sizes less than that configured here (<i>custom-msg-size</i>) are eligible for redirect action. The no form of the command removes the parameters from the configuration.
Parameters	<i>error-code</i> — Specifies the error code for an HTTP error redirect. Values 0 to 4294967295, of which 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 730, 731, and 735 are supported for redirect

custom-msg-size — Specifies the maximum message size above which redirect will not be done.

Values 0 to 4294967295

http-host

Syntax	http-host <i>http-host</i> no http-host
Context	config>app-assure>group>http-error-redirect
Description	This command refers to the http host name of the landing server (Barefruit or Xerocole). It is used in the HTTP GET operation from the client (which is being redirected) to the redirect search landing server. It must contain a valid IP address or HTTP host name / URI for the HTTP GET from the client to the landing server to work. The no form of the command removes the HTTP host string from the configuration.
Default	no http-host
Parameters	<i>http-host</i> — Specifies a string of 255 chars max length, that refers to the HTTP host name of the landing server (barefruit or xerocole).

participant-id

Syntax	participant-id <i>participant-id</i> no participant-id
Context	config>app-assure>group>http-error-redirect
Description	This command specifies a 32-character string assigned to the operator by Barefruit. It is used by barefruit landing servers (applies to template # 1 only).
Default	no participant-id
Parameters	<i>participant-id</i> — Specifies the 32-character string supplied by Barefruit.

template

Syntax	template <i>template-id</i> no template
Context	config>app-assure>group config>app-assure>group>http-error-redirect

Description	This command refers to the template of parameters passed from the AA-ISA to the redirect server via JavaScript in the redirect packet. The template is specific to the redirect server being used in the network. Currently, two partners are used and tested with AA-ISA redirect solution, Barefruit and Xerocole. The no form of the command reverts to the default.
Default	1 = referring to redirect format for Barefruit landing server.
Parameters	<i>template-id</i> — Specifies an HTTP error redirect template. 1 = Barefruit specific template 2 = xerocole.specific template.
Values	0 to 4294967295

http-match-all-requests

Syntax	[no] http-match-all-requests
Context	config>app-assure>group config>app-assure>group>policy>app-filter>entry
Description	This command enables HTTP matching for all requests for a given HTTP expression. The no form of the command restores the default (removes http-match-all-request for this particular expression) by this app-filter entry).
Default	no http-match-all-requests

http-notification

Syntax	http-notification <i>http-notification-name</i> [create] no http-notification <i>http-notification-name</i>
Context	config>app-assure>group
Description	This command configures an http-notification object for subscriber in browser notification. The no form of the command removes the http notification policy from the configuration.
Parameters	<i>http-notification-name</i> — Specifies the name of the HTTP Notification policy. create — Specifies the mandatory keyword to create the policy.

interval

Syntax	interval { one-time <i>minimum-interval</i> }
Context	config>app-assure>group>http-notif
Description	This command configures the minimum interval in between notification messages. It can be set to one-time or a value in minutes from 1 to 1440. The no form of the command removes the interval from the http-notification policy.
Default	interval one-time
Parameters	<i>minimum-interval</i> — Represents the minimum interval value in minutes in between two http notifications. Values 1 to 1440

script-url

Syntax	script-url <i>script-url-name</i> no script-url
Context	config>app-assure>group>http-notif
Description	This command configures the URL of the script used by the http notification policy. The no form of the command removes the script URL from the http-notification policy.
Default	no script-url
Parameters	<i>script-url-name</i> — Specifies the string representing the URL of the script used in the http notification policy, up to 255 characters. create — Keyword to create the script URL.

template

Syntax	template <i>value</i> no template
Context	config>app-assure>group>http-notif
Description	This command configures the template which defines the format and parameters included in the http notification message. The no form of the command removes the template from the configuration.
Default	no template

Parameters	<i>value</i> — Specifies the template id of this HTTP Notification.
Values	1 — Javascript-url with SubID and optional Http-Url-Param 2 — Javascript-url and optional Http-Url-Param

http-redirect

Syntax	http-redirect <i>redirect-name</i> [create] no http-redirect <i>redirect-name</i>
Context	config>app-assure>group
Description	This command configures an HTTP redirect. The no form of the command removes the HTTP redirect policy from the configuration.
Parameters	<i>redirect-name</i> — Specifies the HTTP redirect that will be applied. If no redirect name is specified, then HTTP redirect is not enabled. create — Keyword to create the HTTP redirect policy.

captive-redirect

Syntax	captive-redirect
Context	config>app-assure>group>http-redirect
Description	This command configures the captive redirect capability for an HTTP redirect policy. HTTP redirect policies using captive redirect can be used in conjunction with a session filter policy and will terminate TCP flows in the ISA-AA card before reaching the Internet to redirect subscribers to the predefined redirect URL. Non-HTTP TCP flows are TCP reset. Captive redirect uses the provisioned VLAN id to send the HTTP response to subscribers; therefore this VLAN id must be properly assigned in the same VPN as the subscriber. The operator can select the URL arguments to include in the redirect URL using either a specific template id or by configuring the redirect URL using one of the supported macro substitution keywords.

vlan-id

Syntax	vlan-id <i>service-port-vlan-id</i> no vlan-id
Context	config>app-assure>group>http-redirect>captive-redirect
Description	This command configures the VLAN id for captive redirect. Captive redirect uses the provisioned VLAN id to send the HTTP response to subscribers; therefore this VLAN id must be properly assigned in the same VPN as the subscriber.

Parameters *service-port-vlan-id* — Specifies the vlan-id.

Values 1 to 4094

redirect-https

Syntax **redirect-https**
no redirect-https

Context config>app-assure>group>http-redirect

Description This command configures the http-redirect policy to redirect HTTPS sessions to the configured redirect-url.

The **no** form of the command removes the redirect-https.

redirect-url

Syntax **redirect-url** *redirect-url*
no redirect-url

Context config>app-assure>group>http-redirect

Description This command configures the http redirect URL which is the URL (page) that the user is redirected to when an HTTP redirect takes effect.

The operator can select the URL arguments to include in the redirect-url using either a specific template-id or by configuring the redirect-url using any of the supported macro substitution keywords. Only ESM and ESM-MAC sub types support \$MAC, \$SAP, \$CID, and \$RID macro substitution.

The **no** form of the command removes the redirect-url field from the configuration.

Parameters *redirect-url* — Specifies the URL of the landing page

Values **macro substitutions:**

\$URL	The Request-URI in the HTTP GET Request received.
\$SUB	A string that represents the subscriber ID.
\$IP	A string that represents the IP address of the subscriber host.
\$RTRID	A string that represents the router ID.
\$URLPRM	The HTTP URL parameter associated with the subscriber.
\$MAC	A string that represents the MAC address of the subscriber host.
\$SAP	A string that represents a SAP ID.
\$CID	A string that represents the circuit-id or interface-id of the subscriber host (hexadecimal format).

\$RID A string that represents the remote-id of the subscriber host (hexadecimal format).

tcp-client-reset

Syntax **[no] tcp-client-reset**

Context config>app-assure>group>http-redirect

Description This command enables an HTTP-redirect policy to initiate a TCP reset towards the client if the AA policy results in a redirect with packet drop but the http redirect cannot be delivered. Scenarios for this include HTTPs (TLS) sessions, blocking of non-HTTP TCP traffic, and blocking of existing flows after a policy re-evaluate of an existing subscriber.

 The **no** form of the command disables the command.

template

Syntax **template** *template-id*
no template

Context config>app-assure>group>http-redirect

Description This command configures the template that defines which parameters are appended to the HTTP host redirect field in the redirect message.

 The HTTP redirect template provides HTTP 302 redirect containing only the URL specified in the redirect policy, with no other parameters.

 The **no** form of the command removes the template from the configuration.

Default no template

Parameters *template-id* — Specifies the HTTP Policy Redirect template.

Values

- 1 — Javascript based redirect embedded in HTTP 200 OK response with a predefined number of arguments automatically appended to the redirect URL
- 2 — HTTP 302 Redirect with a predefined number of arguments automatically appended to the redirect URL.
- 3 — HTTP 302 Redirect with no parameters appended to the URL (empty).
- 4 — Empty Redirect format using Javascript.
- 5 — Redirect supporting macro substitution using HTTP 302.
- 6 — Redirect supporting macro substitution using Javascript.

http-x-online-host

Syntax	[no] http-x-online-host
Context	config>app-assure>group
Description	This command specifies whether X-Online-Host header field is used as a replacement for the HTTP Host header field. The no form of the command disables the use of X-Online-Host header field used as a replacement.
Default	no http-x-online-host

ip-prefix-list

Syntax	ip-prefix-list <i>ip-prefix-list-name</i> [create] no ip-prefix-list <i>ip-prefix-list-name</i>
Context	config>app-assure>group
Description	This command configures an IP prefix list.
Parameters	<i>ip-prefix-list-name</i> — Specifies the name of the IP prefix list, up to 32 characters. create — Mandatory keyword used when creating an application profile. The create keyword requirement can be enabled or disabled in the environment>create context.

prefix

Syntax	prefix <i>ip-prefix/ip-prefix-length</i> [name <i>prefix-name</i>] no prefix <i>ip-prefix/ip-prefix-length</i>								
Context	config>app-assure>group>ip-prefix-list								
Description	This command configures an IP prefix within the list. The no form of the command removes the IP prefix from the configuration.								
Parameters	<i>ip-prefix/ip-prefix-length</i> — The IP address in dotted decimal notation. <table><tr><td colspan="2">Values</td></tr><tr><td><i>ipv4-prefix</i></td><td><i>a.b.c.d</i> (host bits must be 0)</td></tr><tr><td><i>ipv4-prefix-length</i></td><td>0 to 32</td></tr><tr><td><i>ipv6-prefix</i></td><td><i>x:x:x:x:x:x:x</i> (eight 16-bit pieces) <i>x:x:x:x:x:d.d.d.d</i></td></tr></table>	Values		<i>ipv4-prefix</i>	<i>a.b.c.d</i> (host bits must be 0)	<i>ipv4-prefix-length</i>	0 to 32	<i>ipv6-prefix</i>	<i>x:x:x:x:x:x:x</i> (eight 16-bit pieces) <i>x:x:x:x:x:d.d.d.d</i>
Values									
<i>ipv4-prefix</i>	<i>a.b.c.d</i> (host bits must be 0)								
<i>ipv4-prefix-length</i>	0 to 32								
<i>ipv6-prefix</i>	<i>x:x:x:x:x:x:x</i> (eight 16-bit pieces) <i>x:x:x:x:x:d.d.d.d</i>								

	<i>x:</i>	[0 to FFFF]H
	<i>d:</i>	[0 to 255]D
<i>prefix-name</i>	32 characters max	

http-enrich

Syntax	http-enrich <i>http-enrich_name</i> [create] no http-enrich <i>http-enrich_name</i>
Context	config>app-assure>group
Description	This command configures an HTTP enrichment policy. The no form of the command removes the http enrichment policy from the configuration
Parameters	<i>http-enrich-name</i> — Specifies the name of the http enrichment policy up to 32 characters. create — Mandatory keyword used when creating an application profile. The create keyword requirement can be enabled and disabled in the environment>create context.

field

Syntax	[no] field <i>field-name</i>
Context	config>app-assure>group>http-enrich
Description	This command configures what fields to be inserted into the HTTP header. The command is repeated for each field to be inserted. The same field cannot be inserted twice into the header under different header names. The no form of the command removes the specified parameter so that it is not inserted into the http header.
Default	none
Parameters	<i>field-name</i> — Specifies which parameters to inserted into the header. Values subscriber-ip, static-string Where: subscriber-ip: header name for the subscriber IP static-string: header name for inserted string subscriber-id: header name for subscriber ID none

anti-spoof

Syntax	[no] anti-spoof
Context	config>app-assure>group>http-enrich>field
Description	This command configures the HTTP header enrichment anti-spoofing functionality. The no form of the command disables anti-spoofing functionality.
Default	no anti-spoof

encode

Syntax	encode type type key key encode type type key hash-key hash encode type type key hash2-key hash2 encode type type cert-profile cert-profile-name no encode
Context	config>app-assure>group>http-enrich>field
Description	This command configures an HTTP header enrichment template field static string. The no form of the command removes the template field static string.
Default	no static-string
Parameters	<i>type</i> — Specifies whether the parameters are hashed with MD5 or encrypted with RC4 using the configured key, or if certificate-based encryption is used with RSA. Values md5, rc4, certificate <i>key</i> — Specifies the key string, 64 characters maximum. <i>hash-key</i> — Specifies the first hashed key. <i>hash-key2</i> — Specifies the second hashed key. hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified. hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the hash2 encrypted variable cannot be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified. <i>cert-profile-name</i> — Specifies the name of the certificate profile to be used. This profile must have already been created using the certificate-profile command.

name

Syntax	name <i>header-name</i>
Context	config>app-assure>group>http-enrich>field
Description	This command configures an HTTP enrichment template field header name. The no form of the command removes the http enrichment template field header name from the configuration.
Parameters	<i>header-name</i> — Specifies the name of the http enrichment policy. It is inserted before the actual field name (e.g. x-subld = subscriberID).

static-string

Syntax	static-string <i>static-string</i> no static-string
Context	config>app-assure>group>http-enrich>field
Description	This command configures an HTTP header enrichment template field static string. The no form of the command removes the template field static string.
Default	no static-string
Parameters	<i>static-string</i> — Specifies a static string.

3.4.2.4 Group Commands

3.4.2.4.1 Transit Subscriber Commands

transit-ip-policy

Syntax	transit-ip-policy <i>ip-policy-id</i> [create] no transit-ip-policy <i>ip-policy-id</i>
Context	config>app-assure>group
Description	This command defines a transit AA subscriber IP policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of the command deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Parameters *ip-policy-id* — An integer that identifies a transit IP profile entry.

Values 1 to 65535

create — Keyword used to create the entry.

3.4.2.4.2 Policer Commands

policer

Syntax **policer** *policer-name* **type** *type* **granularity** *granularity* [**create**]
policer *policer-name*
no policer *policer-name*

Context config>app-assure>group

Description	This command creates application assurance policer profile of a specified type. Policers can be bandwidth or flow limiting and can have a system scope (limits traffic entering AA ISA for all or a subset of AA subscribers), subscriber scope or granularity (limits apply to each AA subscriber traffic).

The policer type and granularity can only be configured during creation. They cannot be modified. The policer profile must be removed from all AQPs in order to be removed. Changes to policer profile parameters take effect immediately for policers instantiated as result of AQP actions using this profile.

The **no** form of the command deletes the specified policer from the configuration.

Parameters

- policer-name* — Specifies a string of up to 32 characters that identifies the policer.
- type* — Specifies the policer type.

Values	single-bucket-bandwidth — Creates a profile for a single bucket (PIR) bandwidth limiting policer. dual-bucket-bandwidth — Creates profile for a dual bucket (PIR, CIR) bandwidth limiting policer. flow-rate-limit — Creates profile for a policer limiting rate of flow set-ups. flow-count-limit — Creates profile for a policer limiting total flow count.

granularity — Specifies the granularity type.

- Values**
- system** — Creates a system policer profile for a policer that limits the traffic in the scope of all or a subset of AA subscribers on a given AA ISA.
 - subscriber** — Creates a policer profile for a policer for each AA subscriber that limits the traffic in the scope of that subscriber.
 - access-network-location** — Creates a policer profile for a policer instance for each ANL that limits traffic bandwidth in the scope of that ANL. For ANL, only single-bucket bandwidth policers can be configured.

create — Keyword used to create the policer name and parameters.

action

Syntax	action {priority-mark permit-deny}
Context	config>app-assure>group>policer
Description	This command configures the action to be performed by single-bucket bandwidth policers for non-conformant traffic. Dual bucket bandwidth policers cannot have their action configured and always mark traffic below CIR in profile, between CIR and PIR out of profile, and drop traffic above PIR. Flow policers always discard non-conformant traffic. When multiple application assurance policers are configured against a single flow (including policers at both subscriber and system), the final action done to the flow/packet will be a logical OR of all policers actions. For example, if only of the policers requires the packet to be discarded, the packet will be dropped regardless of the action of the other policers.
Default	action permit-deny
Parameters	priority-mark — Non-conformant traffic will be marked out of profile and the conformant traffic will be marked in profile. The new marking will overwrite any previous IOM QoS marking done to a packet. permit-deny — Non-conformant traffic will be dropped.

adaptation-rule

Syntax	adaptation-rule pir {max min closest} [cir {max min closest}] no adaptation-rule
Context	config>app-assure>group>policer

Description	This command defines the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined option. To change the CIR adaptation rule only, the current PIR rule must be part of the command executed. The no form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.
Default	adaptation-rule pir closest cir closest
Parameters	max — The operational PIR or CIR for the queue will be equal to or less than the administrative rate specified using the rate command. min — The operational PIR or CIR for the queue will be equal to or greater than the administrative rate specified using the rate command. closest — The operational PIR or CIR for the queue will be the rate closest to the rate specified using the rate command.

congestion-override

Syntax	congestion-override
Context	config>app-assure>group>policer
Description	This command enables the context to configure per subscriber congestion bandwidth policer override rates.

cbs

Syntax	cbs <i>committed-burst-size</i> cbs congested-cbs no cbs
Context	config>app-assure>group>policer config>app-assure>group>policer>congestion-override config>app-assure>group>tod-override
Description	This command provides a mechanism to configure the committed burst size for the policer. It is recommended that CBS is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. CBS is configurable for dual-bucket bandwidth policers only. The no form of the command resets the CBS value to its default.
Default	no cbs

Parameters *committed-burst-size* | *congested-cbs* — Specifies an integer value defining size, in kbytes, for the CBS of the policer.

Values 0 to 131071

cir

Syntax *cir congested-cir*
no cir

Context config>app-assure>group>policer>congestion-override

Description This command provides a mechanism to configure the CIR for the congestion override policer. It is recommended that the CIR is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. The CIR is configurable for dual-bucket bandwidth policers only.

The **no** form of the command resets the CIR value to its default.

Default cir 0

Parameters *congested-cir* — Specifies an integer value defining size, in kilobytes, for the CIR of the policer.

Values 0 to 100000000

pir

Syntax *pir congested-pir*
no pir

Context config>app-assure>group>policer>congestion-override

Description This command provides a mechanism to configure the PIR for the congestion override policer. It is recommended that the PIR is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic.

The **no** form of the command resets the PIR value to its default.

Default pir 0

Parameters *congested-pir* — Specifies an integer value defining size, in kbytes, for the PIR of the policer.

Values 0 to 100000000

flow-count

Syntax	flow-count <i>flow-count</i> no flow-count
Context	config>app-assure>group>policer config>app-assure>group>tod-override
Description	This command configures the flow count for the flow-count-limit policer. It is recommended to configure flow count subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.
Default	no flow-count
Parameters	<i>flow-count</i> — Specifies the flow count for the flow-count-limit policer. Values 0 to 100000000, max

gtp-traffic

Syntax	[no] gtp-traffic
Context	config>app-assure>group>policer
Description	This command provides a mechanism to configure a policer to function at the GTP tunnel level. GTP tunnels are defined by a TEID and destination IP address as oppose to normal flows that are defined by IP 5 tuple values. By setting this value, the policer then can be used to limit GTP traffic (SeGW GTP firewall application). The no form of the command resets policer behavior to act at the normal 5 tuple flow level and not at the GTP tunnel level
Default	no gtp-traffic

mbs

Syntax	mbs <i>congested-mbs</i> mbs <i>maximum-burst-size</i> no mbs
Context	config>app-assure>group>policer config>app-assure>group>policer>congestion-override config>app-assure>group>tod-override
Description	This command provides a mechanism to configure the maximum burst size for the policer. It is recommended that MBS is configured larger than twice the MTU for the traffic handled by the policer to allow for some burstiness of the traffic. MBS is configurable for single-bucket, dual-bucket bandwidth and flow setup rate policers only.

The **no** form of the command resets the MBS value to its default.

Default	no mbs
Parameters	<i>maximum-burst-size</i> <i>congested-mbs</i> — Specifies an integer value defining either size, in kbytes, for the MBS of the bandwidth policer, or flow count for the MBS of the flow setup rate policers.
Values	0 to 131071

rate

Syntax	rate <i>pir-rate</i> [<i>cir cir-rate</i>] no rate
Context	config>app-assure>group>policer config>app-assure>group>tod-override
Description	This command configures the administrative PIR and CIR for bandwidth policers and flow setup rate limits for flow policers. The actual rate sustained by the flow can be limited by other policers that may be applied to that flow's traffic. This command does not apply to flow-count-limit policers. The cir option is applicable only to dual-bucket bandwidth policers. It is recommended to configure flow setup rate subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers. The no form of the command resets the values to defaults.
Default	rate max cir 0
Parameters	<i>pir-rate</i> — Specifies an integer for the PIR rate in kb/s for bandwidth policers. Values 1 to 100000000, max or flows/sec <i>cir-rate</i> — Specifies an integer for the CIR rate in kb/s. Values 0 to 100000000, max

rate-percentage

Syntax	rate-percentage <i>rate-percentage</i> no rate-percentage
Context	config>app-assure>group>policer
Description	This command indirectly configures the rate used by Access-Network-Location (ANL) policers. Because ANL total bandwidth is dynamically measured and estimated by AA, this command allows the operator to configure the ratio of that measured bandwidth to be used by the ANL policer as the policer rate.

The **no** form of the command resets the values to defaults.

Default	no rate-percentage
Parameters	<i>rate-percentage</i> — Specifies an integer value that specifies a percentage that is applied against the ANL estimate maximum bandwidth to produce the actual rate that is used by the policer when ANL congestion occurs. Values 0 to 200 (0: means drop all traffic) Default 0

tod-override

Syntax	tod-override <i>tod-override-id</i> [create] no tod-override <i>tod-override-id</i>
Context	config>app-assure>group>policer
Description	This commands creates a time of day override policy for a given policer. Up to 8 overrides can be configured per policer. Rate/mbs/cbs/flow-rate/flow-count configured in each override-id will override the default policer values at the specified time of day configured in the override.
Parameters	<i>tod-override-id</i> — Specifies the time of day override ID. Values 1 to 255 create — Keyword used to create the time of day override policy.

time-range

Syntax	time-range daily start <i>start-time</i> end <i>end-time</i> [on day [<i>day</i>]] time-range weekly start <i>start-time</i> end <i>end-time</i> no time-range
Context	config>app-assure>group>tod-override
Description	This command configures up to seven time-ranges applicable to a particular override-id. The time-range can be configured as daily or weekly policies. When using a daily override the operator can select which days during the week from Sunday to Saturday it is applicable along with the start/end hour/min time range repeated over these days. When using a weekly override the operator can select between which days in the week the policy start up to the hours/min for both start day and end day.
Default	no time-range

Parameters	daily	— Schedule the override as a daily occurrence.	
	weekly	— Schedule the override as a weekly occurrence.	
Values			
start-time	daily	<hh>:<mm>	
	weekly	<day>,<hh>:<mm>	
end-time		<hh> : 0..23	
		<mm> : 0 15 30 45	
	daily	<hh>:<mm>	
	weekly	<day>,<hh>:<mm>	
		<hh> 0..23	
		<mm> 0 15 30 45	
day	sunday monday tuesday wednesday thursday friday saturday		

3.4.2.4.3 Policy Commands

policy

Syntax	policy
Context	config>app-assure>group>policy
Description	This command enables the context to configure parameters for application assurance policy. To edit any policy content begin command must be executed first to enter editing mode. The editing mode is left when the abort or commit commands are issued.

abort

Syntax	abort
Context	config>app-assure>group>policy
Description	This command ends the current editing session and aborts any changes entered during this policy editing session.

begin

Syntax	begin
Context	config>app-assure>group>policy

- Description** This command begins a policy editing session.
- The editing session continues until one of the following conditions takes place:
- Abort or commit is issued.
 - Control complex resets.
- The editing session is not interrupted by:
- HA activity switch.
 - CLI session termination (for example, as result of closing a Telnet session).

commit

- Syntax** **commit**
- Context** config>app-assure>group>policy
- Description** This command commits changes made during the current editing session. None of the policy changes done will take effect until commit command is issued. If the changes can be successfully committed, no errors detected during the commit during cross-reference verification against exiting application assurance configuration, the editing session will also be closed.
- The newly committed policy takes effect immediately for all new flows, existing flows will transition onto the new policy shortly after the commit.

app-group

- Syntax** **app-group** *application-group-name* [**create**]
no app-group *application-group-name*
- Context** config>app-assure>group>policy
- Description** This command creates an application group for an application assurance policy.
- The **no** form of the command deletes the application group from the configuration. All associations must be removed in order to delete a group.
- Default** no app-group
- Parameters** *application-group-name* — A string of up to 32 characters uniquely identifying this application group in the system.
- create** — Mandatory keyword used when creating an application group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

charging-group

Syntax	charging-group <i>charging-group-name</i> no charging-group
Context	config>app-assure>group>policy>app-group config>app-assure>group>policy>application
Description	This command associates an application or app-group to an application assurance charging group. The no form of the command deletes the charging group association.
Default	no charging-group
Parameters	<i>charging-group-name</i> — Specifies a string of up to 32 characters uniquely identifying an existing charging group in the system.

charging-group

Syntax	charging-group { eq neq } <i>charging-group-name</i> no charging-group
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command associates an application or app-group to an application assurance charging group. The no form of the command deletes the charging group association.
Default	no charging-group
Parameters	<i>charging-group-name</i> — Specifies a string of up to 32 characters uniquely identifying an existing charging group in the system.

charging-group

Syntax	charging-group <i>charging-group-name</i> [create] no charging-group <i>charging-group-name</i>
Context	config>app-assure>group>policy
Description	This command creates a charging group for an application assurance policy. The no form of the command deletes the charging group from the configuration. All associations must be removed to delete a group.
Default	no charging-group

- Parameters** *charging-group-name* — Specifies a string of up to 32 characters uniquely identifying an existing charging group in the system.
- create** — Mandatory keyword used when creating an charging group. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

export-id

- Syntax** **export-id** *export-id*
no export-id
- Context** config>app-assure>group>policy>application
config>app-assure>group>policy>application>charging-group
config>app-assure>group>policy>app-group
- Description** This command assigns an export-id value to a charging group app-group or application to be used for accounting export identification in RADIUS accounting. This ID is encoded in the top 2 bytes of the RADIUS accounting VSA to identify which charging group the counter value represents.
- If no export-id is assigned, that counter cannot be added to the aa-sub stats RADIUS export-type. Once a charging group index is referenced, it cannot be deleted without removing the reference.
- The no form of the command removes the export-id from the configuration.
- Default** no export-id
- Parameters** *export-id* — Specifies an integer that identifies an export-id.
- Values** 1 to 255

app-filter

- Syntax** **app-filter**
- Context** config>app-assure>group>policy
- Description** This command enables the context to configure an application filter for application assurance.

app-qos-policy

- Syntax** **app-qos-policy**
- Context** config>app-assure>group>policy
- Description** This command enables the context to configure an application QoS policy.

app-service-options

Syntax	app-service-options
Context	config>app-assure>group>policy
Description	This command enables the context to configure application service option characteristics.

default-charging-group

Syntax	default-charging-group <i>charging-group-name</i> no default-charging-group
Context	config>app-assure>group>policy
Description	This command associates a charging group to any applications or app-groups that are not explicitly assigned to a charging group, for an application assurance policy. The no form of the command deletes the default charging group from the configuration.
Default	no default-charging-group
Parameters	<i>charging-group-name</i> — A string of up to 32 characters uniquely identifying an existing charging group in the system

diff

Syntax	diff
Context	config>app-assure>group>policy
Description	This command compares the newly configured policy against the operational policy.

application

Syntax	application <i>application-name</i> [create] no application <i>application-name</i>
Context	config>app-assure>group>policy
Description	This command creates an application of an application assurance policy. The no form of the command deletes the application. To delete an application, all associations to the application must be removed.
Default	none

- Parameters** *application-name* — Specifies a string of up to 32 characters uniquely identifying this application in the system.
- create** — Mandatory keyword used when creating an application. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

policy-override

- Syntax** **policy-override**
- Context** config>app-assure>group
- Description** This command enables the context to configure policy override parameters.

policy

- Syntax** **policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-aasub-name} [create]**
no policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-aasub-name}
- Context** config>app-assure>group>policy-override
- Description** This command specifies a given SAP or SDP to be used for a static policy override.
The **no** form of the command removes the policy override.
- Parameters** *sap-id* — Specifies the physical port identifier portion of the SAP definition.
sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.
- Values** 1 to 32767
1 to 4294967295
- transit-aasub-name* — Specifies an existing transit subscriber name, up to 32 characters.
- create** — Keyword used to create the policy override.

characteristic

- Syntax** **characteristic characteristic-name value value-name**
no characteristic characteristic-name
- Context** config>app-assure>group>policy-override>policy
- Description** This command configure an override characteristic and value.
- Parameters** *characteristic-name* — Specifies the characteristic name, up to 32 characters.

value-name — Specifies the override characteristic value for the application profile characteristic used by the Application assurance subscriber.

port-list

Syntax	port-list <i>port-list-name</i> [create] no port-list <i>port-list-name</i>
Context	config>app-assure>group
Description	This command defines an AA group or partition named port-list, which contains a list of port numbers or port ranges. The port list is then referenced in AA policy app-filters, allowing increased flexibility in the use of server ports or HTTP proxy ports for application definition. The no form of the command removes the list.
Parameters	<i>port-list-name</i> — Specifies the name of the port list. Default default

port

Syntax	[no] port <i>port-number</i> [no] port range <i>start-port-num end-port-num</i>
Context	config>app-assure>group>port-list
Description	This command specifies the server TCP or UDP port number to use in the port list definition. The no form of the command restores the default by removing port number from the port list.
Default	no port
Parameters	<i>port-number</i> — Specifies the port number. Values 0 to 65535 <i>start-port-number</i> — Specifies the start port number. Values 0 to 65535 <i>end-port-number</i> — Specifies the end port number. Values 0 to 65535

app-group

Syntax	app-group <i>app-group-name</i>

Context	config>app-assure>group>policy>application
Description	This command associates an application with an application group of an application assurance policy.
Parameters	<i>app-group-name</i> — A string of up to 32 characters uniquely identifying an existing application in the system.

Application Filter Commands

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>app-assure>group>policy>app-filter
Description	This command creates an application filter entry. App filter entries are an ordered list, the lowest numerical entry that matches the flow defines the application for that flow. An application filter entry or entries configures match attributes of an application. The no form of this command deletes the specified application filter entry.
Default	none
Parameters	<i>entry-id</i> — Specifies an integer that identifies an app-filter entry. Values 1 to 65535 create — Keyword used to create the entry.

application

Syntax	application <i>application-name</i>
Context	config>app-assure>group>policy>application config>app-assure>group>policy>app-filter>entry
Description	This command assigns this application filter entry to an existing application. Assigning the entry to Unknown application restores the default configuration.
Default	unknown application
Parameters	<i>application-name</i> — Specifies an existing application name.

expression

Syntax	expression <i>expr-index expr-type {eq neq} expr-string</i> no expression <i>expr-index</i>
Context	config>app-assure>group>policy>app-filter>entry
Description	This command configures string values to use in the application definition.
Parameters	<i>expr-index</i> — Specifies an index value which represents expression substrings. Values 1 to 4 <i>expr-type</i> — Represents a type (and thereby the expression substring). http-host — Matches the string against the HTTP Host field or TLS Server Name Indicator (SNI). http-uri — Matches the string against the HTTP URI field. http-referer — Matches the string against the HTTP Referer field. http-user-agent — Matches the string against the HTTP User Agent field. sip-ua — Matches the string against the SIP UA field. sip-uri — Matches the string against the SIP URI field. sip-mt — Matches the string against the SIP MT field. citrix-app — Matches the string against the Citrix app field. h323-product-id — Matches the string against the h323-product-id field. tls-cert-subj-org-name — Matches the TLS Certificate Subject Organization Name substring. tls-cert-subj-common-name — Matches the TLS Certificate Subject Common Name substring. rtsp-host — Matches the Real Time Streaming Protocol (RTSP) substring host. rtsp-uri — Matches the RTSP URI substring. rtsp-ua — Matches the RTSP UA substring. rtmp-page-host — Matches against the RTMP Page Host Field rtmp-page-uri — Matches against the RTMP Page URI Field rtmp-swf-host — Matches against the RTMP Swf Host Field rtmp-swf-uri — Matches against the RTMP Swf URI Field eq — Specifies the equal to comparison operator to match the specified HTTP string. neq — Specifies the not equal to comparison operator to match the specified HTTP string. <i>expr-string</i> — Specifies an expression string, up to 64 characters, used to define a pattern match. Denotes a printable ASCII substring used as input to an application assurance filter match criteria object. The following syntax is permitted within the substring to define the pattern match criteria: ^<substring>* - matches when <substring> is at the beginning of the object.

<substring> - matches when <substring> is at any place within the object.
 *<substring>\$ - matches when <substring> is at the end of the object.
 ^<substring>\$ - matches when <substring> is the entire object.
 * - matches zero to many of any character. A single wildcard as infix in the expression is allowed.
 \. - matches any single character
 \d - matches any single decimal digit [0-9]
 \l - forces case sensitivity (by default, the expression match are case insensitive), the \l can be specified anywhere between the leading [^*] and trailing [\$*]
 * - matches the asterisk character
 Rules for <substring> characters:
 <substring> must contain printable ASCII characters.
 <substring> must not contain the “double quote” character or the “ ” (space) character on its own.
 <substring> match is case insensitive by default.
 <substring> must not include any regular expression meta-characters other than "*", "\l", "\.", "*" and "\d".
 The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the <substring>:
 Character to match <substring> input
 Hexadecimal Octet YY \xYY
 A <substring> that uses the '\’ (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

Operational notes:

- When matching a TCP flow against HTTP-string based applications, the HTTP header fields are collected from the first HTTP request (for example a GET or a POST) for a given TCP flow. The collected strings are then evaluated against each HTTP flow created within the given TCP flow to determine whether a given HTTP flow matches the application. By not specifying a protocol, the HTTP expressions are matched against all protocols in the HTTP family. By specifying a specific HTTP protocol (for example, http_video) the expression match can be constrained to a subset of the HTTP protocols.
- To uniquely identify a SIP-based application a protocol match is not required in the app-filter entry with the SIP expression. The SIP expression match is performed against any protocol in the SIP family (such as sip and rtp_sip). By specifying a specific SIP protocol (like rtp_sip) the expression match can be constrained to a subset of the SIP protocols.

flow-setup-direction

Syntax **flow-setup-direction {subscriber-to-network | network-to-subscriber | both}**

Context	config>app-assure>group>policy>app-filter>entry
Description	This command configures the direction of flow setup to which the application filter entry is to be applied.
Default	flow-setup-direction both
Parameters	subscriber-to-network — Specifies that the app-filter entry will be applied to flows initiated by a local subscriber. network-to-subscriber — Specifies that the app-filter entry will be applied to flows initiated from a remote destination towards a local subscriber. both — Specifies that the app filter entry will be applied for subscriber-to-network and network-to-subscriber traffic.

http-port

Syntax	http-port {eq neq} <i>port-num</i> http-port {eq neq} port-list <i>port-list-name</i> no http-port
Context	config>app-assure>group>policy>app-filter>entry
Description	This command specifies an HTTP server TCP or UDP port number or port list to use in the application definition. The no form of the command restores the default by removing the HTTP port or port list from the application criteria defined by this app-filter entry.
Default	no http-port
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. <i>port-list-name</i> — Specifies the name of the port list containing a set or range of ports, up to 32 characters. <i>port-num</i> — Specifies a valid server port number. Values 0 to 65535

ip-protocol-num

Syntax	ip-protocol-num {eq neq} <i>protocol-id</i> no ip-protocol-num
Context	config>app-assure>group>policy>app-filter>entry config>app-assure>group>policy>aqp>entry>match

Description	This command configures the IP protocol to use in the application definition. The no form of the command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).
Default	no ip-protocol-num
Parameters	eq — Specifies that the value configured and the value in the flow must be equal. neq — Specifies that the value configured differs from the value in the flow. <i>protocol-id</i> — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17). The no form the command removes the protocol from the match criteria. Values 1 to 255 (Decimal, Hexadecimal, or Binary representation). Supported IANA IP protocol names: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp, tcp, udp, vrrp * - udp/tcp wildcard

network-address

Syntax	network-address {eq neq} <i>ip-address</i> network-address {eq neq} ip-prefix-list <i>ip-prefix-list-name</i> no network-address
Context	config>app-assure>group>policy>app-filter>entry
Description	This command configures the network address to use in application definition. The network address will match the destination IP address in a from-sub flow or the source IP address in a to-sub flow. The no form of the command restores the default (removes the network address from application criteria defined by this entry).
Default	no network-address
Parameters	eq — Specifies a comparison operator indicating that the value configured and the value in the flow are equal. neq — Specifies a comparison operator indicating that the value configured differs from the value in the flow. <i>ip-address</i> — Specifies a valid unicast address. Values ipv4-address a.b.c.d[/mask]

mask - [1..32]
ipv6-address x:x:x:x:x:x/x/prefix-length
x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D
prefix-length [1..128]

ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.

protocol

Syntax	protocol { eq neq } <i>protocol-name</i> no protocol
Context	config>app-assure>group>policy>app-filter>entry
Description	This command configures protocol signature in the application definition. The no form of the command restores the default (removes protocol from match application defined by this app-filter entry).
Default	no protocol
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. <i>protocol-name</i> — A string of up to 32 characters identifying a predefined protocol.

server-address

Syntax	server-address { eq neq } <i>ip-address</i> server-address { eq neq } dns-ip-cache <i>dns-ip-cache-name</i> server-address { eq neq } ip-prefix-list <i>ip-prefix-list-name</i> no server-address
Context	config>app-assure>group>policy>app-filter>entry
Description	This command configures the server address to use in application definition. The server IP address may be the source or destination, network or subscriber IP address. The no form of the command restores the default (removes the server address from application criteria defined by this entry).
Default	no server-address

Parameters	eq — Specifies a comparison operator that the value configured and the value in the flow are equal.				
	neq — Specifies a comparison operator that the value configured differs from the value in the flow.				
	ip-address — Specifies a valid unicast address.				
Values					
	<table> <tr> <td>ipv4-address</td><td>a.b.c.d[/mask] mask - [1..32]</td></tr> <tr> <td>ipv6-address</td><td>x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]</td></tr> </table>	ipv4-address	a.b.c.d[/mask] mask - [1..32]	ipv6-address	x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]
ipv4-address	a.b.c.d[/mask] mask - [1..32]				
ipv6-address	x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]				
	dns-ip-cache-name — Specifies a DNS IP cache name, up to 32 characters.				
	ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.				

server-port

Syntax	server-port {eq neq gt lt} port-num server-port {eq neq} range start-port-num end-port-num server-port {eq} {port-num range start-port-num end-port-num} {first-packet-trusted first-packet-validate} server-port {eq neq} port-list port-list-name server-port {eq} port-list port-list-name {first-packet-trusted first-packet-validate} no server-port
Context	config>app-assure>group>policy>app-filter>entry
Description	This command specifies the server TCP or UDP port number to use in the application definition. The no form of the command restores the default (removes server port number from application criteria defined by this app-filter entry).
Default	no server-port (the server port is not used in the application definition)
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. gt — Specifies all port numbers greater than server-port-number match. lt — Specifies all port numbers less than server-port-number match. port-list-name — Specifies a named port list containing a set or range of ports.

- port-num* — Specifies a valid server port number.
- Values** 0 to 65535
- start-port-num, end-port-num* — Specifies the starting or ending port number.
- Values** 0 to 65535
- Server Port Options:* — •**No option specified:** TCP/UDP port applications with full signature verification:
- AA ensures that other applications that can be identified do not run over a well-known port.
 - Application-aware policy applied once signature-based identification completes (likely requiring several packets).
- **first-packet-validate:** TCP/UDP trusted port applications with signature verification:
- Application identified using well known TCP/UDP port based filters and re-identified once signature identification completes.
 - AA policy applied from the first packet of a flow while continuing signature-based application identification. Policy re-evaluated once the signature identification completes, allowing to detect improper/unexpected applications on a well-known port.
- **first-packet-trusted:** TCP/UDP trusted port applications - no signature verification:
- Application identified using well known TCP/UDP port based filters only.
 - Application Aware policy applied from the first packet of a flow.
 - No signature processing assumes operator/customer trusts that no other applications can run on the well-known TCP/UDP port (statistics collected against trusted_tcp or trusted_udp protocol).

Application Profile Commands

app-profile	
Syntax	app-profile app-profile-name [create] no app-profile app-profile-name
Context	config>app-assure>group>policy
Description	This command creates an application profile and enables the context to configure the profile parameters. The no form of the command removes the application profile from the configuration.
Default	none

- Parameters** *app-profile-name* — Specifies the name of the application profile up to 32 characters.
- create** — Mandatory keyword used when creating an application profile. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

aa-sub-suppressible

- Syntax** **aa-sub-suppressible**
 no aa-sub-suppressible
- Context** config>app-assure>group>policy>app-profile
- Description** This command configures an app-profile as “aa-sub-suppressible”, this function is used in the context of an SRRP group interface. If an SRRP group interface is configured as “suppress-aa-sub” then subscribers with an app-profile configured as “aa-sub-suppressible” will not be diverted to Application Assurance.
- The **no** form of the command restores the default behavior.
- Default** no aa-sub-suppressible

capacity-cost

- Syntax** **capacity-cost** *cost*
 no capacity-cost
- Context** config>app-assure>group>policy>app-profile
- Description** This command configures an application profile capacity cost. Capacity-Cost based load balancing allows a cost to be assigned to diverted SAPs (with the app-profile) and this is then used for load-balancing SAPs between ISAs as well as for a threshold that notifies the operator if/when capacity planning has been exceeded.
- Default** capacity-cost 1
- Parameters** *cost* — Specifies the profile capacity cost.
- Values** 1 to 65535

characteristic

- Syntax** **characteristic** *characteristic-name* **value** *value-name*
 no characteristic *characteristic-name*
- Context** config>app-assure>group>policy>app-profile

Description	This command assigns one of the existing values of an existing application service option characteristic to the application profile. The no form of the command removes the characteristic from the application profile.
Parameters	<i>characteristic-name</i> — Specifies the name of an existing ASO characteristic. <i>value-name</i> — Specifies the name for the application profile characteristic up to 32 characters.

divert

Syntax	[no] divert
Context	config>app-assure>group>policy>app-profile
Description	This command enables the redirection of traffic to AA ISA for the system-wide forwarding classes diverted to application assurance (divert-fc) for AA subscribers using this application profile. The no form of the command stops redirect of traffic to AA ISAs for the AA subscribers using this application profile.
Default	no divert

Application QoS Policy Commands

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>app-assure>group>policy>aqp
Description	This command creates an application QoS policy entry. A flow that matches multiple Application QoS policies (AQP) entries will have multiple AQP entries actions applied. When a conflict occurs for two or more actions, the action from the AQP entry with the lowest numerical value takes precedence. The no form of this command deletes the specified application QoS policy entry.
Default	none
Parameters	<i>entry-id</i> — An integer identifying the AQP entry. Values 1 to 65535

create — Mandatory keyword creates the entry. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

action

Syntax	action
Context	config>app-assure>group>policy>aqp>entry
Description	This command enables the context to configure AQP actions to be performed on flows that match the AQP entry's match criteria.

bandwidth-policer

Syntax	bandwidth-policer <i>policer-name</i> no bandwidth-policer
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command assigns an existing bandwidth policer as an action on flows matching this AQP entry. The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria. When multiple policers apply to a single flow, the final action on a packet is the worst case of all policer outcomes (for example, if one of the policers marks packet out of profile, the final marking will reflect that). The no form of the command removes bandwidth policer from actions on flows matching this AQP entry.
Default	no bandwidth-policer
Parameters	<i>policer-name</i> — The name of the existing flow setup rate policer for this application assurance profile. The <i>policer-name</i> is configured in the config>app-assure>group>policer context.

drop

Syntax	[no] drop
Context	config>app-assure>group>policy>aqp>entry>action

Description	This command configures the drop action on flows matching this AQP entry. When enabled, all flow traffic matching this AQP entry will be dropped. When drop action is part of a set of multiple actions to be applied to a single flow as result of one or more AQP entry match, drop action will be performed first and no other action will be invoked on that flow. The no form of the command disables the drop action on flows matching this AQP entry.
Default	no drop

error-drop

Syntax	error-drop [event-log <i>event-log-name</i>] no error-drop
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command configures a drop action for error flows (bad IP checksums, tcp/udp port 0, and so on).
Default	no error-drop
Parameters	<i>event-log-name</i> — Specifies the event log name, up to 32 characters.

flow-count-limit

Syntax	flow-count-limit <i>policer-name</i> [event-log <i>event-log-name</i>] no flow-count-limit
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command assigns an existing flow count limit policer as an action on flows matching this AQP entry. The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria. When multiple policers apply to a single flow, the final action on a packet is the worst case of all policer outcomes (for example, if one of the policers marks packet out of profile, the final marking will reflect that). The no form of the command removes this flow policer from actions on flows matching this AQP entry.
Default	no flow-count-limit

- Parameters**
- policer-name* — Specifies the name of the existing flow setup rate policer for this application assurance profile. The *policer-name* is configured in the **config>app-assure>group>policer** context.
 - event-log-name* — Specifies the name of the event log used when event logging is enabled, up to 32 characters, which is used when event logging is enabled.

flow-rate-limit

- Syntax** **flow-rate-limit** *policer-name* [**event-log** *event-log-name*]
no flow-rate-limit
- Context** config>app-assure>group>policy>aqp>entry>action
- Description** This command assigns an existing flow setup rate limit policer as an action on flows matching this AQP entry.
- The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.
- When multiple policers apply to a single flow, the final action on a packet is the worst case of all policer outcomes (for example, if one of the policers marks packet out of profile, the final marking will reflect that).
- The **no** form of the command removes this flow policer from actions on flows matching this AQP entry.
- Default** no flow-rate-limit
- Parameters**
- policer-name* — Specifies the policer name up to 32 characters.
 - event-log** *event-log-name* — Specifies the event-log-name up to 32 characters, which will be used when event logging is enabled.

fragment-drop

- Syntax** **fragment-drop** {**all** | **out-of-order**} [**event-log** *event-log-name*]
no fragment-drop
- Context** config>app-assure>group>policy>aqp>entry>action
- Description** This command specifies the action to apply to fragments.
- Default** no fragment-drop
- Parameters**
- all** — All the fragments will be dropped.
 - out-of-order** — All out of order fragments will be dropped.

event-log-name — Specifies if the dropping of fragments should be logged to the specified event log name.

gtp-filter

Syntax	gtp-filter <i>gtp-filter-name</i> no gtp-filter
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command assigns an existing GTP filter as an action on flows matching this AQP entry. The no form of the command removes this GTP filter from actions on flows matching this AQP entry.
Default	no gtp-filter
Parameters	<i>gtp-filter-name</i> — Specifies the name of an existing GTP filter for this application assurance profile. The <i>gtp-filter-name</i> is configured in the config>app-assure>group[:partition]>gtp>gtp-filter context.

http-enrich

Syntax	http-enrich <i>http-enrich-name</i> no http-enrich
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command configures a the HTTP header enrichment template name that will be applied as defined in the tmnxBsxHttpEnrichTable. An empty value specifies no HTTP header enrichment template.
Default	no http-enrich
Parameters	<i>http-enrich-name</i> — Specifies the HTTP header enrichment template name up to 32 characters.

http-error-redirect

Syntax	http-error-redirect <i>redirect-name</i> no http-error-redirect
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command specifies the HTTP error redirect that will be applied as defined in the redirect table. An empty value specifies no HTTP error redirect.

Default	no http-error-redirect
Parameters	<i>redirect-name</i> — Specifies an http-error redirect action, up to 32 characters, for flows matching this entry.

http-notification

Syntax	http-notification <i>http-notification</i> no http-notification
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command configures an HTTP notification action for flows matching this entry.
Default	no http-notification
Parameters	<i>http-notification</i> — specifies the Application-Assurance HTTP Notification that will be applied as defined in the tmnxBsxHttpNotifTable. If no string is configured then no HTTP notification will occur.

http-redirect

Syntax	http-redirect <i>http-redirect-name</i> flow-type <i>flow-type</i> no http-redirect
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command assigns an existing http redirect policy as an action on flows matching this AQP entry. The redirect only takes effect if the matching flows are HTTP and the condition specified after the http-redirect command, admitted flows or dropped-flows, is met. The condition specified by “dropped-flows” means the flow is dropped due to an AQP actions such as “flow rate/count policers” or “drop” actions. HTTP Policy Redirect on admitted-flows allows the operator to redirect HTTP traffic to a web portal while allowing non-HTTP matching the same AQP rule to be forwarded. No HTTP redirect will take place if HTTP redirect action and a “drop/flow-police” action are part of the default AQP policy, because in this case, any flow drop actions will take place before identification of the application/application-group. The no form of the command removes http redirect from actions on flows matching this AQP entry.
Default	no http-redirect

Parameters	<i>http-redirect-name</i> — Specifies the name of the existing http policy redirect for this application assurance profile. The HTTP redirect name is configured in the config>app-assure>group>http-redirect context. <i>flow-type</i> — Specifies the flow type. Values admitted-flows — Redirect HTTP flows matching the AQP criteria. dropped-flows — Redirects those HTTP flows that are dropped due to an AQP action.

mirror-source

Syntax	mirror-source [all-inclusive] <i>mirror-service-id</i> no mirror-source
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command configures an application-based policy mirroring service that uses this AA ISA group's AQP entry as a mirror source. When configured, AQP entry becomes a mirror source for IP packets seen by the AA (the mirrored packet is an IP packet analyzed by AA and does not include encapsulations present on the incoming interfaces).
Default	no mirror-source
Parameters	all-inclusive — Specifies that all packets during identification phase that could match a given AQP rule are mirrored in addition to packets after an application identification completes that match the AQP rule. This ensures all packets of a given flow are mirrored at a cost of sending unidentified packets that once the application is identified will no longer match this AQP entry. <i>mirror-service-id</i> — Specifies the mirror source service ID to use for flows that match this policy. Values 1 to 2147483647 svc-name: 64 characters maximum

overload-drop

Syntax	overload-drop [event-log <i>event-log-name</i>] no overload-drop
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command configures a drop action for cases where flow records are not created (overload).
Parameters	<i>event-log-name</i> — Specifies the event log name, up to 32 characters

remark

Syntax	remark
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command configures remark action on flows matching this AQP entry.

dscp

Syntax	dscp in-profile <i>dscp-name</i> out-profile <i>dscp-name</i> no dscp
Context	config>app-assure>group>policy>aqp>entry>action>remark
Description	This command enables the context to configure DSCP remark action or actions on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured DSCP name. DSCP remark can only be applied when the entry remarks forwarding class or forwarding class and priority. In-profile and out-of profile of a given packet for DSCP remark is assessed after all AQP policing and priority remarking actions took place. The no form of the command stops DSCP remarking action on flows matching this AQP entry.
Default	no dscp
Parameters	in-profile <i>dscp-name</i> — Specifies the DSCP name to use to remark in-profile flows that match this policy. out-profile <i>dscp-name</i> — Specifies the DSCP name to use to remark out-of-profile flows that match this policy.
Values	be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc

Syntax	fc <i>fc-name</i> no fc
Context	config>app-assure>group>policy>aqp>entry>action>remark

Description	This command configures remark FC action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured forwarding class. The no form of the command stops FC remarking action on packets belonging to flows matching this AQP entry
Default	no fc
Parameters	<i>fc-name</i> — Configure the FC remark action for flows matching this entry. Values be, l2, af, l1, h2, ef, h1, nc

priority

Syntax	priority <i>priority-level</i> no priority
Context	config>app-assure>group>policy>aqp>entry>action>remark
Description	This command configures remark discard priority action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured discard priority.
Default	no priority
Parameters	<i>priority-level</i> — Specifies the priority to apply to a packet. Values high, low

sctp-filter

Syntax	sctp-filter <i>sctp-filter-name</i> no sctp-filter
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command assigns an existing SCTP filter as an action on flows matching this AQP entry. The no form of the command removes this SCTP filter from actions on flows matching this AQP entry.
Default	no sctp-filter
Parameters	<i>sctp-filter-name</i> — The name of the existing SCTP filter for this application assurance profile. The <i>sctp-filter-name</i> is configured in the config>app-assure>group[:partition]>sctp-filter context.

tcp-mss-adjust

Syntax	tcp-mss-adjust <i>segment-size</i> no tcp-mss-adjust
Context	config>app-assure>group>aqp>entry>action
Description	This command configures the value to adjust the TCP Maximum Segment Size (MSS) option. The no form of the command disables the segment size adjustment.
Default	no tcp-mss-adjust
Parameters	<i>segment-size</i> — Specifies the value to put into the TCP Maximum Segment Size (MSS) option if not already present, or if the present value is higher. Values 160 to 10240

tcp-validate

Syntax	tcp-validate <i>tcp-validate-name</i> no tcp-validate
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command assigns an existing TCP validation policy as an action on flows matching this AQP entry. tcp-validate can only be called from AQP entries that: • have no matching conditions that relate to information extracted from the incoming IP packets; for example, no application or IP address. • allow the following match conditions: – none – aa-sub – characteristic – traffic-direction (both only) traffic-direction cannot be unidirectional (from or to sub). It can either be set to both or left unspecified. The no form of the command removes the TCP validation policy action from flows matching this AQP entry.
Default	no tcp-validate
Parameters	<i>tcp-validate-name</i> — Specifies the name of the TCP validation policy for this application assurance profile. The TCP validation policy is configured using the config>app-assure>group>tcp-validate <i>tcp-validate-name</i> command.

tls-enrich

Syntax	[no] tls-enrich
Context	config>app-assure>group>aqp>entry>action
Description	This command configures a TLS richment action for flows matching this entry.

url-filter

Syntax	url-filter <i>url-filter-name</i> [characteristic <i>characteristic-name</i>] no url-filter
Context	config>app-assure>group>aqp>entry>action
Description	This command configures a url-filter action for flows matching this entry.
Parameters	<i>url-filter-name</i> — Specifies the name of the url-filter policy. <i>characteristic-name</i> — Specifies the name of the characteristic.

characteristic

Syntax	characteristic <i>characteristic-name</i>
Context	config>app-assure>group>aqp>entry>action
Description	This command enables the system to use the value of the characteristic name specified in the app-qos-policy url-filter action for the configurable ICAP x-header name provisioned in the url-filter policy. The ICAP server can then use this value to decide which url-filter policy to apply instead of applying a filter policy based on the subscriber name.
Parameters	<i>characteristic-name</i> — Specifies the name of the characteristic.

session-filter

Syntax	session-filter <i>session-filter-name</i> no session-filter
Context	config>app-assure>group>policy>aqp>entry>action
Description	This command specifies the Application-Assurance session filter that will be evaluated. If no session filters are specified then no session filters will be evaluated.
Default	no session-filter
Parameters	<i>session-filter-name</i> — Specifies the session filter to be applied.

match

Syntax	match
Context	config>app-assure>group>policy>aqp>entry
Description	This command enables the context to configure flow match rules for this AQP entry. A flow matches this AQP entry only if it matches all the match rules defined (logical and of all rules). If no match rule is specified, the entry will match all flows.

aa-sub

Syntax	aa-sub esm {eq neq} sub-ident-string aa-sub esm-mac {eq neq} esm-mac-name aa-sub sap {eq neq} sap-id aa-sub spoke-sdp {eq neq} sdp-id:vc-id aa-sub transit {eq neq} transit-aasub-name no aa-sub
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command specifies a Service Access Point (SAP) or an ESM subscriber as matching criteria. The no form of the command removes the SAP or ESM matching criteria.
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. <i>sub-ident-string</i> — Specifies the name of an existing application assurance subscriber. <i>esm-mac-name</i> — Specifies the name of an ESM-MAC subscriber. <i>sap-id</i> — Specifies the SAP ID. sap sap-id — Specifies the physical port identifier portion of the SAP definition. <i>sdp-id:vc-id</i> — Specifies the spoke SDP ID and VC ID. Values 1 to 32767 1 to 4294967295 <i>transit-aa-sub-name</i> — Specifies the name of a transit AA subscriber.

app-group

Syntax	app-group {eq neq} application-group-name no app-group

Context	config>app-assure>group>policy>aqp>entry>match
Description	This command adds app-group to match criteria used by this AQP entry. The no form of the command removes the app-group from match criteria for this AQP entry.
Default	no app-group
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. <i>application-group-name</i> — The name of the existing application group entry. The application-group-name is configured in the config>app-assure>group>policy>aqp>entry>match context.

application

Syntax	application {eq neq} application-name no application
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command adds an application to match criteria used by this AQP entry. The no form of the command removes the application from match criteria for this AQP entry.
Default	no application
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. <i>application-name</i> — The name of name existing application name. The application-group-name is configured in the config>app-assure>group>policy>aqp>entry>match context.

characteristic

Syntax	characteristic characteristic-name eq value-name no characteristic
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command adds an existing characteristic and its value to the match criteria used by this AQP entry. The no form of the command removes the characteristic from match criteria for this AQP entry.
Parameters	eq — Specifies that the value configured and the value in the flow are equal.

characteristic-name — The name of the existing ASO characteristic up to 32 characters in length.

value-name — The name of an existing value for the characteristic up to 32 characters in length.

charging-group

Syntax	charging-group { eq neq } <i>charging-group-name</i> no charging-group
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command adds charging-group to match criteria used by this AQP entry. The no form of the command removes the charging-group from match criteria for this AQP entry.
Default	no charging-group
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow. <i>charging-group-name</i> — The name of the existing application group entry. The application-group name is configured in the config>app-assure>group>policy>aqp>entry>match context.

dscp

Syntax	dscp { eq neq } <i>dscp-name</i> no dscp
Context	config>app-assure>group>policy>aqp>entry>match config>app-assure>group>sess-ftr>entry>match
Description	This command adds a DSCP name to the match criteria used by this entry. The no form of the command removes dscp from match criteria for this entry.
Default	no dscp
Parameters	eq — Specifies that the value configured and the value in the flow are equal. neq — Specifies that the value configured differs from the value in the flow.

dscp-name — Specifies the DSCP name to be used in the match.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dst-ip

Syntax	dst-ip {eq neq} ip-address dst-ip {eq neq} ip-prefix-list ip-prefix-list-name no dst-ip				
Context	config>app-assure>group>policy>aqp>entry>match				
Description	This command specifies a destination IP address to use as match criteria.				
Default	no dst-ip				
Parameters	eq — Specifies that a successful match occurs when the flow matches the specified address or prefix. neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix. <i>ip-address</i> — Specifies a valid unicast address. Values <table> <tr> <td>ipv4-address</td><td>a.b.c.d[/mask] mask - [1..32]</td></tr> <tr> <td>ipv6-address</td><td>x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]</td></tr> </table>	ipv4-address	a.b.c.d[/mask] mask - [1..32]	ipv6-address	x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]
ipv4-address	a.b.c.d[/mask] mask - [1..32]				
ipv6-address	x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]				

ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.

dst-port

Syntax	dst-port {eq neq} port-num dst-port {eq neq} port-list port-list-name dst-port {eq neq} range start-port-num end-port-num no dst-port

Context	config>app-assure>group>policy>aqp>entry>match
Description	This command specifies a destination TCP/UDP port, destination port list, or destination range to use as match criteria. The no form of the command removes the parameters from the configuration.
Default	no dst-port
Parameters	eq — Specifies that a successful match occurs when the flow matches the specified port. neq — Specifies that a successful match occurs when the flow does not match the specified port. <i>port-num</i> — Specifies the destination port number. Values 0 to 65535 <i>start-port-num end-port-num</i> — Specifies the start or end destination port number. Values 0 to 65535 <i>port-list-name</i> — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

ip-protocol-num

Syntax	ip-protocol-num {eq neq} protocol-id no ip-protocol-num
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command configures the IP protocol to use to use as match criteria. The no form the command removes the protocol from the match criteria.
Default	no ip-protocol-num
Parameters	eq — Specifies that the value configured and the value in the flow must be equal. neq — Specifies that the value configured differs from the value in the flow. <i>protocol-id</i> — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17). Values 1 to 255 (Decimal, Hexadecimal, or Binary representation). Supported IANA IP protocol names: crtp, crudp, egg, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp

src-ip

Syntax	src-ip {eq neq} <i>ip-address</i> src-ip {eq neq} ip-prefix-list <i>ip-prefix-list-name</i> no src-ip														
Context	config>app-assure>group>policy>aqp>entry>match														
Description	This command specifies a source TCP/UDP address to use as match criteria.														
Default	no src-ip														
Parameters	eq — Specifies that a successful match occurs when the flow matches the specified address or prefix. neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix. <i>ip-address</i> — Specifies a valid unicast address.														
	Values <table> <tr> <td>ipv4-address</td><td>a.b.c.d[/mask]</td></tr> <tr> <td></td><td>mask - [1..32]</td></tr> <tr> <td>ipv6-address</td><td>x:x:x:x:x:x/x/prefix-length</td></tr> <tr> <td></td><td>x:x:x:x:x:x.d.d.d.d</td></tr> <tr> <td></td><td>x - [0..FFFF]H</td></tr> <tr> <td></td><td>d - [0..255]D</td></tr> <tr> <td></td><td>prefix-length [1..128]</td></tr> </table>	ipv4-address	a.b.c.d[/mask]		mask - [1..32]	ipv6-address	x:x:x:x:x:x/x/prefix-length		x:x:x:x:x:x.d.d.d.d		x - [0..FFFF]H		d - [0..255]D		prefix-length [1..128]
ipv4-address	a.b.c.d[/mask]														
	mask - [1..32]														
ipv6-address	x:x:x:x:x:x/x/prefix-length														
	x:x:x:x:x:x.d.d.d.d														
	x - [0..FFFF]H														
	d - [0..255]D														
	prefix-length [1..128]														
	<i>ip-prefix-list-name</i> — Specifies an IP prefix list name, up to 32 characters.														

src-port

Syntax	src-port {eq neq} <i>port-num</i> src-port {eq neq} port-list <i>port-list-name</i> src-port {eq neq} range <i>start-port-num end-port-num</i> no src-port
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command specifies a source IP port, source port list, or source range to use as match criteria. The no form of the command removes the parameters from the configuration.
Default	no src-port
Parameters	eq — Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the source port number.

Values 0 to 65535

start-port-num end-port-num — Specifies the start or end source port number.

Values 0 to 65535

port-list-name — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

traffic-direction

Syntax	traffic-direction { subscriber-to-network network-to-subscriber both }
Context	config>app-assure>group>policy>aqp>entry>match
Description	This command specifies the direction of traffic where the AQP match entry will be applied. To use a policer action with the AQP entry the match criteria must specify a traffic-direction of either subscriber-to-network or network-to-subscriber.
Default	traffic-direction both
Parameters	subscriber-to-network — Traffic from a local subscriber will match this AQP entry. network-to-subscriber — Traffic to a local subscriber will match this AQP entry. both — Combines subscriber-to-network and network-to-subscriber.

Application Service Options Commands

characteristic

Syntax	characteristic <i>characteristic-name</i> [create] no characteristic <i>characteristic-name</i>
Context	config>app-assure>group>policy>aso
Description	This command creates the characteristic of the application service options. The no form of the command deletes characteristic option. To delete a characteristic, it must not be referenced by other components of application assurance.
Default	none

Parameters *characteristic-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic.

create — Mandatory keyword used to create when creating a characteristic. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

default-value

Syntax **default-value** *value-name*
 no default-value

Context config>app-assure>group>policy>aso>char

Description This command assigns one of the characteristic values as default.

 When a default value is specified, app-profile entries that do not explicitly include this characteristic inherit the default value and use it as part of the AQP match criteria based on that app-profile.

 A default-value is required for each characteristic. This is evaluated at commit time.

 The **no** form of the command removes the default value for the characteristic.

Parameters *value-name* — Specifies the name of an existing characteristic value.

value

Syntax [**no**] **value** *value-name*

Context config>app-assure>group>policy>aso>char

Description This command configures a characteristic value.

 The **no** form of the command removes the value for the characteristic.

Parameters *value-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic value.

Custom Protocol Commands

custom-protocol

Syntax **custom-protocol** *custom-protocol-id* **ip-protocol-num** *protocol-id* [**create**]
 custom-protocol *custom-protocol-id*

	no custom-protocol <i>custom-protocol-id</i>
Context	config>app-assure>group>policy
Description	This command creates and enters configuration context for custom protocols. Custom protocols allow the creation of TCP and UDP-based custom protocols (based on the <i>ip-protocol-num</i> option) that employ pattern-match at offset in protocol signature definition. Operator-configurable custom-protocols are evaluated ahead of any Nokia-provided protocol signature in order of custom-protocol-id (the lower ID is matched first in case of flow matching multiple custom-protocols) within the context the protocol is defined. Custom protocols must be created before they can be used in application definition but do not have to be enabled. To reference a custom protocol in application definition, or any other CLI configuration one must use protocol name that is a concatenation of “custom_” and <custom-protocol-id>, (for example custom_01, custom_02 ... custom_10, and so on). This concatenation is also used when reporting custom protocol statistics.
Parameters	<i>custom-protocol-id</i> — Specifies the index into the protocol list that defines a custom protocol for application assurance. Values 1 to 10 <i>protocol-id</i> — Specifies the IP protocol to match against for the custom protocol. Values 6, 17, Protocol numbers accepted in DHB, keywords: tcp, udp create — Mandatory keyword used when creating custom protocol. The create keyword requirement can be enabled/disabled in the environment>create context.

expression

Syntax	expression <i>expr-index</i> eq <i>expr-string</i> offset <i>payload-octet-offset</i> direction <i>direction</i> no expression <i>expr-index</i>
Context	config>app-assure>group>policy>custom-protocol
Description	This command configures an expression string value for pattern-based custom protocols match. A flow matches a custom protocol if the specified string is found at an offset of a TCP/UDP of the first payload packet. Options: • client-to-server — A pattern will be matched against a flow from a TCP client. • server-to-client — A pattern will be matched against a flow from a TCP server. • any — A pattern will be matched against a TCP/UDP flow in any direction (towards or from AA subscriber) The no form of this command deletes a specified string expression from the definition.

Parameters	<i>expr-index</i> — Specifies the expression substring index. Values 1 <i>expr-string</i> — Denotes a printable ASCII string, up to 16 characters, used to define a custom protocol match. Rules for <i>expr-string</i> characters: • Must contain printable ASCII characters. • Must not contain the “double quote” character or the “ ” (space) character on its own. • Match is case sensitive. • Must not include any regular expression meta-characters. The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the <i>expr-string</i> : <table><tr><td>Character to match</td><td><i>expr-string</i> input</td></tr><tr><td>Hexadecimal Octet YY</td><td>\xYY</td></tr></table> An <i>expr-string</i> that uses the “\” (backslash) ESCAPE character which is not followed by a “\” or “x” and a 2-digit hex octet is not valid. offset payload-octet-offset — specifies the offset (in octets) into the protocol payload, where the <i>expr-string</i> match criteria will start. Values 0 to 127 direction direction — Specifies the protocol direction to match against to resolve to a custom protocol. Values client-to-server, server-to-client, any	Character to match	<i>expr-string</i> input	Hexadecimal Octet YY	\xYY
Character to match	<i>expr-string</i> input				
Hexadecimal Octet YY	\xYY				

Session Filter Commands

session-filter

Syntax	session-filter <i>session-filter-name</i> [create] no session-filter <i>session-filter-name</i>
Context	config>app-assure>group
Description	This command creates a session filter.
Parameters	<i>session-filter-name</i> — Creates a session filter name up to 32 characters. create — Keyword used to create the session filter.

default-action

Syntax	default-action { permit deny } [event-log <i>event-log-name</i>]

Context	config>app-assure>group>sess-fltr
Description	This command specifies the default action to take for packets that do not match any filter entries. The no form of the command reverts the default action to the default value (forward).
Default	default-action deny
Parameters	deny — Indicates that packets matching the criteria are denied permit — Indicates that packets matching the criteria are permitted. <i>event-log-name</i> — Specifies the event log name, up to 32 characters.

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>app-assure>group>policy>sess-fltr
Description	This command configures a particular Application-Assurance session filter match entry. Every session filter can have zero or more session filter match entries. An application filter entry or entries configures match attributes of an application. The no form of this command deletes the specified entry.
Default	none
Parameters	<i>entry-id</i> — Specifies an integer that identifies the entry. Values 1 to 65535 create — Keyword used to create the entry.

action

Syntax	action { permit deny } [event-log <i>event-log-name</i>] action application <i>application-name</i> action http-redirect <i>http-redirect-name</i> [event-log <i>event-log-name</i>] action tcp-optimizer <i>tcp-optimizer-name</i>
Context	config>app-assure>group>sess-fltr>entry
Description	This command configures the action for this entry.
Parameters	deny — Packets matching the criteria are denied permit — Packets matching the criteria are permitted.

event-log-name — Specifies the event log name, up to 32 characters.

application-name — Specifies the application name, up to 32 characters.

http-redirect-name — Specifies the HTTP redirect name, up to 32 characters.

tcp-optimizer-name — Specifies the TCP optimizer name, up to 32 characters.

match

Syntax	match
Context	config>app-assure>group>sess-fltr>entry
Description	This command enables the context to configure session conditions for this entry.

dst-ip

Syntax	dst-ip ip-address dst-ip dns-ip-cache dns-ip-cache-name dst-ip ip-prefix-list ip-prefix-list-name no dst-ip
Context	config>app-assure>group>sess-fltr>entry>match
Description	This command configures the destination IP address to match.
Default	no dst-ip
Parameters	ip-address — Specifies a valid unicast address.

Values		
ipv4-address	a.b.c.d[/mask]	
	mask - [1..32]	
ipv6-address	x:x:x:x:x:x/x/prefix-length	
	x:x:x:x:x:x.d.d.d.d	
	x - [0..FFFF]H	
	d - [0..255]D	
	prefix-length [1..128]	

dns-ip-cache-name — Specifies the name of the dns-ip-cache policy.

dst-port

Syntax	dst-port {eq gt lt} port-num

dst-port port-list *port-list-name*
dst-port range *start-port-num end-port-num*
no dst-port

Context	config>app-assure>group>sess-fltr>entry>match
Description	This command specifies a destination TCP/UDP port, destination port list, or destination range to use as match criteria. The no form of the command removes the parameters from the configuration.
Default	no dst-port
Parameters	eq — Specifies that a successful match occurs when the flow matches the specified port. gt — Specifies all port numbers greater than the port-number match. lt — Specifies all port numbers less than the port-number match. <i>port-num</i> — Specifies the destination port number. Values 0 to 65535 <i>start-port-num end-port-num</i> — Specifies the start or end destination port number. Values 0 to 65535 <i>port-list-name</i> — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

ip-protocol-num

Syntax	ip-protocol-num {<i>ip-protocol-number</i> <i>protocol-name</i>} no ip-protocol-num
Context	config>app-assure>group>policy>sess-fltr>entry>match
Description	This command configures the IP protocol to use in the application definition. The no form of the command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).
Default	no ip-protocol-num
Parameters	<i>ip-protocol-number</i> <i>protocol-name</i> — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17). The no form the command removes the protocol from the match criteria. Values 1 to 255 (Decimal, Hexadecimal, or Binary representation). Supported IANA IP protocol names:

none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp, tcp, udp, vrrp
* - udp/tcp wildcard

src-ip

Syntax	src-ip <i>ip-address</i> src-ip ip-prefix-list <i>ip-prefix-list-name</i> no src-ip		
Context	config>app-assure>group>sess-fltr>entry>match		
Description	This command specifies a source TCP/UDP address to use as match criteria.		
Default	no src-ip		
Parameters	<i>ip-address</i> — Specifies a valid unicast address.		
	Values		
	ipv4-address	a.b.c.d[/mask]	
		mask - [1..32]	
	ipv6-address	x:x:x:x:x:x/x/prefix-length	
		x:x:x:x:x:x.d.d.d.d	
		x - [0..FFFF]H	
		d - [0..255]D	
		prefix-length [1..128]	

ip-prefix-list-name — Specifies an IP prefix list name, up to 32 characters.

src-port

Syntax	src-port {eq gt lt} <i>port-num</i> src-port port-list <i>port-list-name</i> src-port range <i>start-port-num end-port-num</i> no src-port		
Context	config>app-assure>group>sess-fltr>entry>match		
Description	This command specifies a source IP port, source port list, or source range to use as match criteria.		
	The no form of the command removes the parameters from the configuration.		

Default	no src-port
Parameters	eq — Specifies that a successful match occurs when the flow matches the specified port. gt — Specifies all port numbers greater than the port-number match. lt — Specifies all port numbers less than the port-number match. <i>port-num</i> — Specifies the source port number. Values 0 to 65535 <i>start-port-num end-port-num</i> — Specifies the start or end source port number. Values 0 to 65535 <i>port-list-name</i> — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

dns-ip-cache

Syntax	dns-ip-cache <i>dns-ip-cache-name</i>
Context	config>app-assure>group>sess-fltr>entry>match
Description	This command configures a DNS IP cache using session filter DST IP match criteria. It is typically combine with an allow action in the context of captive-redirect.
Parameters	<i>dns-ip-cache-name</i> — Specifies the name of the dns-ip-cache policy.

http-redirect

Syntax	http-redirect <i>http-redirect-name</i>
Context	config>app-assure>group>sess-fltr>entry>action
Description	This command configures a session filter entry action to HTTP redirect the subscriber flows. The HTTP redirect policy referenced within this session filter entry is configured for captive redirect with the appropriate VLAN id assigned.
Parameters	<i>http-redirect-name</i> — Specifies the name of the http-redirect-policy.

3.4.2.4.4 Statistics Commands

statistics

Syntax	statistics

Context	config>app-assure>group
Description	This command enables the context to configure accounting and billing statistics for this AA ISA group.

aa-admit-deny

Syntax	aa-admit-deny
Context	config>app-assure>group>statistics
Description	This command enables the context to configure admit-deny statistics generation.

accounting-policy

Syntax	accounting-policy <i>acct-policy-id</i> no accounting-policy
Context	config>app-assure>group>statistics>aa-admit-deny config>app-assure>group>statistics>aa-partition config>app-assure>group>statistics>aa-sub config>app-assure>group>statistics>aa-sub-study config>app-assure>group>statistics>application config>app-assure>group>statistics>app-grp config>app-assure>group>statistics>protocol config>isa>aa-grp>statistics
Description	This command specifies the existing accounting policy to use for AA. Accounting policies are configured in the config>log>accounting-policy context.
Parameters	<i>acct-policy-id</i> — Specifies the existing accounting policy to use for applications.
Values	1 to 99

collect-stats

Syntax	[no] collect-stats
Context	config>app-assure>group>statistics>aa-admit-deny config>app-assure>group>statistics>aa-partition config>app-assure>group>statistics>aa-sub config>app-assure>group>statistics>aa-sub-study config>app-assure>group>statistics>app-grp config>app-assure>group>statistics>application config>app-assure>group>statistics>protocol config>isa>aa-grp>statistics

Description	This command enables statistic collection within the applicable context.

Default	disabled

gtp-filter-stats

Syntax	[no] gtp-filter-stats

Context	config>app-assure>group>statistics>aa-admit-deny

Description	This command configures whether to include or exclude GTP filter admit-deny statistics in accounting records.

Default	no gtp-filter-stats

policer-stats

Syntax	[no] policer-stats

Context	config>app-assure>group>statistics>aa-admit-deny

Description	This command configures whether to include or exclude system and subscriber-level flow count and flow-setup rate policer admit-deny statistics in accounting records.

Default	no policer-stats

policer-stats-resources

Syntax	[no] policer-stats-resources

Context	config>app-assure>group>statistics>aa-admit-deny

Description	This command allows the operator to allocate or deallocate AA partition resources for policer admit-deny statistics.

Default	no policer-stats-resources

sctp-filter-stats

Syntax	[no] sctp-filter-stats

Context	config>app-assure>group>statistics>aa-admit-deny

Description	This command configures whether to include or exclude SCTP filter admit-deny statistics in accounting records.

Default no sctp-filter-stats

session-filter-stats

Syntax [no] session-filter-stats

Context config>app-assure>group>statistics>aa-admit-deny

Description This command configures whether to include or exclude session filter admit-deny statistics in accounting records.

Default no session-filter-stats

tcp-validate-stats

Syntax [no] tcp-validate-stats

Context config>app-assure>group>statistics>aa-admit-deny

Description This command configures whether to include or exclude TCP validation admit-deny statistics in accounting records.

Default no tcp-validate-stats

traffic-type

Syntax [no] traffic-type

Context config>app-assure>group>statistics>aa-partition

Description This command enables traffic type statistics collection within an aa-partition.
The no form of the command disables traffic type statistics collection.

aa-sub

Syntax aa-sub

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per application assurance subscribers.

aggregate-stats

Syntax	aggregate-stats export-using <i>export-method</i> [<i>export-method...</i> (up to 2 max)] aggregate-stats no-export
Context	config>app-assure>group>statistics>aa-sub
Description	This command configures aa-sub accounting statistics for export of aggregate statistics of a given subscriber.
Default	aggregate-stats no-export
Parameters	<i>export-method</i> — Specifies the method of statistics export to be used. Values accounting-policy (this is the only option for sub-aggregate statistics, and it is only supported in residential and VPN sub-scale modes). no-export — Disables the export.

app-group

Syntax	app-group <i>app-group-name</i> export-using <i>export-method</i> [<i>export-method...</i> (up to 2 max)] app-group <i>app-group-name</i> no-export no app-group <i>app-group-name</i>
Context	config>app-assure>group>statistics>aa-sub
Description	This command enables the context to configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition. The no form of the command removes the application group name.
Default	none
Parameters	<i>app-group-name</i> — Specifies an existing application group name, up to 32 characters. <i>export-method</i> — Specifies the method of statistics export to be used. Values accounting-policy, radius-accounting-policy no-export — Allows the operator to enable the referred to application group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the export-using parameter is selected for the respective application group. Usage monitoring must be enabled at the group:partition level (config>app-assure>group>statistics>aa-sub>usage-monitoring) as well in order to allow any application/application group/charging group usage monitoring.

aa-sub-study

Syntax	aa-sub-study <i>study-type</i>
Context	config>app-assure>group>statistics
Description	This command enables the context to configure accounting and statistics collection parameters per application assurance special study subscribers.
Parameters	<i>study-type</i> — Specifies special study protocol subscriber stats.
Values	application, protocol

application

Syntax	application <i>application-name</i> export-using <i>export-method</i> [<i>export-method...</i> (up to 2 max)] application <i>application-name</i> no-export no application <i>application-name</i>
Context	config>app-assure>group>statistics>aa-sub
Description	This command configures aa-sub accounting statistics for export of applications of a given AA ISA group/partition. The no form of the command removes the application name.
Default	none
Parameters	<i>application-name</i> — Specifies an existing application name, up to 32 characters. <i>export-method</i> — Specifies the method of statistics export to be used. Values accounting-policy, radius-accounting-policy no-export — Allows the operator to enable the referred application group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the export-using parameter is selected for the respective application group. Usage monitoring must be enabled at the group:partition level (config>app-assure>group>statistics>aa-sub>usage-monitoring) as well in order to allow any application/application group/charging group usage monitoring.

charging-group

Syntax	charging-group <i>charging-group-name</i> export-using <i>export-method</i> [<i>export-method...</i> (up to 2 max)] charging-group <i>charging-group-name</i> no-export no charging-group <i>charging-group-name</i>

Context	config>app-assure>group>statistics>aa-sub
Description	This command configures aa-sub accounting statistics for export of charging groups of a given AA ISA group/partition. The no form of the command removes the parameters from the configuration.
Default	none
Parameters	<i>charging-group-name</i> — The name of the charging group. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces. export-using <i>export-method</i> — Specifies that the method of stats export to be used. Values accounting-policy, radius-accounting-policy no-export — Allows the operator to enable the referred to a charging group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the export-using parameter is selected for the respective charging group. Usage monitoring must be enabled at the group:partition level (config>app-assure>group>statistics>aa-sub>usage-monitoring) as well in order to allow any application/application group/charging group usage monitoring.

exclude-tcp-retrans

Syntax	[no] exclude-tcp-retrans
Context	config>app-assure>group>statistics>aa-sub
Description	This command is to only to EPC. When enabled, TCP errors and retransmission packets are not counted for the purpose of CBC. This setting has no impact on app/app-group aggregate AA stats.
Default	no exclude-tcp-retrans

max-throughput-stats

Syntax	[no] max-throughput-stats
Context	config>app-assure>group>statistics>aa-sub
Description	This command enables the collection of max-throughput statistics. The no form of the command disables the collection.
Default	no max-throughput-stats

protocol

Syntax	protocol <i>protocol-name</i> export-using <i>export-method</i> no protocol <i>protocol-name</i>
Context	config>app-assure>group>statistics>aa-sub
Description	This command configures aa-sub accounting statistics for export of protocols of a given AA ISA group/partition. The no form of the command removes the protocol name.
Default	none
Parameters	<i>protocol-name</i> — Specifies an existing protocol name up to 32 characters in length. export-using <i>export-method</i> — Specifies that the method of stats export to be used. Accounting-policy is the only option for protocol statistics.

protocol

Syntax	protocol
Context	config>app-assure>group>statistics
Description	This command enables the context to configure accounting and statistics collection parameters per-system for protocols of application assurance for a given AA ISA group/partition.

aa-sub

Syntax	[no] aa-sub { esm <i>sub-ident-string</i> sap <i>sap-id</i> spoke-sdp <i>sdp-id:vc-id</i> transit <i>transit-aasub-name</i> esm-mac <i>esm-mac-name</i> }
Context	config>app-assure>group>statistics>aa-sub-study
Description	This command adds an existing subscriber identification to a group of special study subscribers (for example, subscribers for which per subscriber statistics and accounting records can be collected for protocols and applications of application assurance). The no form of the command removes the subscriber from the special study subscribers. Up to 100 subscribers can be configured into the special study group for protocols and up to a 100 potentially different subscribers can be configured into the special study group for applications. When adding a subscriber to the special study group, accounting records and statistics generation will commence immediately. When removing a subscriber from the group, special study statistics and accounting records for that subscriber in the current interval will be lost.

Default	none
Parameters	<i>sub-ident-string</i> — Specifies the name of a subscriber ID. The subscriber does not need to be currently active. Any sub-ident-string will be accepted. When the subscriber becomes active, statistics generation will start automatically at that time. <i>sap-id</i> — Specifies the physical port identifier portion of the SAP definition. <i>spoke-id sdp-id:vc-id</i> — Specifies the spoke SDP ID and VC ID. Values 1 to 32767 1 to 4294967295 <i>transit-aasub-name</i> — Specifies an existing transit subscriber name string, up to 32 characters in length. <i>esm-mac-name</i> — Specifies an existing ESM-MAC subscriber name, up to 32 characters.

radius-accounting-policy

Syntax	radius-accounting-policy <i>rad-acct-plcy-name</i> no radius-accounting-policy
Context	config>app-assure>group>statistics>aa-sub
Description	This command specifies an existing subscriber RADIUS based accounting policy to use for AA. RADIUS Accounting policies are configured in the config>app-assure>radius-accounting-policy context.
Default	no radius-accounting-policy
Parameters	<i>rad-acct-plcy-name</i> — Specifies the name of the policy. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

usage-monitoring

Syntax	[no] usage-monitoring
Context	config>app-assure>group>statistics>aa-sub
Description	This command enables Gx usage monitoring the given AA group/partition. It can only be enabled if there is enough usage monitoring resources for all existing subs. Once disabled, all monitoring instances for AA subscribers are silently removed (no PCRF notifications) and all subsequent AA Gx usage monitoring messages are ignored.
Default	no usage-monitoring.

threshold-crossing-alert

Syntax	threshold-crossing-alert
Context	config>app-assure>group>statistics
Description	This command enables the context to configure the generation of threshold crossing alerts (TCAs).

error-drop

Syntax	error-drop direction <i>direction</i> [create] no error-drop direction <i>direction</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures a TCA for the counter capturing error drops. An error drop TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating an error-drop TCA.
Default	none
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the error drop TCA.

fragment-drop-all

Syntax	fragment-drop-all direction [create] no fragment-drop-all direction
Context	config>app-assure>group>statistics>tca
Description	This command configures a TCA for the counter capturing drops due to the fragment-drop-all AQP command. A fragment-drop-all TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a fragment-drop-all TCA.
Default	none
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

fragment-drop-out-of-order

Syntax	fragment-drop-out-of-order <i>direction</i> [create] no fragment-drop-out-of-order <i>direction</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures a TCA for the counter capturing drops due to the fragment-drop-out-of-order AQP command. A fragment-drop-out-of-order TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a fragment-drop-out-of-order TCA.
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

gtp-filter

Syntax	gtp-filter <i>filter-name</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures TCA generation for a GTP filter.
Parameters	<i>filter-name</i> — Specifies the name of the GTP filter, up to 32 characters.

max-payload-length

Syntax	max-payload-length <i>direction</i> [create] no max-payload-length <i>direction</i>
Context	config>app-assure>group>statistics>tca>gtp-filter
Description	This command configures a TCA for the counter capturing drops due to the GTP filter maximum payload length. A maximum payload length drop TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a maximum payload length drop TCA.
Default	none
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

message-type

Syntax	message-type
Context	config>app-assure>group>statistics>tca>gtp-filter
Description	This command configures a TCA for the counter capturing hits due to the GTP filter message type.
Default	none

default-action

Syntax	default-action direction <i>direction</i> [create] no default-action direction <i>direction</i>
Context	config>app-assure>group>statistics>tca>gtp-fltr>msg
Description	This command configures a TCA for the counter capturing hits for the specified GTP filter default action. A default action TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a default action TCA.
Default	none
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

entry

Syntax	entry entry-id direction <i>direction</i> [create] no entry entry-id direction <i>direction</i>
Context	config>app-assure>group>statistics>tca>gtp-fltr>msg
Description	This command configures a TCA for the counter capturing hits for the specified GTP filter entry. A GTP filter entry TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a default action TCA.
Default	none
Parameters	<i>entry-id</i> — Specifies the GTP filter message-type entry identifier. Values 1 to 255

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

header-sanity

Syntax **header-sanity direction** *direction* [**create**]
no header-sanity direction *direction*

Context config>app-assure>group>statistics>tca>gtp-fltr>msg

Description This command configures a TCA for the counter capturing hits for the GTP filter header sanity. A GTP filter header-sanity TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Default none

Parameters *direction* — Specifies the traffic direction.
Values from-sub, to-sub
create — Keyword used to create the TCA.

gtp-sanity-drop

Syntax **gtp-sanity-drop direction** *direction* [**create**]
no gtp-sanity-drop direction *direction*

Context config>app-assure>group>statistics>tca

Description This command configures a TCA for the counter capturing drops due to basic GTP header sanity checks, such as validating that the GTP-U version is 1 and that the protocol bit is set to 1 for UDP traffic destined to port 2152. A GTP sanity drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Default none

Parameters *direction* — Specifies the traffic direction.
Values from-sub, to-sub
create — Keyword used to create the TCA.

overload-drop

Syntax	overload-drop direction <i>direction</i> [create] no overload-drop direction <i>direction</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures a TCA for the counter capturing drops due to the overload-drop AQP command. An overload-drop TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating an overload-drop TCA.
Default	none
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

policer

Syntax	policer <i>policer-name</i> direction <i>direction</i> [create] no policer <i>policer-name</i> direction <i>direction</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures a TCA for the counter capturing drops or admit events due to the specified flow policer. A policer TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a policer TCA.
Default	none
Parameters	<i>policer-name</i> — Specifies the name of the flow policer, up to 32 characters <i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

sctp-filter

Syntax	sctp-filter <i>sctp-filter-name</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures TCA generation for an SCTP filter.
Default	none

Parameters *sctp-filter-name* — Specifies the name of the SCTP filter, up to 32 characters

packet-sanity

Syntax **packet-sanity direction** *direction* [**create**]
 no packet-sanity direction *direction*

Context config>app-assure>group>statistics>tca>sctp-filter

Description This command configures a TCA for the counter capturing packet sanity hits for the specified SCTP filter. A packet sanity TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Default none

Parameters *direction* — Specifies the traffic direction.
 Values from-sub, to-sub
 create — Keyword used to create the TCA.

ppid

Syntax **ppid**

Context config>app-assure>group>statistics>tca>sctp-filter

Description This command configures a TCA for the counter capturing PPID hits for the specified SCTP filter.

Default none

default-action

Syntax **default-action direction** *direction* [**create**]

Context config>app-assure>group>statistics>tca>sctp-fltr>ppid

Description This command configures a TCA for the counter capturing hits for the specified SCTP filter default PPID. A default action TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Default none

Parameters *direction* — Specifies the traffic direction.
 Values from-sub, to-sub
 create — Keyword used to create the TCA.

entry

Syntax **entry** *entry-id direction direction* [**create**]
 no entry *entry-id direction direction*

Context config>app-assure>group>statistics>tca>sctp-fltr>ppid

Description This command configures a TCA for the counter capturing hits for the specified SCTP filter PPID entry. An SCTP filter entry TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Default none

Parameters *entry-id* — Specifies the SCTP filter PPID entry identifier.
 Values 1 to 255
 direction — Specifies the traffic direction.
 Values from-sub, to-sub
 create — Keyword used to create the TCA.

ppid-range

Syntax **ppid-range direction direction** [**create**]
 no ppid-range direction direction

Context config>app-assure>group>statistics>tca>sctp-filter

Description This command configures a TCA for the counter capturing hits for the specified SCTP filter PPID range command. An PPIPD range TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Default none

Parameters *direction* — Specifies the traffic direction.
 Values from-sub, to-sub
 create — Keyword used to create the TCA.

session-filter

Syntax	session-filter <i>session-filter-name</i>
Context	config>app-assure>group>statistics>tca
Description	This command configures TCA generation for a session filter.
Default	none
Parameters	<i>session-filter-name</i> — Specifies the name of the session filter, up to 32 characters.

default-action

Syntax	default-action direction <i>direction</i> [create] no default-action direction <i>direction</i>
Context	config>app-assure>group>statistics>tca>session-filter
Description	This command configures a TCA for the counter capturing hits for the specified session filter default action. A default action TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a default action TCA.
Default	none
Parameters	<i>direction</i> — Specifies the traffic direction. Values from-sub, to-sub create — Keyword used to create the TCA.

entry

Syntax	entry entry-id direction <i>direction</i> [create] no entry entry-id direction <i>direction</i>
Context	config>app-assure>group>statistics>tca>session-filter
Description	This command configures a TCA for the counter capturing hits for the specified session filter entry. A session filter entry TCA can be created for traffic generated from the subscriber side of AA (from-sub) or for traffic generated from the network toward the AA subscriber (to-sub). The create keyword is mandatory when creating a TCA.
Default	none
Parameters	<i>entry-id</i> — Specifies the SCTP filter PPID entry identifier. Values 1 to 65535

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

high-wmark

Syntax	high-wmark <i>high-watermark</i> low-wmark <i>low-watermark</i>
Context	<pre> config>app-assure>group>statistics>tca>error-drop config>app-assure>group>statistics>tca>fragment-drop-all config>app-assure>group>statistics>tca>fragment-drop-out-of-order config>app-assure>group>statistics>tca>gtp-fltr>max-payload-length config>app-assure>group>statistics>tca>gtp-fltr>msg>default-action config>app-assure>group>statistics>tca>gtp-fltr>msg>entry config>app-assure>group>statistics>tca>gtp-fltr>msg>header-sanity config>app-assure>group>statistics>tca>gtp-sanity-drop config>app-assure>group>statistics>tca>overload-drop config>app-assure>group>statistics>tca>policer config>app-assure>group>statistics>tca>sctp-fltr>packet-sanity config>app-assure>group>statistics>tca>sctp-fltr>ppid>default-action config>app-assure>group>statistics>tca>sctp-fltr>ppid>entry config>app-assure>group>statistics>tca>sctp-fltr>ppid>ppid-range config>app-assure>group>statistics>tca>sess-fltr>default-action config>app-assure>group>statistics>tca>sess-fltr>entry config>app-assure>group>statistics>tca>tcp-validate </pre>
Description	This command configures the high watermark and low watermark thresholds for the specified TCA.
Default	high-wmark 4294967295 low-wmark 0
Parameters	<i>high-watermark</i> — Specifies the TCA high watermark. Values 1 to 4294967295 Default 4294967295 <i>low-watermark</i> — Specifies the TCA low watermark. Values 0 to 4294967294 Default 0

tcp-validate

Syntax	tcp-validate <i>tcp-validate-name</i> direction <i>direction</i> [create] no tcp-validate <i>tcp-validate-name</i> direction <i>direction</i>
Context	config>app-assure>group>statistics>tca

Description	This command configures TCA for the counter, and enables the capture of drop or admit events due to the specified TCP validation function.
Default	none
Parameters	<i>tcp-validate-name</i> — Specifies the name of the TCP validation policy up to 32 characters. <i>direction</i> — Specifies the traffic direction in relation to the AA subscriber Values from-sub, to-sub create — This keyword is mandatory when creating a TCA instance

3.4.2.4.5 TCP Validation Commands

tcp-validate

Syntax	tcp-validate <i>tcp-validate-name</i> [create] no tcp-validate <i>tcp-validate-name</i>
Context	config>app-assure>group
Description	This command configures a TCP validation policy. The no form of the command removes the specified TCP validation policy.
Default	no tcp-validate
Parameters	<i>tcp-validate-name</i> — Specifies the name of the TCP validation policy up to 32 characters. create — This keyword is mandatory when creating a TCP validation policy.

event-log

Syntax	event-log <i>event-log-name</i> [all] no event-log
Context	config>app-assure>group>tcp-validate
Description	This command enables logging of traffic dropped by TCP validation. The no form of the command disables logging of traffic dropped by TCP validation.
Default	no event-log
Parameters	<i>event-log-name</i> — Specifies the name of the event log up to 32 characters.

all — Logs all dropped traffic. Using the **all** option allows the operator to capture all discards made by the TCP validation policy, including those related to:

- packets that were received after an RST and discarded
- packets received before TCP session establishment (before SYN) and discarded

Without the **all** option, discards related to these cases are not captured in any event log.

strict

Syntax	[no] strict
Context	config>app-assure>group>tcp-validate
Description	This command specifies whether enforcement of TCP sequence and acknowledgment numbers is applied. If a packet does not meet the expected sequence or acknowledgment number, it is dropped. This command should only be enabled if the expected bit error rate or packet loss is low. For example, if acknowledgments are lost before being detected by AA, the server timeouts are triggered and retransmissions occur. If strict is enabled, these retransmissions would resemble a reply attack and would be dropped by AA. The no form of the command removes TCP sequence and acknowledgment number enforcement.
Default	no strict

3.4.2.4.6 Policy Commands

transit-ip-policy

Syntax	transit-ip-policy <i>ip-policy-id</i> [create] no transit-ip-policy <i>ip-policy-id</i>
Context	config>app-assure>group
Description	This command defines a transit AA subscriber IP policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service. The no form of the command deletes the policy from the configuration. All associations must be removed in order to delete a policy.
Default	no transit-ip-policy

Parameters *ip-policy-id* — Specifies an integer that identifies a transit IP profile entry.

Values 1 to 65535

create — A keyword used to create the entry.

diameter

Syntax **diameter**

Context config>app-assure>group>transit-ip

Description This command enables the context to configure dynamic Diameter-based management of transit AA subs for the transit IP policy. This is mutually exclusive to other types of management of transit subs for a given transit IP policy.

application-policy

Syntax [no] **application-policy** *name*

Context config>app-assure>group>transit-ip>diameter

Description This command specifies the Diameter application to be used by seen IP transit subs. The application policy is defined using the **config>subscr-mgmt>diameter-application-policy** command.

 The **no** form of the command removes the policy.

Default no application-policy

Parameters *name* — Specifies the name of the application policy configured using the **diameter-application-policy** command up to 32 characters.

shutdown

Syntax [no] **shutdown**

Context config>app-assure>group>transit-ip>diameter

Description This command removes all transit AA subscribers created via Diameter on this transit AA subscriber IP policy and clears all corresponding Diameter sessions.

gtp

Syntax **gtp**

Context	config>app-assure>group
Description	This command enters the context to configure GTP parameters.

event-log

Syntax	event-log <i>event-log-name</i> no event-log
Context	config>app-assure>group>gtp config>app-assure>group>gtp>gtp-filter
Description	This command allows AA to treat traffic on UDP port number 2152 as GTP-u. Without further specifying any other parameters within this GTP context, AA performs basic GTP-u header sanity checks and discards packets that are malformed. This GTP context allows the operator to configure various GTP filters (maximum of 128 GTP filters).
Default	no event-log
Parameters	<i>event-log-name</i> — Specifies the event log name to be used to log discards due to GTP-u basic header sanity checks.

gtp-filter

Syntax	gtp-filter <i>gtp-filter-name</i> [create] no gtp-filter <i>gtp-filter-name</i>
Context	config>app-assure>group>gtp
Description	This command allows AA to treat traffic on UDP port number 2152 as GTP-u. Without further specifying any other parameters within this GTP context, AA performs basic GTP-u header sanity checks and discards packets that are malformed. This GTP context allows the operator to configure various GTP filters (maximum of 128 GTP filters).
Parameters	<i>gtp-filter-name</i> — Specifies a GTP filter name, up to 32 characters. create — Keyword used to create the GTP filter name and parameters.

max-payload-length

Syntax	max-payload-length <i>bytes</i> no max-payload-length
Context	config>app-assure>group>gtp>gtp-filter
Description	This command specifies the maximum allowed GTP payload size.

The **no** form of the command removes this GTP message length filter.

Default	no max-payload-length
Parameters	<i>bytes</i> — Specifies the packet length in bytes.
Values	0 to 65535

message-type

Syntax	message-type
Context	config>app-assure>group>gtp>gtp-filter
Description	This command specifies the context for configuration of GTP message-type filtering.
Default	None. If no message-type is specified within a filter, then all GTP message types are allowed.

default-action

Syntax	default-action {permit deny}
Context	config>app-assure>group>gtp>gtp-fltr>message-type
Description	This command configures the default action for all GTP message types.
Default	default-action permit
Parameters	permit — Specifies to permit packets that do not match any message entries. deny — Specifies to deny packets that do not match any message entries.

entry

Syntax	entry entry-id value gtp-message-value action {permit deny} no entry entry-id
Context	config>app-assure>group>gtp>gtp-fltr>message-type
Description	This command configures an entry for a specific GTP message type value.
Parameters	<i>entry-id</i> — Specifies the index into the GTP message value list that defines a custom message-type action. Values 1 to 255

gtp-message-value — Specifies the GTP-u message type, either as a numeric value or as a string.

Values 1 to 255 or 256 characters {echo-request, echo-response, error-indication, g-pdu, supported-extension-headers-notification}

permit | deny — Specifies the action to take for packets that match this GTP filter message entry.

mode

Syntax	mode <i>mode</i>
Context	config>app-assure>group>gtp
Description	This command is used to either untunnel GTP-U traffic received on UDP port number 2152, or apply GTP filtering/firewall rules as specified under this GTP CLI context.
Default	mode filtering
Parameters	<i>mode</i> — Specifies the operational mode of the command. Values filtering — AA applies GTP filtering rules to GTP-U traffic, without further analysis of IP traffic tunneled within GTP. untunneling — AA untunnels GTP traffic and provides analytical reporting of the applications running within the GTP tunnels. The rest of the commands under GTP CLI context (such as GTP-filter and event-log) are not applicable in this mode. Please note that for AA to untunnel GTP traffic, the operator must configure “gtp” under the partition by using the config>app-assure>group>gtp command. The following caveats apply: • Only GTP-U traffic with TID <> 0 is untunneled. • Any UDP but non-GTP traffic that uses port 2152 will be identified as UDP traffic. • Only GTP-U packets with message type: G-PDU (0xFF) is untunneled. Other GTP-U packets with different message types are reported as GTP Protocol. • Only GTP-u packets with non-fragmented outer IP and no IPv4 options or IPv6 extension headers are untunneled. Otherwise, no inner GTP tunnel classification is performed and the traffic is identified and reported as GTP protocol.

sctp-filter

Syntax **sctp-filter** *sctp-filter-name* [create]

no sctp-filter *sctp-filter-name*

Context config>app-assure>group

Description This command enables the context to configure Stream Control Transmission Protocol (SCTP) parameters.

The **no** form of the command removes this filter.

Parameters *sctp-filter-name* — Specifies the SCTP filter name, up to 32 characters.
create — Keyword used to create the SCTP filter.

event-log

Syntax **event-log** *event-log-name*
no event-log

Context config>app-assure>group>sctp-filter

Description This command configures an event log for packets dropped by the SCTP filter

Default no event-log

Parameters *event-log-name* — Specifies the event log name to be used.

ppid

Syntax **ppid**

Context config>app-assure>group>sctp-filter

Description This command enables the context to configure actions for specific or default Payload Protocol Identifiers (PPIDs).

default-action

Syntax **default-action** {**permit** | **deny**}

Context config>app-assure>group>sctp-fltr>ppid

Description This command configures the default action for all SCTP PPIDs.

Default default-action permit

Parameters **permit** — Specifies to permit packets that do not match any PPID entries.
deny — Specifies to deny packets that do not match any PPID entries.

entry

Syntax	entry <i>entry-id</i> value <i>ppid-value</i> action { permit deny } no entry <i>entry-id</i>
Context	config>app-assure>group>sctp-fltr>ppid
Description	This command specifies if an SCTP PPID value is allowed or not. The no form of the command removes this PPID. In which case, the default action for the sctp-filter>ppid is applied.
Parameters	<i>entry-id</i> — Specifies the SCTP filter PPID entry identifier. <i>ppid-value</i> — Specifies the PPID value, either as numeric value or as a string. Values 0 to 4294967295 D, 256 chars max action {permit deny} — Specifies to allow or deny the configured PPID.

ppid-range

Syntax	ppid-range min <i>min-ppid</i> max <i>max-ppid</i> no ppid-range
Context	config>app-assure>group>sctp-filter
Description	This command specifies the range of PPID values that are allowed by AA SCTP filter firewall. The no form of the command removes this PPID range.
Default	no ppid-range
Parameters	<i>min-ppid</i> — Specifies the minimum SCTP Payload Protocol Identifier (PPID) to be permitted by the SCTP filter. The value must be less than or equal to the max <i>max-ppid</i> value. Values 0 to 4294967295 <i>max-ppid</i> — Specifies the minimum SCTP Payload Protocol Identifier (PPID) to be permitted by the SCTP filter. The value must be greater or equal to the min <i>min-ppid</i> value. Values 0 to 4294967295

access-network-location

Syntax	access-network-location
Context	config>app-assure>group

Description This command provides the context to configure parameters related to dynamic experience management, also known as Access Network Location (ANL).

These parameters include location source type congestion point and congestion detection parameters (such as roundtrip delay thresholds), if applicable.

source

Syntax **source** *source-type*
source *source-type level level*
no source *source-type*

Context config>app-assure>group>anl

Description This command configures location sources for the dynamic experience management. The location source types are, for example, 3G and congestion point.

Default no source *source-type*

Parameters *source-type* — Specifies the location or access technology.

Values **access-point** — Provides Dynamic Experience Management (DEM) for the WLGW access point.



Note: The access points do not need to support the Nokia CEA function.

level — Specifies which congestion point within the specified source-type to monitor for congestion.

Values **MAC+VLAN** — WLGW access point (MAC) and radio (VLAN).



Note: The access points do not need to support the Nokia CEA function.

rtt-threshold

Syntax **rtt-threshold** *threshold*
no rtt-threshold

Context config>app-assure>group>anl>source>level

Description This command configures the ANL roundtrip delay threshold to be used for congestion detection algorithm (if applicable).

Default	rtt-threshold 173
Parameters	<i>threshold</i> — This parameter is used by the DEM-GW algorithm that determines ANL congestion. It specifies the maximum acceptable round trip time (RTT), in milliseconds, for TCP connections under no congestion. Any measured RTT above the threshold is considered an indication of possible congestion.
Values	0 to 500

rtt-threshold-tolerance

Syntax	rtt-threshold-tolerance <i>tolerance</i> no rtt-threshold-tolerance
Context	config>app-assure>group>anl>source>level
Description	This command configures the ANL roundtrip delay threshold tolerance to be used for congestion detection algorithm (if applicable).
Parameters	<i>tolerance</i> — This parameter is used by the DEM-GW algorithm that determines ANL congestion. It represents the ratio in percentage, of RTTs above the configured threshold (rtt-threshold) over the total RTT measurements. The ratio is calculated as follows, measured across a one-minute period: $\text{rtt-threshold-tolerance} = \#(\text{RTTs} > \text{rtt-threshold}) / (\text{Total } \# \text{RTTs})$ If the rtt-threshold-tolerance ratio is exceeded, the ANL is declared congested.
Values	0 to 100
Default	50

aqp-initial-lookup

Syntax	aqp-initial-lookup no aqp-initial-lookup
Context	config>app-assure>group:[partition]
Description	This command allows AA to perform AQP lookups on flows prior to complete application identification. As usual, AQP will be looked up again on identification complete. Without this, AA executes AQPs that are part of what so called “sub-default policy”. Sub-default policy is formed by regular AQPs that contain ASOs, subID and/or flow direction as matching conditions. This behavior is required, for example, in order to be able apply GTP and SCTP filtering on the first packet of a new GTP/SCTP flow (AQP matching conditions in this case contains protocol id). The no form of the command forces complete AQP look up on identification finish stage only

Default no aqp-initial-lookup

dhcp

Syntax **dhcp**

Context config>app-assure>group>transit-ip-policy

Description This command enables dynamic DHCP-based management of transit aa-subnets for the transit-ip-policy. This is mutually exclusive to other types management of transit subnets for a given transit-ip-policy.

ipv6-address-prefix-length

Syntax **ipv6-address-prefix-length** *IPv6-prefix-length*
no ipv6-address-prefix-length

Context config>app-assure>group>transit-ip-policy

Description This command configures a transit IP policy IPv6 address prefix length.

Default no ipv6-address-prefix-length

Parameters *IPv6-prefix-length* — Specifies the prefix length of IPv6 addresses in this policy for both static and dynamic transits.

Values 32 to 64

def-app-profile

Syntax **def-app-profile** *app-profile-name*
no def-app-profile

Context config>app-assure>group>transit-ip-policy

Description This command configures a default application profile.

Default no def-app-profile

Parameters *app-profile-name* — Specifies the application profile name, up to 32 characters.

detect-seen-ip

Syntax **[no] detect-seen-ip**

Context config>app-assure>group>transit-ip-policy

Description This command enables the detection of transit subscribers based on the IP address.

radius

Syntax **radius**

Context config>app-assure>group>transit-ip-policy

Description This command enables dynamic radius based management of transit aa-subs for the transit-ip-policy. This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

authentication-policy

Syntax **authentication-policy** *name*
no authentication-policy

Context config>app-assure>group>transit-ip>radius

Description This command configures the RADIUS authentication-policy for the IP transit policy.

Default no authentication-policy

Parameters *name* — Specifies the authentication policy name, up to 32 characters.

seen-ip-radius-acct-policy

Syntax **seen-ip-radius-acct-policy** *rad-acct-plcy-name*
no seen-ip-radius-acct-policy

Context config>app-assure>group>transit-ip-policy>radius

Description This command refers to a RADIUS accounting-policy to enable seen-IP notification.
The no form of the command removes the policy.

Default no seen-ip-radius-acct-policy

Parameters *rad-acct-plcy-name* — Specifies the RADIUS accounting policy name, up to 32 characters.

static-aa-sub

Syntax **static-aa-sub** *transit-aasub-name*
static-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]

no static-aa-sub *transit-aasub-name*

Context	config>app-assure>group>transit-ip-policy
Description	This command configures static transit aa-sub with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context. The no form of the command deletes the named static transit aa-sub from the configuration.
Parameters	<i>transit-aasub-name</i> — Specifies the name of a transit subscriber up to 32 characters in length. <i>app-profile-name</i> — Specifies the name of an existing application profile up to 32 characters in length. create — Keyword used to create a new app-profile entry.

ip

Syntax	[no] ip <i>ip-address[/mask]</i>
Context	config>app-assure>group>policy>transit-ip-policy>static-aa-sub
Description	This command configures the /32 IP address for a static transit aa-sub. The no form of the command deletes the ip address assigned to the static transit aa-sub from the configuration.
Parameters	<i>ip-address</i> — Specifies the IP address in a.b.c.d form. Values ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d x [0 to FFFF]H d [0 to 255]D prefix-length /32 to /64

sub-ident-policy

Syntax	sub-ident-policy <i>sub-ident-policy-name</i> no sub-ident-policy
Context	config>app-assure>group>transit-ip-policy

Description	This command associates a subscriber identification policy to this SAP. The subscriber identification policy must be defined prior to associating the profile with a SAP in the <code>config>subscribermgmt>sub-ident-policy</code> context. Subscribers are managed by the system through the use of subscriber identification strings. A subscriber identification string uniquely identifies a subscriber. For static hosts, the subscriber identification string is explicitly defined with each static subscriber host. For dynamic hosts, the subscriber identification string must be derived from the DHCP ACK message sent to the subscriber host. The default value for the string is the content of Option 82 CIRCUIT-ID and REMOTE-ID fields interpreted as an octet string. As an option, the DHCP ACK message may be processed by a subscriber identification policy which has the capability to parse the message into an alternative ASCII or octet string value. When multiple hosts on the same port are associated with the same subscriber identification string they are considered to be host members of the same subscriber. A sub-ident-policy can also be used for identifying dynamic transit subscriber names. The no form of the command removes the default subscriber identification policy from the SAP configuration.
Default	no sub-ident-policy
Parameters	<i>sub-ident-policy-name</i> — Specifies the subscriber identification policy name, up to 32 characters.

transit-auto-create

Syntax	transit-auto-create
Context	config>app-assure>group>transit-ip-policy
Description	This command enables seen-IP auto creation of transit subscribers using the transit-IP-policy name and subscriber IP address as the AA-sub name. The default app-profile configured against the transit-ip-policy is applied to these subscribers.

transit-prefix-ipv4-entries

Syntax	transit-prefix-ipv4-entries <i>entries</i> no transit-prefix-ipv4-entries
Context	config>isa>aa-grp
Description	This command defines the number of transit-prefix IPv4 entries for an ISA. The no form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Default	no transit-prefix-ipv4-entries
Parameters	<i>entries</i> — Specifies an integer that determines the number of transit-prefix-ipv4 entries.
Values	0 to 16383

transit-prefix-ipv4-remote-entries

Syntax	transit-prefix-ipv4-remote-entries <i>entries</i> no transit-prefix-ipv4-remote-entries
Context	config>isa>aa-grp
Description	This command configures the ISA-AA-group transit prefix IPv4 remote entry limit. This entry space is allocated on the IOM within a common area with the second MDA/ISA position of the IOM and also used for IPv4filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv4 entries should be set to allow sufficient space on the IOM for SDP IPv4 filters. The no form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.
Default	no transit-prefix-ipv4-remote-entries
Parameters	<i>entries</i> — Specifies the ISA-AA-Group transit prefix IPv4 remote entry limit.
Values	0 to 2047

transit-prefix-ipv6-entries

Syntax	transit-prefix-ipv6-entries <i>entries</i> no transit-prefix-ipv6-entries
Context	config>isa>aa-grp
Description	This command configures the ISA-AA-group transit prefix IPv6 entry limit for each ISA in the group. This entry space is allocated on the IOM within a common area with the second MDA / ISA position of the IOM and also used for ipv6-filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv6 entries should be set to allow sufficient space on the IOM for SDP ipv6-filters. The no form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.
Default	no transit-prefix-ipv6-entries
Parameters	<i>entries</i> — Specifies the ISA-AA-Group transit prefix IPv6 entry limit.
Values	0 to 8191

transit-prefix-ipv6-remote-entries

Syntax	transit-prefix-ipv6-remote-entries <i>entries</i> no transit-prefix-ipv6-remote-entries
Context	config>isa>aa-grp
Description	This command configures the ISA-AA-group transit prefix IPv6 remote entry limit. This entry space is allocated on the IOM within a common area with the second MDA/ISA position of the IOM and also used for IPv6filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv6 entries should be set to allow sufficient space on the IOM for SDP IPv6 filters. The no form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.
Default	no transit-prefix-ipv6-remote-entries
Parameters	<i>entries</i> — Specifies the ISA-AA-Group transit prefix IPv6 remote entry limit.
	Values 0 to 1023

transit-policy

Syntax	transit-policy ip <i>ip-aasub-policy-id</i> transit-policy prefix <i>prefix-aasub-policy-id</i> no transit-policy
Context	config>service>ies>if>sap config>service>ies>if>spoke-sdp config>service>vprn>if>sap config>service>vprn>if>spoke-sdp config>service>epipe>sap config>service>epipe>spoke-sdp config>service>ipipe>sap config>service>ipipe>spoke-sdp config>service>vpls>sap config>service>vpls>spoke-sdp
Description	This command associates a transit AA subscriber IP or prefix policy to the service. The transit policy must be defined prior to associating the policy with a SAP in the config>app-assure>group>transit-ip-policy or transit-prefix-policy context. The no form of the command removes the association of the policy to the service.
Parameters	<i>ip-aasub-policy-id</i> — Specifies a transit IP policy ID.
	Values 1 to 65535

prefix-aasub-policy-id — Specifies a transit prefix policy ID.

Values 1 to 65535

transit-prefix-policy

Syntax	transit-prefix-policy <i>prefix-policy-id</i> [create] no transit-prefix-policy <i>prefix-policy-id</i>
Context	config>app-assure>group
Description	This command defines a transit aa subscriber prefix policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service. The no form of the command deletes the policy from the configuration. All associations must be removed in order to delete a policy.
Parameters	<i>prefix-policy-id</i> — Indicates the transit prefix policy to which this subscriber belongs. Values 1 to 65535 create — Mandatory keyword used when creating transit prefix policy. The create keyword requirement can be enabled/disabled in the environment>create context.

entry

Syntax	entry <i>entry-id</i> [create] entry <i>entry-id</i> no entry <i>entry-id</i>
Context	config>app-assure>group>transit-prefix-policy
Description	This command configures the index to a specific entry of a transit prefix policy. The no form of the command removes the entry ID from the transit prefix policy configuration.
Default	none
Parameters	<i>entry-id</i> — Specifies a transit prefix policy entry. Values 1 to 4294967295 create — Keyword used when creating an entry.

aa-sub

Syntax	aa-sub <i>transit-aasub-name</i>

no aa-sub

Context	config>app-assure>group>transit-prefix-policy>entry
Description	This command configures a transit prefix policy entry subscriber. The no form of the command removes the transit subscriber name from the transit prefix policy configuration.
Default	none
Parameters	<i>transit-aasub-name</i> — specifies the name of the transit prefix AA subscriber up to 32 characters.

match

Syntax	match
Context	config>app-assure>group>transit-prefix-policy>entry
Description	This command enables the context to configure transit prefix policy entry match criteria.

aa-sub-ip

Syntax	aa-sub-ip <i>ip-address[/mask]</i> no aa-sub-ip
Context	config>app-assure>group>transit-prefix-policy>entry>match
Description	This command configures a transit prefix subscriber ip address prefix. It is used when the site is on the local side, being the same side of the system as the parent SAP. The local aa-sub-ip addresses represent the src-IP in the from-SAP direction and dest-IP in the to-SAP direction. The no form of the command deletes the aa-sub-ip address assigned from the entry configuration.
Default	no aa-sub-ip
Parameters	<i>ip-address[/mask]</i> — Specifies the address type of the subscriber address prefix associated with this transit prefix policy entry.

Values

```
ip-address[/mask]:  ipv4-address - a.b.c.d[/mask]
                    mask - [1..32]
                    ipv6-address - x:x:x:x:x:x/x/prefix-length
                    x:x:x:x:x:x.d.d.d.d
                    x - [0..FFFF]H
```

d - [0..255]D
prefix-length [1..128]

network-ip

Syntax	network-ip <i>ip-address[/mask]</i> no network-ip
Context	config>app-assure>group>transit-prefix-policy>entry>match
Description	This command configures an entry for an address of prefix transit aa-sub and is used when the site is a remote site on the same opposite side of the system as the parent SAP. The network IP addresses represents the dest-IP in the from-SAP direction and src-IP in the to-SAP direction. The no form of the command removes the network IP address/mask from the match criteria.
Parameters	<i>ip-address[/mask]</i> — specifies the network address prefix and length associated with this transit prefix policy entry.
Values	<i>ip-address[/mask]</i> : ipv4-address - a.b.c.d[/mask] mask - [1..32] ipv6-address - x:x:x:x:x:x:x/x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D prefix-length [1..128]

static-aa-sub

Syntax	static-aa-sub <i>transit-aasub-name</i> static-aa-sub <i>transit-aasub-name app-profile app-profile-name [create]</i> no static-aa-sub <i>transit-aasub-name</i>
Context	config>app-assure>group>transit-prefix-policy config>app-assure>group>transit-ip-policy>static
Description	This command configures a static transit aa-sub with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context. The no form of the command deletes the named static transit aa-sub from the configuration.

- Parameters**
- transit-aasub-name* — Specifies a transit aasub-name up to 32 characters.
 - app-profile-name* — Specifies the name of an existing application profile up to 32 characters.
 - create** — Keyword used to create a new app-profile entry

static-remote-aa-sub

- Syntax** **static-remote-aa-sub** *transit-aasub-name*
static-remote-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-remote-aa-sub *transit-aasub-name*
- Context** config>app-assure>group>transit-prefix-policy
- Description** This command configures static remote transit aa-sub with a name and an app-profile. Remote transit subscribers are configured for sites on the opposite side of the system as the parent SAP/spoke- SDP. A new remote transit sub with both a name and an app-profile is configured with the create command. Static remote transit aa-sub must have an explicitly assigned app-profile. An existing remote transit sub can optionally be assigned a different app-profile.
- The **no** form of the command removes the name from the transit prefix policy.
- Parameters**
- transit-aasub-name* — Specifies a transit aasub-name up to 32 characters.
 - app-profile-name* — Specifies the name of an existing application profile up to 32 characters.
 - create** — Keyword used to create a new app-profile entry.

sap

- Syntax** **sap** *card/mda/aa-svc:vlan* [**create**]
no sap
- Context** config>service>vprn>aa-if
config>service>ies>aa-if
- Description** This commands specifies which ISA card and which VLAN is used by a given AA Interface.
- Default** no sap
- Parameters**
- card/mda/aa-svc:vlan* — Specifies the AA ISA card slot/port and VLAN information.
 - create** — Keyword used to create the AARP instance.

group

Syntax	group <i>aa-group-id</i>
Context	admin>app-assure
Description	This commands performs a group-specific upgrade.
Parameters	<i>aa-group-id</i> — Specifies the AA group identifier.
Values	1 to 255

url-list

Syntax	url-list <i>url-list-name</i> [create] no url-list <i>url-list-name</i>
Context	config>app-assure>group
Description	This command configures a url-list object. The url-list points to a file containing a list of URLs located on the system Compact Flash. The url-list is then referenced in a url-filter object in order to filter and redirect subscribers when a URL from this file is accessed. The no form of the command removes the url-list object.
Parameters	<i>url-list-name</i> — Specify the Application-Assurance url-list create — Keyword used to create the URL list.

decrypt-key

Syntax	decrypt-key <i>key</i> <i>hash-key</i> <i>hash2-key</i> [hash hash2] no decrypt-key
Context	config>app-assure>group>url-list
Description	In case the file is encrypted this command is used to configure the decryption key used to read the file. The no form of the command removes the url-list object.
Default	no decrypt-key
Parameters	<i>key</i> <i>hash-key</i> <i>hash2-key</i> — Specify the Application-Assurance url-list decryption key hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

file

Syntax	file <i>file-url</i> no file
Context	config>app-assure>group>url-list
Description	This command specifies the file for the URL list. The no form of the command removes the url-list object.
Default	no file
Parameters	<i>file-url</i> — Specifies the flash ID or file path. Values [<i>cflash-id</i>] <i>file-path</i> : [200 chars max] <i>cflash-id</i> : - cf1: cf1-A: cf1-B: cf2: cf2-A: cf2-B: cf3: cf3-A: cf3-B:

size

Syntax	size <i>url-list-size</i>
Context	config>app-assure>group>url-list
Description	This command specifies the size of the URL list that can be filtered. The size can be set to either standard or extended. Configuring the specified url-list as extended provides support for filtering on a larger number of URLs.
Default	size standard
Parameters	<i>url-list-size</i> — Specifies the size of the AA url-list for URL filtering. Values standard, extended

url-filter

Syntax	url-filter <i>url-filter-name</i> [create] no url-filter <i>url-filter-name</i>
Context	config>app-assure>group

Description	This command configures a URL filter action for flows of a specific type matching this entry. If no URL filters are specified then no URL filters will be evaluated.
Parameters	<i>url-filter-name</i> — Specifies the Application-Assurance URL filter that will be evaluated.

default-action

Syntax	default-action allow default-action block-all default-action block-http-redirect <i>http-redirect-name</i> no default-action
Context	config>app-assure>group>policy>aqp>entry>action>url-filter
Description	This command configures the default action to take when the ICAP server is unreachable.
Default	no default-action
Parameters	allow — Allows all requests. block-all — Blocks all requests. block-http-redirect <i>http-redirect-name</i> — Blocks and redirects requests.

http-request-filtering

Syntax	http-request-filtering {all first}
Context	config>app-assure>group>url-filter
Description	HTTP Filtering can either be enabled for all HTTP request within a flow or limited to the first HTTP request in a flow.
Default	http-request-filtering all
Parameters	all — Specifies all HTTP Request within a flow. first — Specifies the first HTTP Request within a flow.

http-redirect

Syntax	http-redirect <i>http-redirect-name</i> no http-redirect
Context	config>app-assure>group>url-filter

Description	This command specifies the HTTP redirect that will be applied when the Internet Content Adaptation Protocol (ICAP) server blocks an HTTP request.
Default	no http-redirect
Parameters	<i>http-redirect-name</i> — Specifies the ICAP HTTP redirect name up to 32 characters.

server

Syntax	server <i>ip-address[:port]</i> [create] no server <i>ip-address[:port]</i>
Context	config>app-assure>group>url-filter>icap
Description	This command configures the IP address and server port of the ICAP server.
Default	none
Parameters	<i>ip-address[:port]</i> — Specifies the ICAP server IP address and port.

vlan-id

Syntax	vlan-id <i>service-port-vlan-id</i> no vlan-id
Context	config>app-assure>group>url-filter>icap
Description	This command configures the VLAN ID on which the ISA-AA is expected to be emitting traffic mapping to a pre-configured aa-interface.
Default	no vlan-id
Parameters	<i>service-port-vlan-id</i> — Specifies the VLAN ID. Values 1 to 4094

custom-x-header

Syntax	custom-x-header <i>x-header-name</i> no custom-x-header
Context	config>app-assure>group>url-filter>icap
Description	This command configures the url-filter ICAP policy to include a new x-header field; the content of the x-header is populated based on AQP url-filter action which can optionally specify the ASO characteristic value to include in the x-header.

Default	no custom-x-header
Parameters	<i>x-header-name</i> — The name of the x-header added to the ICAP request.

local-filtering

Syntax	local-filtering
Context	config>app-assure>group>url-filter
Description	This command configures a URL filter policy for local filtering in order to filter traffic based on a list of URLs located on a file stored in the router compact flash.

url-list

Syntax	[no] url-list <i>url-list-name</i>
Context	admin>app-assure>group>url-filter>local-filtering
Description	This command adds a URL list to the local filtering URL filter policy. The no form of the command removes the URL list object.
Parameters	<i>url-list-name</i> — Specify the URL list.

wap1x

Syntax	wap1x
Context	config>app-assure>group
Description	This command configures the Wireless Application Protocol (WAP) 1.X.

packet-rate-high-wmark

Syntax	packet-rate-high-wmark <i>high-watermark</i> no packet-rate-high-wmark
Context	config>app-assure
Description	This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent. The no version of this command reverts to the default.
Default	packet-rate-high-wmark max

Parameters	<i>high-watermark</i> — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the packet-rate-low-wmark <i>low-watermark</i> value.
Values	1 to 14880952, max packets/sec (disabled)

packet-rate-low-wmark

Syntax	packet-rate-low-wmark <i>low-watermark</i> no packet-rate-low-wmark
Context	config>app-assure
Description	This command configures the packet rate on the ISA-AA when a packet rate alarm will be cleared by the agent. The no form of the command reverts to the default.
Default	packet-rate-low-wmark 0
Parameters	<i>low-watermark</i> — Specifies the low watermark for packet rate alarms. The value must be lower than or equal to the packet-rate-high-wmark <i>high-watermark</i> value.
Values	0 to 14880952 packets per second

protocol

Syntax	protocol <i>protocol-name</i>
Context	config>app-assure
Description	This command configures the shutdown of protocols system-wide.
Parameters	<i>protocol-name</i> — Specifies a shut-able (disable) protocol name.

shutdown

Syntax	[no] shutdown
Context	config>app-assure>protocol
Description	This command administratively disables the protocol specified in protocol <i>protocol-name</i> . The no form of the command enables the protocol.

radius-accounting-policy

Syntax	radius-accounting-policy <i>rad-acct-plcy-name</i> [create] no radius-accounting-policy <i>rad-acct-plcy-name</i>
Context	config>app-assure config>app-assure>group>statistics>aa-sub
Description	This command specifies an existing subscriber RADIUS-based accounting policy to use for AA. RADIUS accounting policies are configured in the config>app-assure>radius-accounting-policy context.
Default	none
Parameters	<i>rad-acct-plcy-name</i> — Specifies the policy name. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces. create — Keyword used to create the policy.

interim-update-interval

Syntax	interim-update-interval <i>minutes</i> no interim-update-interval
Context	config>app-assure>rad-acct-plcy
Description	This command configures the interim update interval. The no form of the command reverts to the default.
Default	no interim-update-interval
Parameters	<i>minutes</i> — Specifies the interval at which subscriber accounting data will be updated. If set no value is specified then no interim updates will be sent. Values 5 to 1080

radius-accounting-server

Syntax	radius-accounting-server
Context	config>app-assure>rad-acct-plcy
Description	This command creates the context for defining RADIUS accounting server attributes under a given session authentication policy.

access-algorithm

Syntax	access-algorithm { direct round-robin }
Context	config>app-assure>rad-acct-plcy>server
Description	This command configures the algorithm used to access the list of configured RADIUS servers.
Default	access-algorithm direct
Parameters	direct — Specifies that the first server will be used as primary server for all requests, the second as secondary and so on. round-robin — Specifies that the first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

retry

Syntax	retry <i>count</i>
Context	config>app-assure>rad-acct-plcy>server
Description	This command configures the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time. The no form of the command reverts to the default value.
Default	retry 3
Parameters	<i>count</i> — Specifies the retry count. Values 1 to 10

router

Syntax	router <i>router-instance</i> router service-name <i>service-name</i> no router
Context	config>app-assure>rad-acct-plcy>server
Description	This command specifies the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time. The no form of the command reverts to the default value.
Default	no router

- Parameters**
- router-instance* — Specifies the router name or service ID used to specify the router instance.
 - service-name* — Specifies the service name to identify the service, up to 64 characters.

server

- Syntax** **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2**] [**port** *port*] [**create**]
no server *server-index*
- Context** config>app-assure>rad-acct-plcy>server
- Description** This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.
- Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.
- The **no** form of the command removes the server from the configuration.
- Parameters**
- server-index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 16 (a maximum of 5 accounting servers)
 - address ip-address* — The IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.
 - secret** *key* — Specifies the secret key value.

Values The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

 - secret-key* — A string up to 20 characters in length.
 - hash-key* — A string up to 33 characters in length.
 - hash2-key* — A string up to 55 characters in length.
 - hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified
 - hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

port — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

source-address

Syntax **source-address** *ip-address*
no source-address

Context config>app-assure>rad-acct-plcy>server

Description This command configures the source address of the RADIUS packet. The system IP address must be configured in order for the RADIUS client to work. See “Configuring a System Interface” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*. The system IP address must only be configured if the source-address is not specified. When the **no source-address** command is executed, the source address is determined at the moment the request is sent. This address is also used in the nas-ip-address attribute: over there it is set to the system IP address if no source address was given.

The **no** form of the command reverts to the default value, where the source address is the system IP address.

Default no source-address

Parameters *ip-address* — The IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

timeout

Syntax **timeout** *seconds*

Context config>app-assure>rad-acct-plcy>server

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of the command reverts to the default value.

Default default 5

Parameters *seconds* — Specifies the time the router waits for a response from a RADIUS server.

Values 1 to 90

significant-change

Syntax	significant-change <i>delta</i> no significant-change
Context	config>app-assure>rad-acct-plcy
Description	This command configures the significant change required to generate the record. The no form of the command reverts to the default.
Default	no significant-change
Parameters	<i>delta</i> — Specifies the delta change (significant change) that is required for the charging-group counts to be included in the RADIUS Accounting VSAs. Values 0 to 4294967295

aa-interface

Syntax	aa-interface <i>aa-if-name</i> [create] no aa-interface <i>aa-if-name</i>
Context	config>service>ies config>service>vprn
Description	This commands creates a new AA interface within an IES or VPRN service. It is used by the aa-isa to send/receive IPv4 traffic. In the context of ICAP url-filtering this interface is used by the ISA to establish ICAP TCP connections to the ICAP servers. This interface supports /31 subnet only, and uses by default .1q encapsulation. The system will automatically configure the ISA IP address based on the address configured by the operator under the aa-interface object (which represents the ISA sap facing interface on the ISA).
Parameters	<i>aa-if-name</i> — specifies the name of the AA Interface. create — Keyword that specifies to create the interface.

address

Syntax	address [<i>ip-address/mask</i> <i>ip-address netmask</i>] no address [<i>ip-address/mask</i> <i>ip-address netmask</i>]
Context	config>service>ies>aa-interface config>service>vprn>aa-interface
Description	This command assigns an IP address to the interface.

Default	no address
Parameters	<i>ip-address/mask</i> — Specifies an IP address/IP subnet format to the interface. <i>ip-address netmask</i> — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains. create — Keyword that specifies to create the interface.

ip-mtu

Syntax	ip-mtu <i>octets</i> no ip-mtu
Context	config>service>ies>aa-interface config>service>vprn>aa-interface
Description	This command configures the AA interface IP MTU.
Default	no ip-mtu
Parameters	<i>octets</i> — Specifies the MTU value. Values 512 to 9000

sap

Syntax	sap <i>sap-id</i> [create] no sap <i>sap-id</i>
Context	config>service>ies>aa-interface config>service>vprn>aa-interface
Description	This command configures the AA interface SAP.
Parameters	<i>sap-id</i> — specifies the physical port identifier portion of the SAP definition. create — creates the SAP instance.

egress

Syntax	egress
Context	config>service>ies>aa-interface>sap config>service>vprn>aa-interface>sap
Description	This command enables the context to configure egress parameters.

ingress

Syntax	ingress
Context	config>service>ies>aa-interface>sap config>service>vprn>aa-interface>sap
Description	This command enables the context to configure ingress parameters.

filter

Syntax	filter ip <i>ip-filter-id</i> no filter [<i>ip ip-filter-id</i>]
Context	config>service>ies>aa-if>sap>egress config>service>vprn>aa-if>sap>egress
Description	This command applies an IP filter to the SAP.
Default	no filter
Parameters	<i>ip-filter-id</i> — Specifies an existing IP filter ID. Values 1 to 65535, or name up to 64 characters maximum

qos

Syntax	qos <i>policy-id</i> no qos [<i>policy-id</i>]
Context	config>service>ies>aa-if>sap>egress config>service>ies>aa-if>sap>ingress config>service>vprn>aa-if>sap>egress config>service>vprn>aa-if>sap>ingress
Description	This command applies an QoS policy to the SAP.
Default	qos 1
Parameters	<i>policy-id</i> — Specifies an existing QoS policy ID.

3.4.2.4.7 System Persistence Commands

persistence

Syntax	persistence
Context	config>system
Description	This command enables the context to configure persistence parameters on the system. The persistence feature enables state on information learned through DHCP snooping across reboots to be retained. This information includes data such as the IP address and MAC binding information, lease-length information, and ingress SAP information (required for VPLS snooping to identify the ingress interface). If persistence is enabled when there are no DHCP relay or snooping commands enabled, it will simply create an empty file.
Default	no persistence

application-assurance

Syntax	application-assurance
Context	config>system>persistence
Description	This command enables the context to configure application assurance persistence parameters.

location

Syntax	location <i>cflash-id</i> no location
Context	config>system>persistence>application-assurance
Description	This command instructs the system where to write the file. The name of the file is: appassure.db. On boot the system scans the file systems looking for appassure.db, if it finds it, it starts to load it. The no form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.
Default	no location

Parameters *cf-flash-id* — Specifies the compact flash type.
Values cf1:, cf2:, cf3:

3.4.2.5 ISA Commands

3.4.2.5.1 Application Assurance Group Commands

application-assurance-group

Syntax **application-assurance-group** *application-assurance-group-index* [**create**] [**aa-sub-scale** *sub-scale*]
 no application-assurance-group *application-assurance-group-index*

Context config>isa

Description This command enables the context to create an application assurance group with the specified system-unique index and enables the context to configure that group's parameters.

 The **no** form of the command deletes the specified application assurance group from the system. The group must be shutdown first.

Default none

Parameters *application-assurance-group-index* — Specifies an integer to identify the AA group

Values 1 to 255

create — Mandatory keyword used when creating an application assurance group in the ISA context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

sub-scale — Specifies the set of scaling limits that are supported with regards to the maximum number of AA subscribers per ISA and the corresponding policies that can be specified.

Values

residential:	Scaling limits for residential operation.
vpn:	Scaling limits for VPNs.
mobile-gateway:	Scaling limits for Mobile Gateway.
lightweight-internet	Scaling limits for operation as a wireless LAN gateway using DSM subscribers.

Default residential

backup

Syntax	[no] backup <i>mda-id</i>						
Context	config>isa>aa-grp						
Description	This command assigns an AA ISA configured in the specified slot to this application assurance group. The backup module provides the application assurance group with warm redundancy when the primary module in the group is configured. Primary and backup modules have equal operational status and when both module are coming up, the ones that becomes operational first becomes the active module. A module can serve as a backup for multiple AA ISA cards but only one can fail to it at one time. On an activity switch from the primary module, configurations are already on the backup MDA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported. Operator is notified through SNMP events when: • When the AA service goes down (all modules in the group are down) or comes back up (a module in the group becomes active). • When AA redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up). • When an AA activity switch occurred. The no form of the command removes the specified module from the application assurance group.						
Parameters	<i>mda-id</i> — Specifies the card/slot identifying a provisioned module to be used as a backup module.						
Values	<table><tr><td>mda-id:</td><td><i>slot/mda</i></td></tr><tr><td>slot</td><td>1 to 10 depending on chassis model</td></tr><tr><td>mda</td><td>1 to 2</td></tr></table>	mda-id:	<i>slot/mda</i>	slot	1 to 10 depending on chassis model	mda	1 to 2
mda-id:	<i>slot/mda</i>						
slot	1 to 10 depending on chassis model						
mda	1 to 2						

divert-fc

Syntax	[no] divert-fc <i>fc-name</i>
Context	config>isa>aa-grp
Description	This command selects a forwarding class in the system to be diverted to an application assurance engine for this application assurance group. Only traffic to/from subscribers with application assurance enabled is diverted. To divert multiple forwarding classes, the command needs to be executed multiple times specifying each forwarding class to be diverted at a time.

The **no** form of the command stops diverting of the traffic to an application assurance engine for this application assurance group.

Parameters *fc-name* — Creates a class instance of the forwarding class fc-name.

Values be, l2, af, l1, h2, ef, h1, nc

fail-to-open

Syntax [no] fail-to-open

Context config>isa>aa-grp

Description This command configures the mode of operation during an operational failure of this application assurance group when no application assurance engines are available to service traffic. When enabled, all traffic that was to be inspected will be dropped. When disabled, all traffic that was to be inspected will be forwarded without any inspection as if the group was not configured at all.

Default no fail-to-open

http-enrich-maximum

Syntax [no] http-enrich-maximum

Context config>isa>aa-grp

Description This command configures the maximum HTTP enriched packet size.

isa-capacity-cost-high-threshold

Syntax isa-capacity-cost-high-threshold *threshold*
no isa-capacity-cost-high-threshold

Context config>isa>aa-grp

Description This command configures the ISA-AA capacity cost high threshold.

The **no** form of the command reverts the threshold to the default value.

Default isa-capacity-cost-high-threshold 4294967295

Parameters *threshold* — Specifies the capacity cost high threshold for the ISA-AA group.

Values 0 to 4294967295

isa-capacity-cost-low-threshold

Syntax	isa-capacity-cost-low-threshold <i>threshold</i> no isa-capacity-cost-low-threshold
Context	config>isa>aa-grp
Description	This command configures the ISA-AA capacity cost low threshold. The no form of the command reverts the threshold to the default value.
Default	isa-capacity-cost-low-threshold 0
Parameters	<i>threshold</i> — Specifies the capacity cost low threshold for the ISA-AA group. Values 0 to 4294967295

isa-overload-cut-through

Syntax	[no] isa-overload-cut-through
Context	config>isa>aa-grp
Description	This command configures the ISA group to enable cut-through of traffic if an overload event occurs, triggered when the IOM weighted average queues depth exceeds the wa-shared-high-wmark . In this ISA state, packets are cut-through from application analysis but retain subscriber context with default subscriber policy applied. The no form of the command disables cut-through processing on overload.
Default	no isa-overload-cut-through

minimum-isa-generation

Syntax	minimum-isa-generation <i>min-isa-generation</i>
Context	config>isa>aa-grp
Description	This command configures the scale parameters for the ISA group. When <i>min-isa-generation</i> is configured as 1, the group and per-ISA limits are the MS-ISA scale. If there is a mix of ISA 1s and 2s, the <i>min-isa-generation</i> must be left as 1. When min-isa-gen is configured as 2, the per-isa resource limits shown in the show isa application-assurance-group 1 load-balance output will increase to show ISA2 limits.
Default	minimum-isa-generation 1

Parameters	<i>min-isa-generation</i> — Specifies the minimum ISA Generation allowed in this group.
Values	1 – ISA (ISA1) 2 – ISA2

overload-sub-quarantine

Syntax	overload-sub-quarantine
Context	config>isa>aa-grp
Description	This command enables the context for overload subscriber detection for this application assurance group.

shutdown

Syntax	[no] shutdown
Context	config>isa>aa-grp>overload-sub-quarantine
Description	This command disables the overload subscriber detection algorithm in the ISA group for the purpose of quarantining an overloaded subscriber. It is possible to manually quarantine an AA subscriber even when this command is disabled (shutdown). The no form of this command enables the overload subscriber detection algorithm in the ISA group. When enabled, each ISA monitors the traffic on a continuous basis to identify AA subscribers that occupy more than their fair share of ISA resources and need to be quarantined
Default	shutdown

partitions

Syntax	[no] partitions
Context	config>isa>aa-grp
Description	This command enables partitions within an ISA-AA group. When enabled, partitions can be created The no form of the command disables partitions within an ISA-AA group.
Default	no partitions

primary

Syntax	[no] primary mda-id
Context	config>isa>aa-grp
Description	This command assigns an AA ISA module configured in the specified slot to this application assurance group. Primary and backup ISAs have equal operational status and when both ISAs are coming up, the one that becomes operational first becomes the active ISA. On an activity switch from the primary ISA, all configurations are already on the backup ISA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported. Operator is notified through SNMP events when: • When AA service goes down (all ISAs in the group are down) or comes back up (an ISA in the group becomes active) • When AA redundancy fails (one of the ISAs in the group is down) or recovers (the failed MDA comes back up) • When an AA activity switch occurred. The no form of the command removes the specified ISA from the application assurance group.
Parameters	mda-id — Specifies the slot/mda identifying a provisioned AA ISA.
	Values
	mda-id: slot/mda
	slot 1 to 10 depending on chassis model
	mda 1 to 2

qos

Syntax	qos
Context	config>isa>aa-grp
Description	This command enables the context for Quality of Service configuration for this application assurance group.

statistics

Syntax	statistics
Context	config>isa>aa-grp

Description	This command enables the context to configure statistics generation.

performance

Syntax	performance
Context	config>isa>aa-grp>statistics
Description	This command configures the ISA group to enable the aa-performance statistic record. This record contains information on the traffic load and resource consumption for each ISA in the group, to allow tracking of ISA load for long term capacity planning and short term anomalies. The user can configure the accounting policy to be used, and enables the record using the [no] collect-stats command.

egress

Syntax	egress
Context	config>isa>aa-grp>qos
Description	This command enables the context for IOM port-level Quality of Service configuration for this application assurance group in the egress direction (traffic entering an application assurance engine).

from-subscriber

Syntax	from-subscriber
Context	config>isa>aa-grp>qos>egress
Description	This command enables the context for Quality of Service configuration for this application assurance group from-subscriber logical port, traffic entering the system from AA subscribers and entering an application assurance engine.

pool

Syntax	pool [pool-name] no pool
Context	config>isa>aa-grp>qos>egress>from-subscriber config>isa>aa-grp>qos>egress>to-subscriber
Description	This command enables the context to configure an IOM pool as applicable to the specific application assurance group traffic. The user can configure resv-cbs (as percentage) values and slope-policy similarly to other IOM pool commands.

Default	pool default
Parameters	<i>pool-name</i> — Specifies the name of the pool, up to 32 characters.

resv-cbs

Syntax	resv-cbs <i>percent-or-default</i> no resv-cbs
Context	config>isa>aa-grp>qos>egress>from-subscriber>pool config>isa>aa-grp>qos>egress>to-subscriber>pool
Description	This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command. • A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated. • The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting. This command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueueing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The resv-cbs parameter can be changed at any time. If the total pool size is 10 MB and the resv-cbs set to 5, the 'reserved size' is 500 KB. The no form of this command restores the default value.
Default	default (30%)
Parameters	<i>percent-or-default</i> — Specifies the pool buffer size percentage.
Values	0 to 100, default

slope-policy

Syntax	slope-policy <i>slope-policy-name</i> no slope-policy
Context	config>isa>aa-grp>qos>egress>from-subscriber>pool config>isa>aa-grp>qos>egress>to-subscriber>pool

Description	This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The slope policy is defined in the config>qos>slope-policy context.
Parameters	<i>slope-policy-name</i> — The name of the slope policy, up to 32 characters.

port-scheduler-policy

Syntax	port-scheduler-policy <i>port-scheduler-policy-name</i> no port-scheduler-policy
Context	config>isa>aa-grp>qos>egress>from-subscriber config>isa>aa-grp>qos>egress>to-subscriber
Description	This command assigns an existing port scheduler policy as applicable to the specific application assurance group traffic.
Default	no port-scheduler-policy
Parameters	<i>port-scheduler-policy-name</i> — Specifies the name of an existing port scheduler policy.

queue-policy

Syntax	queue-policy <i>network-queue-policy-name</i> no queue-policy
Context	config>isa>aa-grp>qos>egress>from-subscriber config>isa>aa-grp>qos>egress>to-subscriber
Description	This command assigns an IOM network queue policy as applicable to specific application assurance group traffic.
Default	queue-policy default
Parameters	<i>network-queue-policy-name</i> — The name of the network queue policy defined in the system.

wa-shared-high-wmark

Syntax	wa-shared-high-wmark <i>percent</i> no wa-shared-high-wmark
Context	config>isa>aa-grp>qos>egress>from-sub config>isa>aa-grp>qos>egress>to-sub

Description	This command configures the high watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool for each ISA. When a buffer pool is not in the overload state and the wa-shared buffer utilization for an ISA crosses above the high watermark value in the ISA from-subscriber buffer pool enters an overload state and an overload notification is raised. The no version of this command reverts to the default.
Default	wa-shared-high-wmark max
Parameters	<i>percent</i> — Specifies the weighted average shared buffer utilization high watermark. Values 1 to 100, max percent (disabled)

wa-shared-low-wmark

Syntax	wa-shared-low-wmark <i>percent</i> no wa-shared-low-wmark
Context	config>isa>aa-grp>qos>egress>from-sub config>isa>aa-grp>qos>egress>to-sub
Description	This command configures the low watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool. When a buffer pool is in an overloaded state and the wa-shared buffer utilization for an ISA drops below low watermark value ISA from-subscriber buffer pool leaves the overload state and a is sent to indicate the overload state has cleared. The no version of this command reverts to the default.
Default	wa-shared-low-wmark 0
Parameters	<i>percent</i> — Specifies the weighted average shared buffer utilization low watermark Values 0 to 99

shared-resources

Syntax	shared-resources
Context	config>isa>aa-grp
Description	This command enables the context to configure the shared resources pool.

tcp-adv-func

Syntax	tcp-adv-func <i>size</i>

Context	config>isa>aa-grp>shr-res-pool
Description	This command configures the allocation of shared resource pool for TCP advanced functions.
Default	tcp-adv-func 100
Parameters	<i>size</i> — Specifies the allocation of the shared resource pool
Values	0 to 100

to-subscriber

Syntax	to-subscriber
Context	config>isa>aa-grp>qos>egress
Description	This command enables the context for Quality of Service configuration for this application assurance group to-subscriber logical port, traffic destined to AA subscribers and entering an application assurance engine.

ingress

Syntax	ingress
Context	config>card>mda>network>ingress
Description	This command enables the context for MDA-level IOM Quality of Service (QoS) configuration.

3.5 Show, Tools, Clear, and Debug Command Reference

3.5.1 Command Hierarchies

- [Show Commands](#)
- [Tools Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)

3.5.1.1 Show Commands

```

show
  — application-assurance
    — aarp
    — aarp aarpId
    — group aa-group-id[:partition-id]
      — aa-interface isa mda-id
      — aa-sub esm sub-ident-string [snapshot]
      — aa-sub esm-mac esm-mac-name [snapshot]
      — aa-sub sap sap-id [snapshot]
      — aa-sub spoke-sdp sdp-id:vc-id [snapshot]
      — aa-sub transit transit-aasub-name [snapshot]
        — app-group [app-group-name] count [detail]
        — app-group count top granularity [max-count max-count]
        — app-group application [application-name] count [detail]
        — app-group count top granularity [max-count max-count]
        — application [application-name] count [detail]
        — application count top granularity [max-count max-count]
        — charging-group [charging-group-name] count [detail]
        — charging-group count top granularity [max-count max-count]
        — count [detail]
        — policers
        — protocol [protocol-name] count [detail]
        — protocol count top granularity [max-count max-count]
        — summary
        — usage-monitor app-group [app-group-name] count
        — usage-monitor application [application-name] count
        — usage-monitor charging-group [charging-group-name] count
        — usage-monitor count
        — usage-monitor status
    — aa-sub-list [isa mda-id]
    — aa-sub-list policers-exceeded
    — aa-sub-list summary
  
```

- **aa-sub-study** **esm** *sub-ident-string* [snapshot]
- **aa-sub-study** **esm-mac** *esm-mac-name* [snapshot]
- **aa-sub-study** **sap** *sap-id* [snapshot]
- **aa-sub-study** **spoke-sdp** *sdp-id:vc-id* [snapshot]
- **aa-sub-study** **transit** *transit-aasub-name* [snapshot]
 - **application** [*application-name*] **count** [detail]
 - **application** **count top** *granularity* [max-count *max-count*]
 - **protocol** [*protocol-name*] **count** [detail]
 - **protocol** **count top** *granularity* [max-count *max-count*]
- **app-group** *app-group-name* **count** [detail]
- **app-group** **count** [detail]
- **app-group** **count top** *granularity* [max-count *max-count*]
- **application** *application-name* **count** [detail]
- **application** **count** [detail]
- **application** **count top** *granularity* [max-count *max-count*]
- **cflowd**
 - **collector** [detail]
 - **direct-export**
 - **collector** *collector-id*
 - **status**
- **dns-ip-cache** *cache-name* **isa** *mda-id*
- **dns-ip-cache** *cache-name*
- **event-log** *event-log-name* **syslog**
- **gtp**
- **gtp** **gtp-filter** *gtp-filter-name*
- **http-enrich** *enrichment-name*
 - **detail** [*partition*]
 - **field** *field-name*
 - **summary**
- **http-error-redirect** *redirect-name*
- **http-notification** *http-notification-name* [summary]
- **http-redirect** *redirect-name* [detail]
- **partition** **summary**
- **policer**
- **policer** *policer-name* [detail]
- **policer** **summary**
- **policy**
 - **admin**
 - **app-filter** [*entry-id*]
 - **app-group** [*app-group-name*]
 - **app-profile** [*app-prof-name*]
 - **app-profile** *app-prof-name* **associations**
 - **app-qos-policy** [*entry-id*]
 - **app-qos-policy** **non-zero**
 - **app-service-option** [*characteristic-name*]
 - **application** [*app-name*]
 - **charging-group**
 - **charging-group** *charging-group-name*
 - **custom-protocol**
 - **summary**
- **protocol** *protocol-name* **count** [detail]
- **protocol** **count** [detail]
- **protocol** **count top** *granularity* [max-count *max-count*]
- **sctp-filter** *sctp-filter-name*

- **session-filter**
- **session-filter** *session-filter-name*
- **status** [isa mda-id] **cflowd**
- **status** [isa mda-id]
- **status** [isa mda-id] **detail**
- **status** isa mda-id **cpu** [sample-period seconds]
- **status** isa mda-id **overload**
- **status** isa mda-id **qos count**
- **status** isa mda-id **qos pools**
- **tcp-validate** tcp-validate-name [isa mda-id]
- **traffic-type** **detail**
- **traffic-type** **ip-family**
- **traffic-type** **ip-protocol**
- **transit-ip-policy** ip-policy-id
- **transit-ip-policy** ip-policy-id **summary**
- **transit-ip-policy** **summary**
- **transit-prefix-policy** transit-prefix-policy-id
- **transit-prefix-policy** **summary**
- **transit-prefix-policy** transit-prefix-policy-id **summary**
- **url-filter** [url-filter-name]
- **url-filter** url-filter-name isa mda-id [detail]
- **url-list** url-list-name
- **http-enrich**
 - **field** field-name
 - **fields**
- **http-error-redirect**
 - **error-codes**
 - **template**
- **http-notification**
 - **template**
- **http-redirect**
 - **template**
- **protocol** [protocol-name]
- **protocol** [protocol-name] **detail**
- **radius-accounting-policy** [rad-acct-plcy-name]
- **radius-accounting-policy** rad-acct-plcy-name **associations**
- **radius-accounting-policy** rad-acct-plcy-name **statistics**
- **threshold-crossing-alert** [detail]
- **version**
- **debug** [application]
- **isa**
 - **application-assurance-group** [aa-group-id [load-balance [unassigned]]]
- **mda** slot [lmda] [detail]
- **service**
 - **aa-sub-using**
 - **aa-sub-using** **app-profile** app-profile-name
 - **sap-using** **aarp** aarp-id
 - **sap-using** **app-profile** app-profile-name
 - **sap-using** **transit-policy** **ip** transit-ip-policy
 - **sap-using** **transit-policy** **prefix** transit-prefix-policy
 - **sdp-using** **aarp** aarp-id
 - **sdp-using** **app-profile** app-profile-name
 - **sdp-using** **transit-policy** **ip** transit-ip-policy
 - **sdp-using** **transit-policy** **prefix** transit-prefix-policy

- **subscriber-using app-profile** *app-profile-name*

3.5.1.2 Tools Commands

- ```
tools
 — dump
 — application-assurance
 — aarp aarpld event-history [clear]
 — group aa-group-id resources
 — aa-anl-list [congested-only] [sort-type {top-by-subs | top-by-rate}
 [isa mda-id]
 — aa-anl-list summary
 — aa-sub dsm mac mac-address [snapshot]
 — aa-sub esm-mac esm-mac-name
 — aa-sub esm sub-ident-string
 — aa-sub transit transit-aasub-name
 — aa-sub-list [filter-by-type sub-type] [isa mda-id] quarantined-only
 — aa-sub-list [filter-by-type sub-type] [isa mda-id] policers-exceeded
 — aa-sub-list summary
 — aa-sub-search search-type granularity [direction direction] [max-
 count max-count]
 — policer policer-name day day time time-of-day
 — group aa-group-id [:partition-id]
 — admit-deny-stats
 — dns-ip-cache cache-name url file-url
 — dns-ip-cache cache-name isa mda-id [url file-url]
 — event-log log-event url file-url
 — event-log log-event isa mda-id [url file-url]
 — flow-record-search aa-sub {esm sub-ident-string | sap sap-id | spoke-
 sdp sdp-id:vc-id | transit transit-aasub-name | mobile {imsi imsi-
 msisdn | msisdn imsi-msisdn | imei imei} apn apn-name | dsm mac
 mac-address | esm-mac esm-mac-name} [protocol protocol-name]
 [application app-name] [app-group app-group-name] [flow-status
 flow-status] [start-flowid start-flowid] [classified classified] [server-
 ip ip-address] [server-port port-num] [client-ip ip-address] [bytes-
 tx kbytes] [flow-duration minutes] [max-count max-count] [search-
 type search-type] [url file-url]
 — flow-record-search isa mda-id [protocol protocol-name] [application
 app-name] [app-group app-group-name] [flow-status flow-
 status] [start-flowid start-flowid] [classified classified] [server-ip ip-
 address] [server-port port-num] [client-ip ip-address] [bytes-tx
 kbytes] [flow-duration minutes] [max-count max-count] [search-
 type search-type] [url file-url]
 — http-host-recorder detail detail [isa mda-id] url file-url
 — http-host-recorder status status [isa mda-id]
 — http-host-recorder top granularity [max-count max-count] [isa mda-
 id]
 — port-recorder detail [flow-count flow-count] [byte-count kbytes] [isa
 mda-id] url file-url
 — port-recorder status [isa mda-id]
 — port-recorder top granularity [max-count max-count] [isa mda-id]
```

- **traffic-capture** detail url *file-url*
- **traffic-capture** status
- **seen-ip** transit-ip-policy *ip-policy-id*
- **seen-ip** transit-ip-policy *ip-policy-id* clear

tools

- perform
  - application-assurance
    - **aarp** aarpId force-evaluate
    - **group** aa-group-id load-balance [**service** service-id]
      - **aa-sub** esm sub-ident-string
      - **aa-sub** esm-mac esm-mac-name
      - **aa-sub** sap sap-id
      - **aa-sub** spoke-sdp sdp-id:vc-id
      - **aa-sub** transit transit-aasub-name
        - **clear-quarantine**
        - **quarantine**

### 3.5.1.3 Clear Commands

clear

- application-assurance
  - **group** aa-group-id cflowd
  - **group** aa-group-id event-log event-log
  - **group** aa-group-id statistics
  - **group** aa-group-id status
  - **group** aa-group-id[:partition] gtp
  - **radius-accounting-policy** rad-acct-plcy-name [**server** server-index] statistics

### 3.5.1.4 Debug Commands

debug

- application-assurance
  - **group** aa-group-id[:partition-id]
    - [no] **http-host-recorder**
      - [no] **filter**
        - **default-filter-action** default-action
        - **expression** expr-index expr-type eq expr-string {record | no-record}
        - no **expression** expr-index
        - **record** {all-hosts | http-host-app-filter-candidates}
      - **rate** sample-rate
      - no **rate**
      - [no] **shutdown**
    - [no] **port-recorder**
      - [no] **application** application-name
      - **rate** sample-rate
      - no **rate**

---

```

 — [no] shutdown
 — [no] traffic-capture
 — [no] match
 — application {eq | neq} application-name
 — no application
 — client-ip {eq | neq} ip-address
 — no client-ip
 — client-port {eq | neq} port-num
 — no client-port
 — dst-ip {eq | neq} ip-address
 — no dst-ip
 — dst-port {eq | neq} port-num
 — no dst-port
 — ip-addr1 {eq | neq} ip-address
 — no ip-addr1
 — ip-addr2 {eq | neq} ip-address
 — no ip-addr2
 — ip-protocol-num {eq | neq} protocol-id
 — no ip-protocol-num
 — port1 {eq | neq} port-num
 — no port1
 — port2 {eq | neq} port-num
 — no port2
 — server-ip {eq | neq} ip-address
 — no server-ip
 — server-port {eq | neq} port-num
 — no server-port
 — src-ip {eq | neq} ip-address
 — no src-ip
 — src-port {eq | neq} port-num
 — no src-port
 — record
 — cut-through-packets cut-through-packets
 — limit {all-packet-matches | first-session-match}
 — start {immediate | on-new-session}
 — [no] shutdown

debug
 — mirror-source service-id
 — isa-aa-group aa-group-id {all | unknown}
 — no isa-aa-group aa-group-id

debug
 — system
 — persistence [persistence-client]
 — no persistence

```

## 3.5.2 Command Descriptions

### 3.5.2.1 Show Commands

#### debug

|                    |                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>debug</b> [ <i>application</i> ]                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | show                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | This command displays the debug points that have been set.                                                                                                                                                                                                                                                                                                                |
| <b>Parameters</b>  | <i>application</i> — Specifies the application debug points that have been set.                                                                                                                                                                                                                                                                                           |
| <b>Values</b>      | aaa, application-assurance, atm, bgp, cisco-hdlc, cmpv2, diameter, ethernet, filter, frame-relay, igmp, ip, ipsec, isis, l2tp, lag, ldp, local-dhcp-server, mcast-management, mirror, mld, mpls, msdp, mtrace, nat, oam, ocsp, open-flow, ospf, ospf3, pim, ppp, radius, radius-proxy, rip, ripng, rsvp, service, snmp, srrp, subscriber-mgmt, system, vrrp, wlan-gw, wpp |

#### application-assurance-group

|                    |                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>application-assurance-group</b> [ <i>aa-group-id</i> [ <b>load-balance</b> [ <b>unassigned</b> ]]]                                                                                             |
| <b>Context</b>     | show>isa                                                                                                                                                                                          |
| <b>Description</b> | This command displays ISA group information.                                                                                                                                                      |
| <b>Parameters</b>  | <i>aa-group-id</i> — Specifies the AA ISA group ID.<br><b>load-balance</b> — Specifies load balancing information.<br><b>unassigned</b> — Specifies load balancing unassigned aa-sub information. |
| <b>Output</b>      | <a href="#">Table 18</a> describes the show command output fields:                                                                                                                                |

**Table 18** Show Application Assurance Group Output Fields

| Label              | Description                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------|
| ISA-AA Group Index | Indicates the group number of this group of MDAs.                                                               |
| Description        |                                                                                                                 |
| Primary ISA-AA     | Displays the primary slot and card number and whether the status is up or down and is either active or standby. |

**Table 18** Show Application Assurance Group Output Fields (Continued)

| Label                         | Description                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup ISA-AA                 | Displays the backup slot and card number and whether the status is up or down and is either active or standby. The status should be up and standby.                                                  |
| Last Active change            | Indicates the last time a successful change was performed.                                                                                                                                           |
| Admin State                   | Displays the administrative state, up or down.                                                                                                                                                       |
| Oper State                    | Displays the operational state, up or down.                                                                                                                                                          |
| Diverted FCs                  | Displays the forwarding class to be diverted.                                                                                                                                                        |
| Fail to mode                  | Displays how traffic is handled when there are no available ISA-AA cards to handle the traffic, either failToWire or failToOpen.                                                                     |
| Partitions                    | Indicates whether partitions are enabled or <b>disabled</b> within an ISA-AA group. When the value of this object is set to <b>enabled</b> , partitions can be created in the tmnxBsxAaGrpPartTable. |
| Egress <b>from</b> subscriber |                                                                                                                                                                                                      |
| Pool                          | Displays the buffer pool as defined in TIMETRA-PORT-MIB::tmnxObjectAppPool for subscriber to network traffic egressing towards the ISA-AA MDA.                                                       |
| Reserved Cbs                  | Displays the percentage of the buffer pool reserved for high priority traffic for subscriber to network traffic egressing towards the ISA-AA MDA.                                                    |
| Slope Policy                  | Displays the policy as defined in TIMETRA-QOS-MIB::tSlopePolicyTable for subscriber to network traffic egressing towards the ISA-AA MDA.                                                             |
| Queue Policy                  | Displays the policy as defined in TIMETRA-QOS-MIB::tNetworkQueueTable for subscriber to network traffic egressing towards the ISA-AA MDA.                                                            |
| Scheduler Policy              | Displays the policy as defined in TIMETRA-QOS-MIB::tSlopePolicyTable for network to subscriber traffic egressing towards the ISA-AA MDA                                                              |
| Egress <b>to</b> subscriber   |                                                                                                                                                                                                      |
| Pool                          | Displays the buffer pool as defined in TIMETRA-PORT-MIB::tmnxObjectAppPool for network to subscriber traffic egressing towards the ISA-AA MDA.                                                       |
| Reserved Cbs                  | Displays the percentage of the buffer pool reserved for high priority traffic for network to subscriber traffic egressing towards the ISA-AA MDA.                                                    |



**Table 18 Show Application Assurance Group Output Fields (Continued)**

| Label                   | Description                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Slope Policy            | Displays the policy as defined in TIMETRA-QOS-MIB::tSlopePolicyTable for network to subscriber traffic egressing towards the ISA-AA MDA.     |
| Queue Policy            | Displays the policy as defined in TIMETRA-QOS-MIB::tNetworkQueueTable for network to subscriber traffic egressing towards the ISA-AA MDA.    |
| Scheduler Policy        | Displays the policy as defined in TIMETRA-QOS-MIB::tSchedulerPolicyTable for network to subscriber traffic egressing towards the ISA-AA MDA. |
| Overload Sub-quarantine | Displays the overload quarantine state, up or down.                                                                                          |
| Overload Cut Through    | Displays the overload cut through state, enabled or disabled.                                                                                |

### Sample Output

```
*A:Dut-A# show isa application-assurance-group 1
=====
ISA Application-assurance-groups
=====
ISA-AA Group Index : 1
Description : (Not Specified)
Subscriber Scale : residential
WLAN GW Group Index : N/A
Primary ISA-AA : 5/1 up/active
Backup ISA-AA : none
Minimum ISA Generation : 2
Last Active change : 04/06/2018 10:18:50
Admin State : Up
Oper State : Up
Diverted FCs : be 12
Fail to mode : fail-to-wire
Partitions : disabled
QoS
 Egress from subscriber
 Pool : default
 Reserved Cbs : default
 Slope Policy : aa_spoll
 Queue Policy : aa_nqpolEgr
 Scheduler Policy : aa_pspFrmSub
 Egress to subscriber
 Pool : default
 Reserved Cbs : default
 Slope Policy : aa_spoll
 Queue Policy : aa_nqpolEgr
 Scheduler Policy : aa_pspToSub
Capacity Cost
 High Threshold : 4294967295
 Low Threshold : 0
```

```

Overload Sub-quarantine : Down
Overload Cut Through : disabled
Transit Prefix
 Max IPv4 entries : 0
 Max IPv6 entries : 0
 Max IPv6 remote entries : 0
HTTP Enrichment
 Max Packet Size : 1500 octets
Shared Resources
 TCP Advanced Functions : 100%
=====

```

```
A:ALU>show>isa#
```

```
*A:Dut-C>show isa application-assurance-group 1 load-balance
```

```
=====
ISA Application-assurance-group 1
=====
```

```
load-balance status : Complete
isa-capacity-cost-threshold : low 0
 : high 4294967295
=====
```

|           | capacity<br>cost | aa-sub | aa-sub<br>stats | ip<br>addresses | transit-prefix-entries |       |      |       |
|-----------|------------------|--------|-----------------|-----------------|------------------------|-------|------|-------|
|           |                  |        |                 |                 | ipv4                   | v4-rm | ipv6 | v6-rm |
| 1/2       | 4                | 4      | 8               | 3               | 0                      | 0     | 0    | 0     |
| 3/1       | 3                | 3      | 6               | 1               | 0                      | 0     | 0    | 0     |
| Mda Limit | n/a              | 1024   | 32768           | 16384           | 0                      | 0     | 0    | 0     |

```
=====
aa-sub type count for group 1
=====
```

|               | all | esm | esm-mac | sap | spoke-sdp transit |       |
|---------------|-----|-----|---------|-----|-------------------|-------|
| 1/2           | 4   | 1   | 3       | 0   | 0                 | 0     |
| 3/1           | 3   | 2   | 1       | 0   | 0                 | 0     |
| Unassigned(*) | 0   | 0   | 0       | 0   | 0                 | n/a** |

```

(*) Subscribers are not initially load balanced until configuration and
persistence files have been processed.
(**) For unassigned transits, refer to unassigned subscriber load-balance
screen for details.
=====

```

```
Last tools load-balance complete reason:
```

```

Tool never performed or last performed on another AA group
Subs moved : 0
Next sub : n/a
Service Id : n/a
=====

```

```
*A:Dut-C# show isa application-assurance-group 84 load-balance unassigned
```

```
=====
ISA Application-assurance-group 84 unassigned
=====
```

| type | SvcId | aa-sub     | App-Profile |
|------|-------|------------|-------------|
| esm  | 2     | Sub1       | Cost30      |
| esm  | 50    | Sub2       | Cost31      |
| sap  | 29    | 2/1/10:527 | Cost29      |

|         |     |                   |        |
|---------|-----|-------------------|--------|
| sap     | 30  | 2/1/10:528        | Cost29 |
| sap     | 31  | 2/1/10:529        | Cost29 |
| sap     | 31  | 2/1/10:530        | Cost29 |
| sap     | 31  | 2/1/10:531        | Cost29 |
| sap     | 32  | 2/1/10:546        | Cost29 |
| sap     | 32  | 2/1/10:547        | Cost29 |
| sap     | 33  | 2/1/10:548        | Cost29 |
| spoke   | 201 | 199:10            | Cost27 |
| spoke   | 202 | 199:17            | Cost10 |
| spoke   | 202 | 199:18            | Cost10 |
| spoke   | 202 | 199:19            | Cost10 |
| esm-mac | 100 | Sub3-000102030405 | Cost30 |

=====

\*A:Dut-C#

## aarp

|                    |                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>aarp</b><br><b>aarp <i>aarpld</i></b>                                                                                                                   |
| <b>Context</b>     | show>app-assur                                                                                                                                             |
| <b>Description</b> | This command displays the Application Assurance Redundancy Protocol (AARP) instance status.                                                                |
| <b>Parameters</b>  | <b><i>aarpld</i></b> — Specifies an integer that identifies an AARP instance<br><b>Values</b> 1 to 65535<br><b>detail</b> — Displays detailed information. |

## group

|                    |                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>group <i>aa-group-id</i> [:<i>partition-id</i>]</b>                                                                                                                         |
| <b>Context</b>     | show>app-assure                                                                                                                                                                |
| <b>Description</b> | This command enables the context to display application-assurance group information.                                                                                           |
| <b>Parameters</b>  | <b><i>aa-group-id</i></b> — Specifies an AA ISA group ID.<br><b>Values</b> 1<br><b><i>partition-id</i></b> — Specifies a partition within a group.<br><b>Values</b> 1 to 65535 |

## aa-interface

**Syntax** **aa-interface isa *mda-id***

|                    |                                                 |          |                                   |
|--------------------|-------------------------------------------------|----------|-----------------------------------|
| <b>Context</b>     | show>app-assure>group                           |          |                                   |
| <b>Description</b> | This command displays AA interface information. |          |                                   |
| <b>Parameters</b>  | <i>mda-id</i> — Specifies the MDA ID.           |          |                                   |
|                    | <b>Values</b>                                   | <mda-id> | <slot>/<mda>                      |
|                    |                                                 | slot     | [1 to 10] (depending on platform) |
|                    |                                                 | mda      | [1 to 2]                          |

## aa-sub

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |  |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| <b>Syntax</b>      | <b>aa-sub esm</b> <i>sub-ident-string</i> [ <b>snapshot</b> ]<br><b>aa-sub esm-mac</b> <i>esm-mac-name</i> [ <b>snapshot</b> ]<br><b>aa-sub sap</b> <i>sap-id</i><br><b>aa-sub spoke-id</b> <i>sdp-id:vc-id</i> [ <b>snapshot</b> ]<br><b>aa-sub transit</b> <i>transit-aasub-name</i> [ <b>snapshot</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |  |
| <b>Context</b>     | show>app-assure>group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |  |
| <b>Description</b> | This command displays per-subscriber statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |  |
| <b>Parameters</b>  | <b>esm</b> <i>sub-ident-string</i> — Specifies an existing subscriber identification string.<br><b>esm-mac</b> <i>esm-mac-name</i> — Specifies an existing subscriber MAC.<br><b>sap</b> <i>sap-id</i> — Specifies the physical port identifier portion of the SAP definition.<br><b>spoke-id</b> <i>sdp-id:vc-id</i> — Specifies the spoke SDP ID and VC ID.<br><b>Values</b> 1 to 17407<br>1 to 4294967295<br><b>snapshot</b> — Specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.<br><b>transit</b> <i>transit-aasub-name</i> — Specifies an existing transit subscriber name string up to 32 characters in length. |  |  |
| <b>Output</b>      | The following is an example of show output for the <b>aa-sub</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |  |

### Sample Output

```
*A:Dut-C# show application-assurance group 1 aa-sub spoke-sdp 1:1 snapshot applicati
on count
=====
Application-Assurance Subscriber 1:1 (spoke-sdp)
Application Statistics (snapshot)
=====
```

```

Application Disc Octets Packets Flows

Unknown 0% 0 0 0
=====
*A:Dut-C#

show application-assurance group 1 aa-sub {esm <sub-ident-string> | esm-mac <esm-
mac-name> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> } summary
=====
Application-Assurance Subscriber summary (realtime | snapshot)
=====
AA-Subscriber : <sub-ident-string> or <sap-id> or <sdp-id:vc-id>
ISA assigned : <Slot/MDA> Unassigned
App-Profile : <app-profile-name>
App-Profile divert : Yes or No
capacity-cost : 100 // for sap/spoke-sdp & esm aa-sub)
Traffic Octets Packets Flows

Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber:
Total flow duration: 0 seconds
Terminated flows:
Short Duration flows:
Medium Duration flows:
Long Duration flows:

Top App-Groups Octets Packets Flows

<app-group-name> 100000 3000 30
<app-group-name> 90000 3000 30
<app-group-name> 80000 3000 30
=====
Application Service Options (ASO)
=====
Characteristic Value Derived from

Server Block default
ServiceBw SuperUser app-profile
Teleworker Yes override
VideoBoost Priority override

Total characteristics : 4
Total derived from aso defaults : 1
Total derived from app-profile : 1
Total derived from overrides : 2
=====

A:ALA-IPD# show application-assurance group 1 aa-sub {esm <sub-ident-string>
| esm-mac <esm-mac-name> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit
<transit-aasub-name>} summary
=====
Application-Assurance Subscriber summary (realtime | snapshot)
=====

```

```

AA-Subscriber : 1:1 (spoke-sdp)
ISA assigned : 3/1
App-Profile : app_prof_D_4
App-Profile divert : Yes
Capacity cost : 1

```

```

Traffic Octets Packets Flows

Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber:
Total flow duration: 0 seconds
Terminated flows:
Short Duration flows:
Medium Duration flows:
Long Duration flows:

```

```

Top App-Groups Octets Packets Flows

<app-group-name> 100000 3000 30
<app-group-name> 90000 3000 30
<app-group-name> 80000 3000 30
=====

```

A:ALA-IPD#

A:ALA-IPD# show application-assurance group 1 aa-sub transit <transit-aasub-name>  
summary

=====

Application-Assurance Subscriber summary (realtime | snapshot)

=====

```

AA-Subscriber : <transit-aasub-name>
App-Profile : <app-profile-name>

```

```

aa-filter : aa-ip <aa-ip-filter-id> or aa-prefix <aa-prefix-filter-id>
 Parent : SAP <sap-id> or Spoke-SDP <id> or N/A
 Parent ISA assigned : <Slot/MDA> or <None (fail-to-closed | fail-to-open)> or
Unassigned or N/A
 Parent app-profile : <app-profile-name> or N/A
 Parent divert : Yes or No or N/A
 Parent capacity-cost : 2000 or N/A

```

```

Traffic Octets Packets Flows

Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber:
Total flow duration: 0 seconds
Terminated flows:
Short Duration flows:
Medium Duration flows:
Long Duration flows:

```

```

Top App-Groups Octets Packets Flows

```

```

<app-group-name> 100000 3000 30
<app-group-name> 90000 3000 30
<app-group-name> 80000 3000 30
=====
A:ALA-IPD#
show application-assurance group 1 aa-sub {esm <sub-ident-string> | esm-mac <esm-
mac-name> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-aasub-
name>} count

A:ALA-IPD# show application-assurance group 1 aa-sub {esm <sub-ident-string> | esm-
mac <esm-mac-name> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-
aasub-name>} snapshot
count
=====
Application-Assurance Subscriber esm|sap|spoke-sdp|transit <name>
Application Group, Application and Protocol Statistics (realtime | snapshot)
=====
Application Group Disc Octets Packets Flows

Games 0% 0 0 0
Mail 0% 0 0 0
Peer to Peer 0% 0 0 0
Unknown 0% 0 0 0
Web 0% 0 0 0
=====
Application Disc Octets Packets Flows

SIP 0% 0 0 0

Protocol statistics are not configured in statistics>aa-sub
=====
A:ALA-IPD#

A:ALA-IPD# show application-assurance group 1 aa-sub {esm <sub-ident-string> | esm-
mac <esm-mac-name> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-
aasub-name>}
application count detail
=====
Application-Assurance Subscriber esm|esm-mac|sap|spoke-sdp|transit <name>
Application Statistics (realtime | snapshot)
=====
Subscriber Application:
Type Octets Packets Flows

name
Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber:
Max per min from sub: 1000 10
Max per min to sub: 2000 20
Total flow duration: 0 seconds
Terminated flows:
Short Duration flows:
Medium Duration flows:

```

```

Long Duration flows: 0
=====
A:ALA-IPD#

```

## aa-sub-list

- Syntax** **aa-sub-list** [*isa mda-id*]  
**aa-sub-list policers-exceeded**  
**aa-sub-list summary**
- Context** show>app-assure>group
- Description** This command displays AA subscriber lists.
- Parameters** **isa mda-id** — Displays the slot and MDA ID.  
**Values** 1 to 10 (depending on chassis model)  
1, 2  
**policers-exceeded** — Displays the policer resources which are exceeded.  
**summary** — Displays summary information.
- Output** The following is an example show output for the **aa-sub-list** command.

### Sample Output

```

*A:Dut-C# show application-assurance group 74:40346 aa-sub-list summary
=====
Application-Assurance Subscriber Summary for Group 74:40346
=====

```

|           | all | esm | sap | spoke-sdp | transit | esm-mac |
|-----------|-----|-----|-----|-----------|---------|---------|
| Total     | 100 | 0   | 0   | 0         | 0       | 100     |
| Overrides | 100 | 0   | 0   | 0         | 0       | 100     |

```

Total number of aa-subs found : 100
Total number of aa-subs with overrides found : 100
=====

*A:Dut-C# show application-assurance group 224:10559 aa-sub-list
=====
Application-Assurance Subscriber List for Group 224:10559
=====

```

| type | aa-sub    | ISA<br>assigned | App-Profile      | divert |
|------|-----------|-----------------|------------------|--------|
| sap  | 1/1/1:113 | 3/2             | prof_224_10559_1 | Yes    |
| sap  | 1/1/1:241 | 3/2             | prof_224_10559_1 | Yes    |
| sap  | 1/1/1:369 | 3/2             | prof_224_10559_1 | Yes    |
| sap  | 1/1/1:497 | 3/2             | prof_224_10559_1 | Yes    |
| sap  | 1/1/4:113 | 3/2             | prof_224_10559_2 | Yes    |
| sap  | 1/1/4:241 | 3/2             | prof_224_10559_2 | Yes    |
| sap  | 1/1/4:369 | 3/2             | prof_224_10559_2 | Yes    |



```

sap 1/1/4:497 3/2 prof_224_10559_2 Yes

Total number of aa-sub found : 8
=====
*A:Dut-C#

*A:Dut-C# show application-assurance group 224:10559 aa-sub-list isa 3/2
=====
Application-Assurance Subscriber List for Group 224:10559, isa 3/2
=====
type aa-sub ISA App-Profile divert
 assigned

sap 1/1/1:113 3/2 prof_224_10559_1 Yes
sap 1/1/1:241 3/2 prof_224_10559_1 Yes
sap 1/1/1:369 3/2 prof_224_10559_1 Yes
sap 1/1/1:497 3/2 prof_224_10559_1 Yes
sap 1/1/4:113 3/2 prof_224_10559_2 Yes
sap 1/1/4:241 3/2 prof_224_10559_2 Yes
sap 1/1/4:369 3/2 prof_224_10559_2 Yes
sap 1/1/4:497 3/2 prof_224_10559_2 Yes

Total number of aa-sub found : 8
=====
*A:Dut-C#

A:ALA-IPD# show application-assurance group 2 aa-sub-list [isa <mda-id>]
=====
Application-Assurance Subscriber List for Group 2, isa <slot/mda>
=====
type aa-sub ISA App-Profile divert
 assigned

group 2:50

esm Bob 3/1 Grp2P50appProf1 Yes
esm Fred 1/1 Grp2P50appProf2 Yes
sap 1/2/9 3/1 Grp2P50appProf1 Yes
sap 1/2/10 1/1 Grp2P50appProf2 Yes
spoke-sdp 1:7 1/1 Grp2P50appProf1 Yes
spoke-sdp 2:101 3/1 Grp2P50appProf2 Yes
esm-mac Sub3-000102030405 1/1 Grp2P50appProf2 Yes

group 2:32656

esm Alex 1/1 appProf1 Yes
esm Sub1 3/1 Lite Yes
esm Max 3/1 appProf1 Yes
esm tcpr_sub 1/1 appProf2 Yes
sap 1/2/5 3/1 appProf1 Yes
sap 1/2/6 1/1 appProf1 Yes
sap 2/2/4:111 1/1 Power Yes
spoke-sdp 1:6 1/1 appProf1 Yes
spoke-sdp 2:100 3/1 appProf2 Yes
esm-mac Sub4-000203040506 3/1 appProf2 Yes

Number of aa-sub found in group 2:50 : 6
Number of aa-sub found in group 2:32656 : 9
Total number of aa-sub found : 15

```

```

=====
A:ALA-IPD#

A:ALA-IPD# show application-assurance group 2:32656 aa-sub-list [isa <mda-id>
=====
Application-Assurance Subscriber List for Group 2:32656, isa <slot/mda>
=====
type aa-sub ISA App-Profile divert
 assigned

esm Alex 1/1 appProf1 Yes
esm Sub1 3/1 Lite Yes
esm Max 3/1 appProf1 Yes
esm tcpr_sub 1/1 appProf2 Yes
sap 1/2/5 3/1 appProf1 Yes
sap 1/2/6 1/1 appProf1 Yes
sap 2/2/4:111 1/1 Power Yes
spoke-sdp 2:100 1/1 appProf8 Yes
esm-mac diameter_esm-000100000001 3/2 appProf2 Yes
esm-mac diameter_esm-000100000002 3/2 appProf2 Yes

Number of aa-subs : 8
=====
A:ALA-IPD#

*A:Dut-C# show application-assurance group 74 aa-sub-list isa 3/2
=====
Application-Assurance Subscriber List for Group 74, isa 3/2
=====
type aa-sub ISA App-Profile divert
 assigned

group 74:40346

esm-mac diameter_esm-000100000001 3/2 appProf2 Yes
esm-mac diameter_esm-000100000002 3/2 appProf2 Yes

```

## aa-sub-study

**Syntax**

```

aa-sub-study esm sub-ident-string [snapshot]
aa-sub-study esm-mac esm-mac-name [snapshot]
aa-sub-study sap sap-id [snapshot]
aa-sub-study spoke-sdp sdp-id:vc-id [snapshot]
aa-sub-study transit transit-aasub-name [snapshot]

```

**Context** show>app-assure>group

**Description** This command displays per-subscriber special study statistics.

**Parameters**

- esm** *sub-ident-string* — Specifies an existing subscriber identification string.
- esm-mac** *esm-mac-name* — Specifies an existing subscriber MAC.
- sap** *sap-id* — Specifies the physical port identifier portion of the SAP definition.

*spoke-id sdp-id:vc-id* — Specifies the spoke SDP ID and VC ID.

**Values** 1 to 17407  
1 to 4294967295

**snapshot** — Specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.

**transit** *transit-aasub-name* — Specifies an existing transit subscriber name string.

## app-group

|                    |                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>app-group</b> [ <i>app-group-name</i> ] <b>count</b> [ <b>detail</b> ]<br><b>app-group count top granularity</b> [ <b>max-count</b> <i>max-count</i> ]                                                     |
| <b>Context</b>     | show>app-assure>group>aa-sub<br>show>app-assure>group                                                                                                                                                         |
| <b>Description</b> | This command displays per-application-group statistics. System-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.                                  |
| <b>Parameters</b>  | <i>app-group-name</i> — Displays information about the specified application group name.<br><b>count</b> — Displays the counters for the application group.<br><b>detail</b> — Displays detailed information. |
| <b>Output</b>      | The following is an example show output for the <b>app-group</b> command.                                                                                                                                     |

### Sample Output

```
A:ALU>show>app-assure>group# app-group count
=====
App-group Statistics
=====
Application Group Disc Octets Packets Flows

File Transfer 0% 0 0 0
Games 0% 3865532 4952 144
Infrastructure 0% 174524 1217 1177
Instant Messaging 0% 2979117 9930 97
Local Content 0% 10581539 10942 74
Mail 0% 57940 346 24
MultiMedia 0% 76911464 79417 198
NNTP 0% 0 0 0
Peer to Peer 0% 10903442 13901 485
Premium Partner 0% 0 0 0
Remote Connectivity 0% 0 0 0
Server 0% 1097 8 2
Suspect 72% 1012 11 11
Tunneling 0% 19872617 33989 204
Unknown 0% 5243395 27510 2648
Web 0% 82135303 91828 2152
```

```

A:ALU>show>app-assure>group#

A:ALU>show>app-assure>group# app-group "MultiMedia" count detail
=====
App-group "MultiMedia" Statistics
=====
Application Group:
Type Octets Packets Flows

MultiMedia:
Admitted from subscriber: 193605 1797 23
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 4835822 3366 23
Denied to subscriber: 0 0 0
Active flows to subscriber:
Total flow duration: 433 seconds
Terminated flows:
Short Duration flows:
Medium Duration flows:
Long Duration flows:
Active subscribers: 0
=====
A:ALU>show>app-assure>group#
```

application

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>application</b> [ <i>application-name</i> ] <b>count</b> [ <b>detail</b> ]<br><b>application count top</b> <i>granularity</i> [ <b>max-count</b> <i>max-count</i> ]                                                                                                                                                                                                                                                                  |
| Context     | show>app-assure>group>aa-sub<br>show>app-assure>group<br>show>app-assure>group>aa-sub-study                                                                                                                                                                                                                                                                                                                                             |
| Description | <p>This command displays per-application statistics. The system-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.</p> <p>Subscriber statistics are available for special-study subscribers and account for all completed and active flows at the moment of this statistics request.</p>                                                                                     |
| Parameters  | <p><i>application-name</i> — Displays information about the specified application name.</p> <p><b>count</b> — Displays counter information.</p> <p><b>detail</b> — Displays detailed information.</p> <p><b>top</b> — Displays counters sorted by granularity.</p> <p><i>granularity</i> — Displays counters sorted by octets, packets, or floe. This is indicated by granularity.</p> <p><b>Values</b>      octets, packets, flows</p> |

*max-count* — If the value is greater than 0, displays up to the indicated value of statistic rows. If 0, displays all.

**Values** 1 to 4294967295

**Output** The following is an example show output for the **application** command.

### Sample Output

```
A:ALU-ABC>show>app-assure>group# application count
=====
Application Statistics
=====
Application Disc Octets Packets Flows

...
DHT 0% 0 0 0
DNS_53 0% 96781 627 627
DNS_Local 0% 0 0 0
DNS_Server 0% 276 3 3
DNS_Suspect 100% 736 8 8
FTP 0% 0 0 0
...
=====
A:ALU-ABC>show>app-assure>group#
```

```
A:ALU-ABC>show>app-assure>group# application "POP3" count detail
=====
Application "POP3" Statistics
=====
Application:
Type Octets Packets Flows

POP3:
Admitted from subscriber: 14095 149 10
Denied from subscriber: 0 0 0
Active flows from subscriber: 0
Admitted to subscriber: 30707 128 10
Denied to subscriber: 0 0 0
Active flows to subscriber: 0
Total flow duration: 7 seconds
Terminated flows: 20
Active subscribers: 0
A:ALU-ABC>show>app-assure>group#
```

```
A:ALU>show>app-assure>group# application "HTTP_Video" count detail
=====
Application "HTTP_Video" Statistics
=====
Application:
Type Octets Packets Flows

HTTP_Video:
Admitted from subscriber: 369528 5404 36
Denied from subscriber: 0 0 0
Active flows from subscriber: 1
```

```
Admitted to subscriber: 15387734 10629 36
Denied to subscriber: 0 0 0
Active flows to subscriber: 1
Total flow duration: 463 seconds
Terminated flows: 72
Short Duration flows: 66
Medium Duration flows: 6
Long Duration flows: 0
Active subscribers: 1
=====
A:ALU>show>app-assure>group#
```

cflowd

- Syntax** cflowd
- Context** show>app-assure>group
- Description** This command enables the context to display cflowd output.

collector

- Syntax** collector [detail]
- Context** show>app-assure>group>cflowd
- Description** This command enables the context to display cflowd output.
- Parameters** detail — Displays detailed information.
- Output** The following is an example show output for the **collector** command.

Sample Output

```
A:ALU-A# show application-assurance group 1 cflowd collector
=====
Application Assurance Cflowd Collectors for group 1
=====
Host Address Port Version Admin Oper Recs Sent

192.168.7.7 2055 10 up up 0
192.168.7.8 2055 10 up up 0

Collectors : 2

A:ALU-A#

A:ALU-A# show application-assurance group 1 cflowd collector detail
=====
Application Assurance Cflowd Collectors for group 1
=====
Address : 192.168.7.7
```

```

Port : 2055
Description : AA Collector 1
Version : 10
Admin State : up
Oper State : up
Records Sent : 0
Last Changed : 07/27/2009 13:36:50

Address : 192.168.7.8
Port : 2055
Description : AA Collector 2
Version : 10
Admin State : up
Oper State : up
Records Sent : 0
Last Changed : 07/27/2009 13:37:10
=====
A:ALU-A#

```

## direct-export

**Syntax** **direct-export**

**Context** show>app-assure>group>cflowd

**Description** This command enables the context to display cflowd direct-export output.

## collector

**Syntax** **collector** *collector-id*

**Context** show>app-assure>group>cflowd>dir-exp

**Description** This command enables the context to display cflowd direct-export collector output.

**Parameters** *collector-id* — Specifies the ID of the cflowd direct export collector.

**Output** The following is an example show output for the **collector** command.

### Sample Output

```

A:Sim# show application-assurance group 1 cflowd direct-export collector 1
=====
Application Assurance Group 1 Cflowd Direct-Export Collector 1
=====
Collector Status : Inactive
VLAN Id : N/A
Cflowd Version : 10
Admin State : down
Description : (Not Specified)

```

```

Host Address Port Admin Oper Records Sent

192.168.2.1 4739 DOWN DOWN 0
192.168.2.2 4739 down down 0

No. of Cflowd Direct Export Collector Addresses: 2
=====
Application Assurance Group 1 Cflowd Collectors
Collector Status : Active
=====
Address : 192.168.2.1
Port : 4739
Description :
Version : 10
Admin State : down
Oper State : down
Records Sent : 5400
Last Changed : 08/12/2015 19:12:28
Address : 192.168.2.2
Port : 4739
Description :
Version : 10
Admin State : down
Oper State : down
Records Sent : 5400
Last Changed : 08/12/2015 19:12:35
=====
status [isa <slot/mda>] cflowd

```

## status

- Syntax**     **status**
- Context**    show>app-assure>group>cflowd
- Description** This command displays status information.
- Output**     The following is an example show output for the **status** command.

### Sample Output

```

A:ALU-A# show application-assurance group 1 status [isa 1/2] cflowd
=====
Application-Assurance Group Cflowd Status
=====
Cflowd Admin Status : Enabled
Cflowd Oper Status : Enabled

Volume :

Sample Rate : <Disabled> or <1 in 500 packets>
Active Flows : 23102
Records Reported : 12345
Records Dropped : 10
Records Per Second : 45

```



```

Packets Sent : 1763
Packets Sent Per Sec : 7

TCP Performance :

Sample Rate : <Disabled> or <1 in 1000 flows>
Active Flows : 32103
Flows Not Allocated : 33
Records Reported : 12345678
Records Dropped : 100
Records Per Second : 456
Packets Sent : 2057613
Packets Sent Per Sec : 76
=====
A:ALU-A#

A:ALU-A#show application-assurance group <aa-group-id:[partition]> cflowd status
=====
Application-Assurance Group:Partition Cflowd Status
=====

Volume :

Admin State : Up
Records Reported : 12345
Records Dropped : 10

TCP Performance :

Admin State : Up
Flows Not Allocated : 33
Records Reported : 12345678
Records Dropped : 100
=====
A:ALU-A#

```

## dns-ip-cache

|                    |                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dns-ip-cache</b> <i>cache-name</i> <i>isa</i> <i>mda-id</i><br><b>dns-ip-cache</b> <i>cache-name</i>                                    |
| <b>Context</b>     | show>app-assure>group                                                                                                                      |
| <b>Description</b> | This command displays the application assurance DNS IP cache statistics and status information.                                            |
| <b>Parameters</b>  | <i>cache-name</i> — Specifies the DNS IP cache for a particular ISA-AA card, up to 32 characters.<br><i>mda-id</i> — Specifies the AA ISA. |
|                    | <b>Values</b> slot 1 to 10, mda 1 to 2                                                                                                     |
| <b>Output</b>      | <a href="#">Table 19</a> describes the <b>show</b> command output fields.                                                                  |

**Table 19** Show DNS IP Cache Output Fields

| Label                   | Description                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Status            | Indicates the administrative status of the DNS IP cache. [Up   Down]                                                                                                                                                       |
| Domain expressions      | Indicates the number of DNS domain expressions configured.                                                                                                                                                                 |
| Server addresses        | Indicates the number of server-addresses configured                                                                                                                                                                        |
| High-Watermark          | Indicates the value, in percentage, of the configured high watermark.                                                                                                                                                      |
| Low-Watermark           | Indicates the value, in percentage, of the configured low watermark.                                                                                                                                                       |
| Cache-size              | Indicates the value of the configured maximum cache size.                                                                                                                                                                  |
| Usage                   | Indicates the value, in percentage, of the total for the number of entries in the cache.                                                                                                                                   |
| Alarm State             | Indicates the status of the alarm related to the DNS IP cache high/low watermark utilization. The alarm is raised when the high watermark is crossed; it is cleared when it goes below the low watermark. [Clear   Raised] |
| Hit-Count               | Indicates the number of times an IP address lookup in this cache was successful.                                                                                                                                           |
| Total responses         | Indicates the total number of DNS responses analyzed.                                                                                                                                                                      |
| Domain name matched     | Indicates the number of times a domain name defined in the DNS match criteria matched a DNS response.                                                                                                                      |
| Domain & server matched | Indicates the number of times both the domain name and server address defined in the DNS match criteria matched a DNS response.                                                                                            |
| Total entries added     | Indicates the total number of IP entries added in the cache.                                                                                                                                                               |
| Total entries removed   | Indicates the total number of IP entries removed from the cache after the entry expired.                                                                                                                                   |
| Full count              | Indicates the total number of IP entries in the cache.                                                                                                                                                                     |
| Hit Count               | Indicates the number of times an IP address lookup in this cache was successful. The IP address lookup is performed in app-filters and is successful if the server address DNS IP cache criteria is met.                   |

**Table 19 Show DNS IP Cache Output Fields (Continued)**

| Label      | Description                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Miss Count | Indicates the number of times an IP address lookup in this cache was unsuccessful. The IP address lookup is performed in app-filters and is unsuccessful if the server address DNS IP cache criteria is not met. |

### Sample Output

```
*A:7750# show application-assurance group 1 dns-ip-cache "Default DNS IP Cache"
=====
Application Assurance Group 1 dns-ip-cache "Default DNS IP Cache"
=====
Admin Status : Up

Domain expressions : 11 (out of 32)
Server addresses : 0 (out of 64)
High watermark : 40%
Low watermark : 35%
Cache size : 5000

ISA Usage (%) Alarm Hit Count
 State

1/2 0 (0.00%) clear 0
3/2 133 (88.66%) raised 18
=====

*A:7750# show application-assurance group 1 dns-ip-
cache "Default DNS IP Cache" isa 3/1
=====
Application Assurance Group 1 dns-ip-cache "Default DNS IP Cache" ISA 3/1
=====
Admin Status : Up

Domain expressions : 11 (out of 32)
Server addresses : 0 (out of 64)
High watermark : 40%
Low watermark : 35%
Cache size : 5000

ISA 3/1 DNS Stats

DNS
 Total responses : 5751
 Domain name matched : 106
 Domain & server matched : 106
Cache
 Total entries added : 118
 Total entries removed : 0
 Usage : 118 (2.36%) threshold alarm clear
 Full count : 0
```

```

Hit count : 274
Miss count : 20379

```

## event-log

|                    |                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>event-log</b> <i>event-log-name</i> <b>syslog</b>                                                                                   |
| <b>Context</b>     | show>app-assure>group                                                                                                                  |
| <b>Description</b> | This command displays event log information.                                                                                           |
| <b>Parameters</b>  | <i>event-log-name</i> — Specifies the event log name, up to 32 characters.<br><b>syslog</b> — Specifies to display syslog information. |
| <b>Output</b>      | The following is a sample output displaying event log information:                                                                     |

### Sample Output

```
*A:Dut-B# show application-assurance group 1:1 event-log "sampleLog" syslog
=====
Application Assurance Group 1:1 Event Log "sampleLog" Syslog
=====
Event-log admin status : down
Description : (Not Specified)
Address : (Not Specified)
Port : 514
VLAN ID : (Not Specified)
Facility : local7
Severity : info

ISA Events Sent Events Failed

1/2 0 0
2/1 0 0
2/2 0 0
=====
*A:Dut-B#
```

## gtp

|                    |                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>gtp</b><br><b>gtp gtp-filter</b> <i>gtp-filter-name</i>                                                                                    |
| <b>Context</b>     | show>app-assure>group                                                                                                                         |
| <b>Description</b> | This command displays GTP (General packet radio service (GPRS) Tunneling Protocol) information.                                               |
| <b>Parameters</b>  | <i>gtp-filter-name</i> — Specifies a GTP filter. When a filter is specified, all traffic is examined as described in the tmnxBsxCtpFltrTable. |

## http-enrich

|                    |                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-enrich</b> <i>enrichment-name</i>                                                       |
| <b>Context</b>     | show>app-assure>group                                                                           |
| <b>Description</b> | This command displays HTTP enrichment information.                                              |
| <b>Parameters</b>  | <i>enrichment-name</i> — Specifies the name of the HTTP enrichment policy, up to 32 characters. |
| <b>Output</b>      | The following is an example output for the <b>http-enrich</b> command.                          |

### Sample Output

```
show application-assurance group 1 http-enrich "MyTemplate"
=====
Application Assurance Group 1 HTTP Enrichment "MyTemplate"
=====
Description : (Not Specified)
Admin Status : Up
AQP Referenced: No

Name Field Enabled
 Sub-ID Features

subscriber-ip MyField M
subscriber-id Sub-ID AC

 A=anti-spoof,C=encode-cert,M=encode-
md5,R=encode-rc4

Group Enriched Not Enriched

1 0 0

Total 0 0

=====
```

## detail

|                    |                                                                                          |
|--------------------|------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>detail</b> [ <i>partition</i> ]                                                       |
| <b>Context</b>     | show>app-assure>group>http-enrich                                                        |
| <b>Description</b> | This command displays detailed HTTP Enrichment information.                              |
| <b>Parameters</b>  | <i>partition</i> — Specifies the partition within the group.<br><b>Values</b> 1 to 65535 |

## field

|                    |                                                                    |
|--------------------|--------------------------------------------------------------------|
| <b>Syntax</b>      | <b>field</b> <i>field-name</i>                                     |
| <b>Context</b>     | show>app-assure>group>http-enrich<br>show>app-assure>http-enrich   |
| <b>Description</b> | This command displays HTTP enrichment field information.           |
| <b>Parameters</b>  | <i>field-name</i> — Specifies the field name, up to 32 characters. |

## fields

|                    |                                               |
|--------------------|-----------------------------------------------|
| <b>Syntax</b>      | <b>fields</b>                                 |
| <b>Context</b>     | show>app-assure>http-enrich                   |
| <b>Description</b> | This command displays HTTP enrichment fields. |

## summary

|                    |                                                               |
|--------------------|---------------------------------------------------------------|
| <b>Syntax</b>      | <b>summary</b>                                                |
| <b>Context</b>     | show>app-assure>group>http-enrich                             |
| <b>Description</b> | This command displays summarized HTTP enrichment information. |

## count

|                    |                                                                                     |
|--------------------|-------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>count</b> [ <b>detail</b> ]                                                      |
| <b>Context</b>     | show>app-assure>group>aa-sub                                                        |
| <b>Description</b> | This command displays per-subscriber app-group application and protocol statistics. |
| <b>Parameters</b>  | <b>detail</b> — Displays detailed information.                                      |
| <b>Output</b>      | The following is an example output for the <b>count</b> command.                    |

### Sample Output

```
A:ALU>show>app-assure>group>aa-sub# count
=====
Application-Assurance Subscriber TestSubscriberName
Application Group, Application and Protocol Statistics
=====
Application Group Disc Octets Packets Flows

```

|                     |               |       |      |
|---------------------|---------------|-------|------|
| Database            | 0% 0          | 0     | 0    |
| File Transfer       | 0% 27243      | 169   | 22   |
| Games               | 0% 0          | 0     | 0    |
| Infrastructure      | 0% 71494      | 555   | 515  |
| Instant Messaging   | 0% 4947792    | 25587 | 411  |
| Local Content       | 0% 923        | 8     | 2    |
| Mail                | 0% 53729      | 318   | 22   |
| Mail Server         | 0% 0          | 0     | 0    |
| MultiMedia          | 0% 31670667   | 33087 | 142  |
| NNTP                | 0% 0          | 0     | 0    |
| Peer to Peer        | .45% 11096224 | 16339 | 2431 |
| Premium Partner     | 0% 0          | 0     | 0    |
| Remote Connectivity | 0% 15321      | 171   | 2    |
| Server              | 0% 0          | 0     | 0    |
| Suspect             | 72% 1012      | 11    | 11   |
| Tunneling           | 0% 19659289   | 33535 | 164  |
| Unknown             | 0% 1945164    | 6317  | 287  |
| Web                 | 0% 29538078   | 34873 | 1022 |
| Web Server          | 0% 0          | 0     | 0    |

| Application | Disc | Octets | Packets | Flows |
|-------------|------|--------|---------|-------|
| HTTP_Local  | 0%   | 923    | 8       | 2     |

| Protocol | Disc | Octets | Packets | Flows |
|----------|------|--------|---------|-------|
| dns      | 1.8% | 40010  | 277     | 277   |

A:ALU>show>app-assure>group>aa-sub#

A:ALU>show>app-assure>group>aa-sub# count detail

Application-Assurance Subscriber TestSubscriberName  
Application Group, Application and Protocol Statistics

| Subscriber                    | Application Group: |         |       |
|-------------------------------|--------------------|---------|-------|
| Type                          | Octets             | Packets | Flows |
| TestSubscriberName            |                    |         |       |
| Instant Messaging:            |                    |         |       |
| Admitted from subscriber:     | 2558576            | 12720   | 229   |
| Denied from subscriber:       | 0                  | 0       | 0     |
| Active flows from subscriber: |                    |         | 0     |
| Admitted to subscriber:       | 2389216            | 12867   | 182   |
| Denied to subscriber:         | 0                  | 0       | 0     |
| Active flows to subscriber:   |                    |         | 0     |
| Total flow duration:          | 2912 seconds       |         |       |
| Terminated flows:             |                    |         | 411   |
| Short Duration flows:         |                    |         | 387   |
| Medium Duration flows:        |                    |         | 22    |
| Long Duration flows:          |                    |         | 2     |
| ...                           |                    |         |       |
| TestSubscriberName            |                    |         |       |
| Web:                          |                    |         |       |
| Admitted from subscriber:     | 2343429            | 22806   | 511   |
| Denied from subscriber:       | 0                  | 0       | 0     |
| Active flows from subscriber: |                    |         | 1     |
| Admitted to subscriber:       | 56359191           | 40528   | 511   |
| Denied to subscriber:         | 0                  | 0       | 0     |
| Active flows to subscriber:   |                    |         | 1     |

```

Total flow duration: 4783 seconds
Terminated flows: 1020
Short Duration flows: 989
Medium Duration flows: 31
Long Duration flows: 0
=====
Subscriber Application:
Type Octets Packets Flows

TestSubscriberName HTTP_Local:
Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber: 0
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber: 0
Total flow duration: 0 seconds
Terminated flows: 0
Short Duration flows: 0
Medium Duration flows: 0
Long Duration flows: 0
=====
Subscriber Protocol:
Type Octets Packets Flows

TestSubscriberName dns:
Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber: 0
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber: 0
Total flow duration: 0 seconds
Terminated flows: 0
Short Duration flows: 0
Medium Duration flows: 0
Long Duration flows: 0
=====
A:ALU>show>app-assure>group>aa-sub#

```

## admin

|                    |                                                                             |
|--------------------|-----------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>admin</b>                                                                |
| <b>Context</b>     | show>app-assure>group>policy                                                |
| <b>Description</b> | This command displays the application-assurance policy uncommitted changes. |
| <b>Output</b>      | The following is an example output for the <b>admin</b> command.            |

### Sample Output

```

*A:ALA-48>show>app-assure>group>policy# admin
begin
app-filter

```



```
entry 10 create
shutdown
exit
exit
app-qos-policy
entry 10 create
shutdown
exit
exit
commit
*A:ALA-48>show>app-assure>group>policy#
```

app-filter

|             |                                                                                        |
|-------------|----------------------------------------------------------------------------------------|
| Syntax      | app-filter [ <i>entry-id</i> ]                                                         |
| Context     | show>app-assure>group>policy                                                           |
| Description | This command displays application-assurance policy filter information.                 |
| Parameters  | <i>entry-id</i> — Specifies an existing application filter entry.<br>Values 1 to 65535 |

app-group

|             |                                                                                     |
|-------------|-------------------------------------------------------------------------------------|
| Syntax      | app-group [ <i>app-group-name</i> ]                                                 |
| Context     | show>app-assure>group>policy                                                        |
| Description | This command displays application-assurance policy application group information.   |
| Parameters  | <i>app-group--name</i> — Specifies the application group name, up to 32 characters. |

app-profile

|             |                                                                                                                                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | app-profile [ <i>app-prof-name</i> ]<br>app-profile <i>app-prof-name</i> associations                                                 |
| Context     | show>app-assure>group>policy                                                                                                          |
| Description | This command displays application-assurance policy application profile information.                                                   |
| Parameters  | <i>app-prof-name</i> — Specifies an existing application profile name.<br>associations — Displays subscriber management associations. |

---

## app-qos-policy

|                    |                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>app-qos-policy</b> [ <i>entry-id</i> ]<br><b>app-qos-policy non-zero</b>                                                                                    |
| <b>Context</b>     | show>app-assure>group>policy                                                                                                                                   |
| <b>Description</b> | This command displays application-assurance policy application QoS policy information.                                                                         |
| <b>Parameters</b>  | <i>entry-id</i> — Specifies an existing application QoS policy entry id.<br><b>Values</b> 1 to 65535<br><b>non-zero</b> — Selects only non-zero count entries. |

## app-service-option

|                    |                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>app-service-option</b> [ <i>characteristic-name</i> ]                                   |
| <b>Context</b>     | show>app-assure>group>policy                                                               |
| <b>Description</b> | This command displays application-assurance policy application service option information. |
| <b>Parameters</b>  | <i>characteristic-name</i> — Specifies the characteristic name, up to 32 characters.       |

## application

|                    |                                                                             |
|--------------------|-----------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>application</b> [ <i>app-name</i> ]                                      |
| <b>Context</b>     | show>app-assure>group>policy                                                |
| <b>Description</b> | This command displays application-assurance policy application information. |
| <b>Parameters</b>  | <i>app-name</i> — Specifies the application name, up to 32 characters.      |

## charging-group

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>charging-group</b><br><b>charging-group</b> <i>charging-group-name</i>         |
| <b>Context</b>     | show>app-assure>group>policy                                                      |
| <b>Description</b> | This command displays application-assurance policy application information.       |
| <b>Parameters</b>  | <i>charging-group-name</i> — Specifies the application name, up to 32 characters. |

## custom-protocol

|                    |                                                                                 |
|--------------------|---------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>custom-protocol</b>                                                          |
| <b>Context</b>     | show>app-assure>group>policy                                                    |
| <b>Description</b> | This command displays application-assurance policy custom protocol information. |

## summary

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>summary</b>                                                          |
| <b>Context</b>     | show>app-assure>group>policy                                            |
| <b>Description</b> | This command displays application-assurance policy summary information. |

## policers

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>policers</b>                                                     |
| <b>Context</b>     | show>app-assure>group>policy>aa-sub                                 |
| <b>Description</b> | This command displays policer configuration information.            |
| <b>Output</b>      | The following is an example output for the <b>policers</b> command. |

### Sample Output

```
A:cpm-a>show>app-assure>group>aa-sub# policers
=====
Application-Assurance Subscriber Policer Summary
=====
AA-Subscriber : Alex (esm)

Type: single-bucket-bandwidth Direction: subscriber-to-network

AQP Policer Resources Exceeded?

61 SuspectUp_policer N

Type: single-bucket-bandwidth Direction: network-to-subscriber

AQP Policer Resources Exceeded?

62 SuspectDown_policer N

Policer usage counts:
single-bucket-bandwidth
 subscriber-to-network 1 out of 32
 network-to-subscriber 1 out of 32
```

```

dual-bucket-bandwidth
 subscriber-to-network 0 out of 1
 network-to-subscriber 0 out of 1
flow-count-limit 0 out of 8
flow-rate-limit 0 out of 8
=====
A:cpm-a>show>app-assure>group>aa-sub#

```

## summary

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>summary</b>                                                          |
| <b>Context</b>     | show>app-assure>group>policy<br>show>app-assure>group>aa-sub            |
| <b>Description</b> | This command displays application-assurance policy summary information. |

## protocol

|                    |                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>protocol</b> [ <i>protocol-name</i> ] <b>count</b> [ <b>detail</b> ]<br><b>protocol count</b> [ <b>detail</b> ]<br><b>protocol count top</b> <i>granularity</i> [ <b>max-count</b> <i>max-count</i> ]                                                                                                                                  |
| <b>Context</b>     | show>app-assure>group>aa-sub<br>show>app-assure>group                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command displays per-protocol statistics. The system-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.<br><br>Subscriber statistics are available for special study subscribers and account for all completed and active flows at the moment of this statistics request. |
| <b>Parameters</b>  | <i>protocol-name</i> — Displays information about the specified protocol name.<br><b>count</b> — Displays protocol counters.<br><b>detail</b> — Displays detailed information.                                                                                                                                                            |
| <b>Output</b>      | The following is an example output for the <b>protocol</b> command.                                                                                                                                                                                                                                                                       |

### Sample Output

```

A:ALU>show>app-assure>group# protocol count
=====
Protocol Statistics
=====
Protocol Disc Octets Packets Flows

aim_oscar 0% 0 0 0
aim_oscar_file_xfer 0% 0 0 0
aim_oscar_video_voice 0% 0 0 0

```

```
aim_toc 0% 0 0 0
bittorrent 0% 0 0 0
...

A:ALU>show>app-assure>group# protocol "http_audio" count detail
=====
Protocol "http_audio" Statistics
=====
 Protocol:
Type Octets Packets Flows

 http_audio:
Admitted from subscriber: 14958 201 2
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 587590 396 2
Denied to subscriber: 0 0 0
Active flows to subscriber:
Total flow duration: 21 seconds
Terminated flows:
Short Duration flows:
Medium Duration flows:
Long Duration flows:
Active subscribers: 1
=====
A:ALU>show>app-assure>group#
```

## sctp-filter

|                    |                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>sctp-filter</b> <i>sctp-filter-name</i>                                                                                                                              |
| <b>Context</b>     | show>app-assure>group                                                                                                                                                   |
| <b>Description</b> | This command displays Stream Control Transmission Protocol (SCTP) filter information                                                                                    |
| <b>Parameters</b>  | <i>sctp-filter-name</i> — Specifies an SCTP filter, up to 256 characters. When a filter is specified, all traffic is examined as described in the tmnxBsxSctpFltrTable. |

## session-filter

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>session-filter</b><br><b>session-filter</b> <i>session-filter-name</i>         |
| <b>Context</b>     | show>app-assure>group                                                             |
| <b>Description</b> | This command displays session filter information.                                 |
| <b>Parameters</b>  | <i>session-filter-name</i> — Specifies a session-filter-name up to 32 characters. |
| <b>Output</b>      | The following is an example show output for the <b>session-filter</b> command.    |

**Sample Output**

```

show application-assurance group <aa-group-id>[:<partition>] session-filter <filter-
name>
session-filter<filter-id>
=====
AA Session Filter
=====
Filter Name : Block UDP Session Initiation
Applied : Yes Def. Action : Permit
Entries : 1
Description : Block UDP initiated towards subscribers

Filter Match Criteria

Entry : 1
Description : (Not Specified)
Protocol : 17
Action : deny
Hit Count : 0 pkts
=====

```

**summary**

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>summary</b>                                                          |
| <b>Context</b>     | show>app-assure>group>aa-sub                                            |
| <b>Description</b> | This command displays a summary of statistics for a specific aa-sub.    |
| <b>Output</b>      | The following is an example show output for the <b>summary</b> command. |

**Sample Output**

```

A:ALU>show>app-assure>group>aa-sub# summary
=====
Application-Assurance Subscriber Summary
=====
AA-Subscriber : TestSubscriberName
ISA assigned : 3/2
App-Profile : Power_Profile
App-Profile divert : Yes
Sub-quarantined : No
Capacity cost : 1

Traffic Octets Packets Flows

Admitted from subscriber: 7092548 52935 2843
Denied from subscriber: 51160 617 374
Active flows from subscriber: 12
Admitted to subscriber: 73705675 73538 1453
Denied to subscriber: 0 0 0
Active flows to subscriber: 12
Total flow duration: 12750 seconds

```

```
Terminated flows: 4646
Short Duration flows: 4516
Medium Duration flows: 130
Long Duration flows: 0

Top App-Groups Octets Packets Flows

MultiMedia 29060053 29961 138
Tunneling 19659289 33535 164
Web 14856331 19829 932
=====
A:ALU>show>app-assure>group>aa-sub#
```

## usage-monitor

- Syntax**     **usage-monitor app-group** [*app-group-name*] **count**  
              **usage-monitor application** [*application-name*] **count**  
              **usage-monitor charging-group** [*charging-group-name*] **count**  
              **usage-monitor count**  
              **usage-monitor status**
- Context**     show>app-assure>group>aa-sub
- Description**   This command displays per-subscriber usage-monitoring statistics.
- Parameters**   *app-group-name* — Specifies an application group name, up to 32 characters.  
                  *application-name* — Specifies an application name, up to 32 characters.  
                  *charging-group-name* — Specifies a charging group name, up to 32 characters.  
                  **count** — Displays counters.  
                  **status** — Displays the status.

## status

- Syntax**     **status** [*isa mda-id*] **cflowd**  
              **status** [*isa mda-id*]  
              **status** [*isa mda-id*] **detail**  
              **status** [*isa mda-id*] **cpu** [*sample-period seconds*]  
              **status** [*isa mda-id*] **overload**  
              **status** {*isa mda-id*} **qos count**  
              **status** {*isa mda-id*} **qos pools**
- Context**     show>app-assure>group
- Description**   This command displays system statistics.

- Parameters**
- isa mda-id** — Displays information about the specified AA ISA.
    - Values** mda-id: slot/mda: slot: 1 to 10, mda: 1 or 2
  - cflowd** — Displays cflowd status information.
  - detail** — Displays detailed status information.
  - cpu [sample-period seconds]** — Displays DPU utilization info about the specified AA ISA. The **isa mda-id** must be specified. The sample period can be specified within a range of 1 5 seconds (default 1s).
    - Values** 1 to 5
  - overload** — Displays the overload status.
  - qos count** — Displays information about queue statistics. The **isa mda-id** must be specified.
  - qos pools** — Displays information about pool utilization. The **isa mda-id** must be specified.

**Output** The following is an example show output for the **status** command.

### Sample Output

```
*A:Dut-C# show application-assurance group 1 status
=====
Application-Assurance Status
=====
Last time change affecting status : 01/25/2018 18:55:08
Number of Active ISAs : 2
Flows : 0
Flow Resources In Use : 0
AA Subs Created : 0
AA Subs Deleted : 0
AA Subs Modified : 0
AA Subs Quarantined : 0
Seen IP Requests Sent : 0
Seen IP Requests Dropped : 0

Active Flows : 0 0 0
Flow Setup Rate (per second) : 0 0 0
Traffic Rate (Mbps) : 0 0 0
Packet Rate (per second) : 0 0 0
AA-Subs Downloaded : 0 0 0
Active Subs : 0 0 0

Packets Octets

Diverted traffic : 0 0
Diverted discards : 0 0
 Congestion : 0 0
 Errors : 0 N/A
Entered ISA-AAs : 0 0
Buffered in ISA-AAs : 0 0
Discarded in ISA-AAs : 0 0
```



```

Policy : 0 0
Congestion : 0 0
Errors : 0 0
Modified in ISA-AAs : 0 0
 Packet size increased : 0 0
 Packet size decreased : 0 0
Errors (policy bypass) : 0 0
Errors (cut-through) : 0 0
Generated in ISA-AAs : 0 0
 HTTP Redirect : 0 0
Exited ISA-AAs : 0 0
Returned discards : 0 0
 Congestion : 0 0
 Errors : 0 N/A
Returned traffic : 0 0

```

```

=====
*A:Dut-C# show application-assurance group 1 status detail
=====

```

#### Application-Assurance Status

```

=====
Last time change affecting status : 01/25/2018 18:55:08

```

```

Number of Active ISAs : 2
Flows : 0
Flow Resources In Use : 0
AA Subs Created : 0
AA Subs Deleted : 0
AA Subs Modified : 0
Seen IP Requests Sent : 0
Seen IP Requests Dropped : 0

```

```

Current Average Peak

Active Flows : 0 0 0
Flow Setup Rate (per second) : 0 0 0
Traffic Rate (Mbps) : 0 0 0
Packet Rate (per second) : 0 0 0
AA-Subs Downloaded : 0 0 0
Active Subs : 0 0 0

```

```

from-sub packets from-sub octets
to-sub packets to-sub octets

Diverted traffic : 0 0 0
Diverted discards : 0 0 0
 Congestion : 0 0 0
 Errors : 0 N/A
Entered ISA-AAs : 0 0 N/A
Buffered in ISA-AAs : 0 0 0
Discarded in ISA-AAs : 0 0 0
 Policy : 0 0 0

```

|                        |     |     |     |
|------------------------|-----|-----|-----|
|                        |     | 0   | 0   |
| Congestion             | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Errors                 | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Modified in ISA-AAs    | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Packet size increased  | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Packet size decreased  | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Errors (policy bypass) | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Errors (cut-through)   | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Generated in ISA-AAs   | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| HTTP Redirect          | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Exited ISA-AAs         | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Returned discards      | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Congestion             | : 0 | 0   | 0   |
|                        |     | 0   | 0   |
| Errors                 | : 0 | N/A | N/A |
|                        |     | 0   | 0   |
| Returned traffic       | : 0 | 0   | 0   |
|                        |     | 0   | 0   |

```
A:ALU>show>app-assure>group#
```

```
=====
Application-Assurance Status
=====
```

```
Last time change affecting status : 09/28/2012 14:19:05
```

```
Number of Active ISAs : 1
Flows : 62
Flow Resources In Use : 0
AA-Subs Created : 200
AA-Subs Deleted : 149
AA-Subs Modified : 3
Seen-IP Requests Sent : 0
Seen-IP Requests Dropped : 0
```

```

Current Average Peak

Active Flows : 0 0 16
Flow Setup Rate (per second) : 0 0 1
Traffic Rate (Mbps) : 0 0 0
Packet Rate (per second) : 0 0 6
AA-Subs Downloaded : 51 51 51
Active Subs : 0 0 1
```

```
show application-assurance group <aa-group-id> status [isa <slot/mda>] overload
```

```
=====
Application Assurance Group 1 overload
=====
```

```

Trap Configuration High Watermark Low Watermark

Flow usage 95% 90%
Flow setup rate (fps) 60000 55000
Bit rate (Mbps) 9000 8500
Packet rate (pps) 12345678901234567890 12345678901234567890
Datapath CPU usage 95% 90%

ISA 4/1 Total up-time (s) : 12345678901234567890
TCA Type
 Current Level Average Level Peak Level
 State Count Duration (s)

Flow resources
 75.1% 50.0% 82.8%
 cleared 12345678901234567890 12345678901234567890
Flow setup rate
12345678901234567890 12345678901234567890 12345678901234567890
 cleared 0 0
Bit rate
 11000 5000 12000
 raised 1 123456789
Packet rate
 1500000 750000 1600000
 cleared 2 12345
Datapath CPU usage
 15.1% 10.5% 32.1%
 cleared 0 0
Management CPU usage
 65.2% 50.0% 77.5%
 N/A N/A N/A

Overload Trap Configuration High Watermark Low Watermark

From-sub WA buffer depth 80% 75%
To-sub WA buffer depth 80% 75%

Isa-overload-cut-through : enabled
Overload cut-through TCA
 Current from-sub WA : 30%
 Current to-sub WA : 40%
 State : cleared
 Count : 3
 Duration (s) : 123
=====

A:ALU>show>app-assure>group# status isa 3/2 qos count
=====
Application-assurance Queue Statistics for ISA-AA Group: 1, isa 3/2
=====

Egress From-Subscriber
 Queue 1 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0

```

|                         |         |          |
|-------------------------|---------|----------|
| Out/Exc Prof forwarded: | 28940   | 3767233  |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 2                 | Packets | Octets   |
| In Profile forwarded :  | 0       | 0        |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |
| Egress To-Subscriber    |         |          |
| Queue 1                 | Packets | Octets   |
| In Profile forwarded :  | 0       | 0        |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 44499   | 53066848 |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 2                 | Packets | Octets   |
| In Profile forwarded :  | 0       | 0        |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |
| Ingress From-Subscriber |         |          |
| Queue 1                 | Packets | Octets   |
| In Profile forwarded :  | 25548   | 3361023  |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 1       | 60       |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 2                 | Packets | Octets   |
| In Profile forwarded :  | 2921    | 365606   |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 9                 | Packets | Octets   |
| In Profile forwarded :  | 0       | 0        |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 10                | Packets | Octets   |
| In Profile forwarded :  | 0       | 0        |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |
| Ingress To-Subscriber   |         |          |
| Queue 1                 | Packets | Octets   |
| In Profile forwarded :  | 39541   | 46899769 |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 1       | 92       |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 2                 | Packets | Octets   |
| In Profile forwarded :  | 5050    | 6291204  |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |
| Queue 9                 | Packets | Octets   |
| In Profile forwarded :  | 0       | 0        |
| In Profile dropped :    | 0       | 0        |
| Out/Exc Prof forwarded: | 0       | 0        |
| Out/Exc Prof dropped :  | 0       | 0        |

```

Queue 10 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0
Out/Exc Prof forwarded: 0 0
Out/Exc Prof dropped : 0 0
=====
A:ALU>show>app-assure>group#

A:ALU>show>app-assure>group# status isa 3/2 qos pools
=====
Pool Information
=====
MDA : 3/2
Application : Net-Ing Pool Name : default
Resv CBS : 50%

Utilization State Start-Avg Max-Avg Max-Prob

High-Slope Up 70% 90% 80%
Low-Slope Up 50% 75% 80%

Time Avg Factor : 7
Pool Total : 40960 KB
Pool Shared : 20480 KB Pool Resv : 20480 KB

High Slope Start Avg : 12288 KB High slope Max Avg : 16384 KB
Low Slope Start Avg : 10240 KB Low slope Max Avg : 14336 KB

Pool Total In Use : 0 KB
Pool Shared In Use : 0 KB Pool Resv In Use : 0 KB
WA Shared In Use : 0 KB

Hi-Slope Drop Prob : 0 Lo-Slope Drop Prob : 0

FC-Maps Dest MBS Depth A.CIR A.PIR
Q-Grp Q-Id CBS

be af 11 h2 ef h1 nc 5/* 20480 0 8000000 20000000
 1 1280 0 8000000 Max
be af 11 h2 ef h1 nc 4/* 20480 0 8000000 20000000
 1 1280 0 8000000 Max
be af 11 h2 ef h1 nc 3/1 20480 0 8000000 20000000
 1 1280 0 8000000 Max
be af 11 h2 ef h1 nc 2/1 20480 0 8000000 20000000
 1 1280 0 8000000 Max
be af 11 h2 ef h1 nc 1/1 20480 0 8000000 20000000
 1 1280 0 8000000 Max
be af 11 h2 ef h1 nc 5/* 20480 0 8000000 20000000
 1 1280 0 8000000 Max
be af 11 h2 ef h1 nc 4/* 20480 0 8000000 20000000
 1 1280 0 8000000 Max
...
=====
Pool Information
=====
Port : 3/2/fm-sub
Application : Net-Egr Pool Name : default
Resv CBS : 50%

```

```

Queue-Groups

Utilization State Start-Avg Max-Avg Max-Prob

High-Slope Up 70% 90% 80%
Low-Slope Up 50% 75% 80%

Time Avg Factor : 7
Pool Total : 12288 KB
Pool Shared : 6144 KB Pool Resv : 6144 KB

High Slope Start Avg : 4096 KB High slope Max Avg : 5120 KB
Low Slope Start Avg : 3072 KB Low slope Max Avg : 4096 KB

Pool Total In Use : 0 KB
Pool Shared In Use : 0 KB Pool Resv In Use : 0 KB
WA Shared In Use : 0 KB

Hi-Slope Drop Prob : 0 Lo-Slope Drop Prob : 0

FC-Maps ID MBS Depth A.CIR A.PIR
Q-Grp Q-Id CBS

be af l1 h2 ef h1 nc 3/2/fm-* 8192 0 4000000 10000000
 1 5120 4000000 5000000
12 3/2/fm-* 6144 0 6000000 10000000
 2 3584 5000000 5000000
=====
Pool Information
=====
Port : 3/2/to-sub
Application : Net-Egr Pool Name : default
Resv CBS : 50%

Queue-Groups

Utilization State Start-Avg Max-Avg Max-Prob

High-Slope Up 70% 90% 80%
Low-Slope Up 50% 75% 80%

Time Avg Factor : 7
Pool Total : 24576 KB
Pool Shared : 12288 KB Pool Resv : 12288 KB

High Slope Start Avg : 8192 KB High slope Max Avg : 10240 KB
Low Slope Start Avg : 6144 KB Low slope Max Avg : 8192 KB

Pool Total In Use : 0 KB
Pool Shared In Use : 0 KB Pool Resv In Use : 0 KB
WA Shared In Use : 0 KB

Hi-Slope Drop Prob : 0 Lo-Slope Drop Prob : 0

FC-Maps ID MBS Depth A.CIR A.PIR
Q-Grp Q-Id CBS

be af l1 h2 ef h1 nc 3/2/to-* 16384 0 4000000 10000000

```

```

12 1 10240 4000000 Max
 3/2/to-* 12288 0 6000000 10000000
 2 7168 6000000 Max
=====
A:ALU>show>app-assure>group#

```

## tcp-validate

- Syntax** `tcp-validate tcp-validate-name [isa mda-id]`
- Context** `show>app-assure>group`
- Description** This command displays TCP validation policy information.
- When the *mda-id* parameter is included, only TCP validation policy information for the specified adapter card is displayed.
- Parameters** *tcp-validate-name* — Specifies the name of the TCP validation policy. 32 characters maximum.
- mda-id* — Specifies the slot number of an adapter card, in the format *slot/mda*.
- Output** The following output is an example of TCP validation policy information.

### Sample Output

```

A:NOK# show application-assurance group 1 tcp-validate "test" isa 1/1
=====
Application Assurance Group 1 tcp-validate "test"
=====
Description : (Not Specified)
Event log : (Not Specified)
Strict Validation: Yes
AQP referenced : No

Decision Statistics sub-to-net net-to-sub

Total

Allowed
 Octets 0 0
 Packets 0 0
Dropped
 Octets 0 0
 Packets 0 0
Dropped Reason

Bad Flags
 Octets 0 0
 Packets 0 0
Bad Options
 Octets 0 0
 Packets 0 0
Bad Sequence Number
 Octets 0 0

```

|                              |   |   |
|------------------------------|---|---|
| Packets                      | 0 | 0 |
| Bad Acknowledgment Number    |   |   |
| Octets                       | 0 | 0 |
| Packets                      | 0 | 0 |
| No Establishment             |   |   |
| Octets                       | 0 | 0 |
| Packets                      | 0 | 0 |
| SYN After Conn Establishment |   |   |
| Octets                       | 0 | 0 |
| Packets                      | 0 | 0 |
| Asymmetric Traffic           |   |   |
| Octets                       | 0 | 0 |
| Packets                      | 0 | 0 |
| Traffic After Reset (RST)    |   |   |
| Octets                       | 0 | 0 |
| Packets                      | 0 | 0 |
| Fragmented                   |   |   |
| Octets                       | 0 | 0 |
| Packets                      | 0 | 0 |

## traffic-type

**Syntax** **traffic-type detail**  
**traffic-type ip-family**  
**traffic-type ip-protocol**

**Context** show>app-assure>group

**Description** This command displays per traffic type statistics.

**Parameters** **detail** — Displays detailed statistics.  
**ip-family** — Displays IP family statistics.  
**ip-protocol** — Displays IP protocol statistics.

### Output

#### Sample Output

```
*A:Dut-C>show>app-assure>group# traffic-type ip-family
=====
Application-Assurance Traffic Type Statistics Per IP Family
=====
IP Family Disc Octets Packets Flows

IPv4 0% 0 0 0
IPv6 0% 0 0 0
DS-Lite 0% 0 0 0
6RD 0% 0 0 0
Teredo 0% 0 0 0
v4inv4Gtp 0% 0 0 0
v4inv6Gtp 0% 0 0 0
v6inv4Gtp 0% 0 0 0
v6inv6Gtp 0% 0 0 0
```



```
=====
*A:Dut-C>show>app-assure>group# traffic-type ip-protocol detail

IP Protocol: Other IP Family: v4inv4Gtp
Type Octets Packets Flows

From subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows
To subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows
Flow counts:
 Terminated
 Short duration
 Med duration
 Long duration
Total flow duration : 0 seconds

IP Protocol: TCP IP Family: v4inv4Gtp
Type Octets Packets Flows

From subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows
To subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows
Flow counts:
 Terminated
 Short duration
 Med duration
 Long duration
Total flow duration : 0 seconds

IP Protocol: UDP IP Family: v4inv4Gtp
Type Octets Packets Flows

From subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows
To subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows
Flow counts:
 Terminated
 Short duration
 Med duration
 Long duration
Total flow duration : 0 seconds
```

## transit-ip-policy

|                    |                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>transit-ip-policy</b> <i>ip-policy-id</i><br><b>transit-ip-policy summary</b><br><b>transit-ip-policy</b> <i>ip-policy-id</i> <b>summary</b>          |
| <b>Context</b>     | show>app-assure>group                                                                                                                                    |
| <b>Description</b> | This command displays transit IP policy information.                                                                                                     |
| <b>Parameters</b>  | <i>ip-policy-id</i> — Displays information for the specified IP policy.<br><b>Values</b> 1 to 65535<br><b>summary</b> — Displays summarized information. |

## transit-prefix-policy

|                    |                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>transit-prefix-policy</b> <i>transit-prefix-policy-id</i><br><b>transit-prefix-policy summary</b><br><b>transit-prefix-policy</b> <i>transit-prefix-policy-id</i> <b>summary</b> |
| <b>Context</b>     | show>app-assure>group                                                                                                                                                               |
| <b>Description</b> | This command displays transit prefix policy information.                                                                                                                            |
| <b>Parameters</b>  | <i>transit-prefix-policy-id</i> — Displays information for the specified transit prefix policy.<br><b>Values</b> 1 to 65535<br><b>summary</b> — Displays summarized information.    |

## url-list

|                    |                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>url-list</b> <i>url-list-name</i>                                                                 |
| <b>Context</b>     | show>app-assure>group                                                                                |
| <b>Description</b> | This command displays information about the configured url-list providing the following information: |
| <b>Parameters</b>  | <i>url-list-name</i> — Specifies the name of the URL list to display.                                |
| <b>Output</b>      | <a href="#">Table 20</a> describes the show command output fields:                                   |

**Table 20 Show URL List Output Fields**

| Label                     | Description                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Status              | [Up   Down] - Administrative status of the url-list                                                                                                                                                                      |
| Oper Status               | [Up   Down] - Operational status of the url-list                                                                                                                                                                         |
| Oper Flags                | [admin-down   file-does-not-exist   invalid-file-format   too-many-urls   switch-over-error]                                                                                                                             |
| File Deployed to ISA      | [Yes   No] - This flag describes if the file located in the compact flash is the one deployed in the ISA, in the event the file is overwritten and before the admin upgrade command is used this flag will display "No". |
| <b>Upgrade Statistics</b> |                                                                                                                                                                                                                          |
| Last Success              | Last time the list was successfully upgraded                                                                                                                                                                             |
| File Name                 | File name for the last successful upgrade                                                                                                                                                                                |
| URL Entries               | Number of URLs loaded at the last success                                                                                                                                                                                |
| Blank/Comment Lines       | Number of blank or commented out lines                                                                                                                                                                                   |
| Last Attempt              | Last time the operator tried to upgrade the list                                                                                                                                                                         |
| Result                    | Success   Failure. Result of the last upgrade                                                                                                                                                                            |
| File Name                 | File name for the last upgrade attempt                                                                                                                                                                                   |
| Error Line                | Line error resulting in a failure to upgrade.                                                                                                                                                                            |
| Reason                    | [invalid-file-format   too-many-urls] - Reason for the failure to upgrade                                                                                                                                                |
| Detail                    | Details related to the failed upgrade (example: decryption failed)                                                                                                                                                       |

### Sample Output

```

7750# show application-assurance group 1 url-list "url-list1"
=====
Application Assurance Group 1 url-list "url-list2"
=====
Description : (Not Specified)
Admin Status : Up
Oper Status : Up
Oper Flags : <none>
File deployed to ISAs : Yes

Upgrade Statistics

Last Success : 01/20/2015 11:33:29
 Deployed
 File Name : cf3:\url-list1.enc

```

```
URL Entries : 1000
Blank/Comment Lines : 0
Last Attempt : 01/20/2015 11:33:29
Result : Success
File Name : cf3:\url-list1.enc
```

```
=====
7750# show application-assurance group 1 url-list "url-list1"
=====
```

```
Application Assurance Group 1 url-list "url-list1"
=====
```

```
Description : (Not Specified)
Admin Status : Up
Oper Status : Up
Oper Flags : <none>
File deployed to ISAs : Yes
```

```

Upgrade Statistics

```

```
Last Success : 01/21/2015 14:03:54
Deployed
 File Name : cf3:\url-list1.txt
 URL Entries : 0
 Blank/Comment Lines : 0
Last Attempt : 01/21/2015 14:06:39
Result : Failure
 File Name : cf3:\url-list1.txt
 Error Line : 0
 Reason : invalid-file-format
 Detail : Decryption failed
=====
```

## url-filter

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>url-filter</b> <i>url-filter-name</i><br><b>url-filter</b> <i>url-filter-name</i> <b>isa</b> <i>card/mda</i> [ <b>detail</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | show>app-assure>group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | <p>This command displays information about the configured url-filter policy along with some associated raw statistics. These output statistics are:</p> <ul style="list-style-type: none"> <li>• Vlan Id: Vlan id used by the aa interfaces</li> <li>• Admin Status: Up / Down</li> <li>• Oper Status: Up / Down</li> <li>• Oper Flags: adminDown, no-aa-if, aa-if-down, icap-server-down</li> <li>• Default Action: default policy action taken by the url-filter</li> <li>• ICAP HTTP Redirect: HTTP redirect Policy</li> <li>• AQP Referenced: Yes/No</li> <li>• HTTP Request: Number of subscriber HTTP requests</li> <li>• HTTP Errors: Impossible to send an ICAP request, this can be caused by either no TCP connection available, associated flow with a drop action due to another aqp policy, system resource exhausted</li> <li>• ICAP Request: Number of ICAP request sent</li> <li>• ICAP Errors: ICAP request timeout, unexpected ICAP response, internal TCP errors.</li> <li>• Custom-x-header: Name of the custom-x-header, if configured. If it is not configured, the value is "Not Specified".</li> </ul> <p>In addition to these counters the system will count the type of action taken by the url-filter policy (allow, block, redirect, default) as well as the type of responses received from the icap server (allow, block, redirect, late).</p> |
| <b>Parameters</b>  | <p><i>url-filter-name</i> — Specifies the name of the url-filter policy.</p> <p><i>card/mda</i> — Specifies the card/mda reference of the ISA card.</p> <p><b>detail</b> — Specifies detailed statistics related to the ISA card.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output</b>      | The following is an example show output for the <b>url-filter</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Sample Output

```
A:7750# show application-assurance group 1 url-filter "filter1"
=====
Application Assurance Group 1 URL Filter "filter1"
=====
Description : (Not Specified)
Admin Status : Up
Oper Status : Up
Oper Flags : <none>

Default Action : block-http-redirect http-redirect-portal
```

```

HTTP Request Filtering : all
HTTP Redirect : http-redirect-portal
AQP Referenced : Yes

```

```

ICAP Filter
 Custom X-Header : Filtering-Policy
 VLAN Id : 10

```

-----

Total Connection Stats

-----

|                       |      |                 |          |
|-----------------------|------|-----------------|----------|
| HTTP Requests         | : 17 | ICAP Requests   | : 17     |
| HTTP Req Errors       | : 0  | ICAP Req Errors | : 0      |
| HTTP Response Actions |      | ICAP Responses  |          |
| Allow                 | : 0  | Allow           | : 0      |
| Block                 | : 0  | Block           | : 0      |
| Redirect              | : 0  | Redirect        | : 0      |
| Default               | : 0  | Late ICAP Resp  | : 0      |
|                       |      | Packets Disc    | : 168    |
|                       |      | Octets Disc     | : 229440 |

=====

A:7750# show application-assurance group 1 url-filter "filter1" isa 1/2

=====

Application Assurance Group 1 URL Filter "filter1" ISA 1/2

=====

```

Description : (Not Specified)
Admin Status : Up
Oper Status : Up
Oper Flags : <none>

Default Action : block-http-redirect http-redirect-portal
HTTP Request Filtering : all
HTTP Redirect : http-redirect-portal
AQP Referenced : Yes

```

```

ICAP Filter
 Custom X-Header : Filtering-Policy
 VLAN Id : 10
 AA Interface : aa-if1
 Service : IES 1
 SAP Id : 1/2/aa-svc:10
 ICAP Client IP : 172.16.2.0/31

```

-----

ISA 1/2 Connection Stats

-----

|                       |      |                 |          |
|-----------------------|------|-----------------|----------|
| HTTP Requests         | : 17 | ICAP Requests   | : 17     |
| HTTP Req Errors       | : 0  | ICAP Req Errors | : 0      |
| HTTP Response Actions |      | ICAP Responses  |          |
| Allow                 | : 17 | Allow           | : 17     |
| Block                 | : 0  | Block           | : 0      |
| Redirect              | : 0  | Redirect        | : 0      |
| Default               | : 0  | Late ICAP Resp  | : 0      |
|                       |      | Packets Disc    | : 168    |
|                       |      | Octets Disc     | : 229440 |

-----

ISA 1/2 ICAP Connection Stats

-----

```

ICAP Server Oper Request Rate Round Trip
 Status (per second) (microsecond)

172.16.1.101 Up 0 1909

=====

A:7750# show application-assurance group 1 url-filter "filter1" isa 1/2 detail
=====
Application Assurance Group 1 URL Filter "filter1" ISA 1/2
=====
Description : (Not Specified)
Admin Status : Up
Oper Status : Up
Oper Flags : <none>

Default Action : block-http-redirect http-redirect-portal
HTTP Request Filtering : all
HTTP Redirect : http-redirect-portal
AQP Referenced : Yes

ICAP Filter
 Custom X-Header : Filtering-Policy
 VLAN Id : 10
 AA Interface : aa-if1
 Service : IES 1
 SAP Id : 1/2/aa-svc:10
 ICAP Client IP : 172.16.2.0/31

ISA 1/2 Connection Stats

HTTP Requests : 17 ICAP Requests : 17
HTTP Req Errors : 0 ICAP Req Errors : 0

HTTP Response Actions ICAP Responses
 Allow : 17 Allow : 17
 Block : 0 Block : 0
 Redirect : 0 Redirect : 0
 Default : 0 Late ICAP Resp : 0
 Packets Disc : 168
 Octets Disc : 229440

ICAP Server 172.16.1.101 ISA 1/2

Description : (Not Specified)
Admin Status : Up
Oper Status : Up
Oper Flags : <none>

Established Connections : 10 of 10 connections
Connection Utilization : 0%
Request Rate : 0 per second
Round Trip Time : 1909 microseconds
=====

```

## url-list

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>url-list</b> <i>url-list-name</i>                             |
| <b>Context</b>     | show>app-assure>group                                            |
| <b>Description</b> | This command displays information about the configured URL list. |
| <b>Parameters</b>  | <i>url-list-name</i> — Specifies the name of the URL list.       |
| <b>Output</b>      | The following output examples show URL list information.         |

### Output

```

7750# show application-assurance group 1 url-list "url-list1"
=====
Application Assurance Group 1 url-list "url-list2"
=====
Description : (Not Specified)
Size : Standard
Admin Status : Up
Oper Status : Up
Oper Flags : <none>
File deployed to ISAs : Yes

Upgrade Statistics

Last Success : 01/20/2015 11:33:29
 Deployed
 File Name : cf3:\url-list1.enc
 URL Entries : 1000 (6.66%)
 URL Characters : 1000 (15.00%)
 Blank/Comment Lines : 0
Last Attempt : 01/20/2015 11:33:29
 Result : Success
 File Name : cf3:\url-list1.enc
=====

7750# show application-assurance group 1 url-list "url-list1"
=====
Application Assurance Group 1 url-list "url-list1"
=====
Description : (Not Specified)
Size : Standard
Admin Status : Up
Oper Status : Up
Oper Flags : <none>
File deployed to ISAs : Yes

Upgrade Statistics

Last Success : 01/21/2015 14:03:54
 Deployed
 File Name : cf3:\url-list1.txt
 URL Entries : 0
 Blank/Comment Lines : 0
Last Attempt : 01/21/2015 14:06:39

```



```
Result : Failure
File Name : cf3:\url-list1.txt
Error Line : 0
Reason : invalid-file-format
Detail : Decryption failed
=====
```

Table 21 describes the URL list show command output fields.

**Table 21** URL List Show Command Field Descriptions

| Label                     | Description                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Size                      | [standard   extended] Specifies the size parameter for the URL list                                                                                                                                                      |
| Admin Status              | [Up   down] - Administrative status of the URL list                                                                                                                                                                      |
| Oper Status               | [Up   down] - Operational status of the URL list                                                                                                                                                                         |
| Oper Flags                | [admin-down   file-does-not-exist   invalid-file-format   too-many-urls   switch-over-error]                                                                                                                             |
| File Deployed to ISA      | [Yes   No] - This flag describes if the file located in the compact flash is the one deployed in the ISA, in the event the file is overwritten and before the admin upgrade command is used this flag will display "No". |
| <b>Upgrade Statistics</b> |                                                                                                                                                                                                                          |
| Last Success              | Last time the list was successfully upgraded                                                                                                                                                                             |
| File Name                 | File name for the last successful upgrade                                                                                                                                                                                |
| URL Entries               | Number of URLs loaded at the last success and percentage to full                                                                                                                                                         |
| URL Characters            | Number of characters loaded at the last success and percentage to full                                                                                                                                                   |
| Blank/CommentLines        | Number of blank or commented out lines                                                                                                                                                                                   |
| Last Attempt              | Last time the operator tried to upgrade the list                                                                                                                                                                         |
| Result                    | [Success   Failure]. Result of the last upgrade                                                                                                                                                                          |
| File Name                 | File name for the last upgrade attempt                                                                                                                                                                                   |
| Error Line                | Line error resulting in a failure to upgrade                                                                                                                                                                             |
| Reason                    | [invalid-file-format   too-many-urls] - Reason for the failure to upgrade                                                                                                                                                |

**Table 21** URL List Show Command Field Descriptions (Continued)

| Label  | Description                                                        |
|--------|--------------------------------------------------------------------|
| Detail | Details related to the failed upgrade (example: decryption failed) |

## charging-group

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>charging-group</b> [ <i>charging-group-name</i> ] <b>count</b> [ <b>detail</b> ]<br><b>charging-group count top</b> <i>granularity</i> [ <b>max-count</b> <i>max-count</i> ]                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | show>app-assure>group>aa-sub                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command displays application-assurance group charging group information.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>charging-group-name</i> — Specifies an existing charging group.<br><b>count</b> — Displays the counters for the charging group.<br><b>detail</b> — Displays detailed information.<br><b>top</b> — Displays counters sorted by granularity.<br><i>granularity</i> — Specifies the granularity of the search.<br><b>Values</b> octets, packets, flows<br><i>max-count max-count</i> — Specifies the maximum flows to display.<br><b>Values</b> 1 to 4294967295 |

## http-notification

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-notification</b> <i>http-notification-name</i> [ <b>summary</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | show>app-assure>group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | This command displays information about the configured http-notification policy with associated raw statistics: <ul style="list-style-type: none"><li>• Template: Template Id in use</li><li>• Script URL: URL address of the script used in the notification message</li><li>• Admin Status: Up / Down</li><li>• AQP Referenced: Yes/No</li><li>• Notified: Total number of notifications sent</li><li>• Notification criteria selection not matched: Number of HTTP request not matching the selection criteria for in browser notification</li></ul> |
| <b>Parameters</b>  | <i>http-notification-name</i> — Displays the name of the http-notification policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Output** The following is an example show output for the **http-notification** command.

### Sample Output

```
A:7750# show application-assurance group 1 http-notification "in-browser-
notification"
=====
Application Assurance Group 1 HTTP Notification "in-browser-notification"
=====
Description : IBN Demo ALU Message
Template : 1 - Javascript-url with subId and optional Http-Url-Param
Script URL : http://10.1.1.1/In-Browser-Notification/script.js
Admin Status : Up
AQP Ref : Yes

```

|       | Notified | Notification Selection<br>Criteria Not Matched |
|-------|----------|------------------------------------------------|
| 1:1   | 3        | 0                                              |
| 1:2   | 2        | 0                                              |
| 1:3   | 0        | 0                                              |
| 1:4   | 0        | 0                                              |
| 1:5   | 0        | 0                                              |
| Total | 5        | 0                                              |

```

=====
```

## http-notification

**Syntax** **http-notification** *http-notification-name* **summary**

**Context** show>app-assure>group

**Description** This command displays information about the configured http-notification policy with associated raw statistics summed over all partitions.

- Template: Template Id in use
- Script URL: URL address of the script used in the notification message
- Admin Status: Up / Down
- AQP Referenced: Yes/No
- Notified: Total number of notifications sent
- Notification criteria selection not matched: Number of HTTP request not matching the selection criteria for in browser notification

**Parameters** *http-notification-name* — Displays the name of the http-notification policy.

**summary** — Displays summarized information about the http-notification policy.

**Output** The following is an example show output for the **http-notification** command.

**Sample Output**

```

A:Dut-D# show application-assurance group 1 http-notification "in-browser-
notification" summary
=====
Application Assurance Group 1 HTTP Notification "in-browser-notification"
=====
Description : IBN Demo ALU Message
Template : 1 - Javascript-url with subId and optional Http-Url-Param
Script URL : http://10.1.1.1/In-Browser-Notification/script.js
Admin Status : Up
AQP Ref : Yes

 Notified Notification Selection
 Criteria Not Matched

Total 5 0

=====

```

**partition**

**Syntax** **partition summary**

**Context** show>app-assure>group

**Description** This command displays partition information.

**Parameters** **summary** — Displays partition summary information.

**policer**

**Syntax** **policer**  
**policer** *policer-name* [**detail**]  
**policer summary**

**Context** show>app-assure>group

**Description** This command displays application-assurance policer information.

**Parameters** *policer-name* — Displays information about the specified policer.  
**detail** — Displays detailed information about policers on this node.  
**summary** — Displays summarized information about policers on this node.

**Output** The following is an example show output for the **policer** command.

**Sample Output**

```
show application-assurance group 1 policer <policer-name> detail
```

```
=====
Policer Instance "lm-dwn"
=====
Description : (Not Specified)
Type : dual-bucket-bandwidth
Granularity : subscriber
Adaptation Rule : pir closest cir closest

Active tod-override : none

PIR : max Oper PIR : max
CIR : 0 kbps Oper CIR : 0 kbps
MBS : 20000 KB Oper MBS : 20000 KB
CBS : 0 KB Oper CBS : 0 KB

No. of tod-overrides : 2

Time of Day Override Instance 10

Description : (Not Specified)
Admin State : in-service

Occurrence : daily (monday tuesday wednesday thursday friday)
Start time : 19:00
End time : 22:00

PIR : max
CIR : 0 kbps
MBS : 10000 KB
CBS : 0 KB

Time of Day Override Instance 20

Description : (Not Specified)
Admin State : in-service

Occurrence : daily (sunday saturday)
Start time : 19:00
End time : 22:00

PIR : max
CIR : 0 kbps
MBS : 5000 KB
CBS : 0 KB
=====
```

### Sample Output

```
*A:Dut-C>show>app-assure>group# policer "test"
=====
Policer Instance "test"
=====
Description : (Not Specified)
Type : single-bucket-bandwidth
Granularity : access-network-location
Action : permitDeny
Adaptation Rule : pir closest
Rate-Percentage : 10
```

---

## policy

|                    |                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>policy</b>                                                                                       |
| <b>Context</b>     | show>app-assure>group                                                                               |
| <b>Description</b> | This command enables the context to display application-assurance policy configuration information. |

## http-error-redirect

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-error-redirect</b> <i>redirect-name</i>                                       |
| <b>Context</b>     | show>app-assure>group                                                                 |
| <b>Description</b> | This command enables the context to display http-error-redirect static definitions.   |
| <b>Parameters</b>  | <i>redirect-name</i> — Specifies the HTTP error redirect policy, up to 32 characters. |
| <b>Output</b>      | The following is an example show output for the <b>policy</b> command.                |

### Sample Output

```

*A:cses-E11>show application-assurance group 1 http-error-redirect <redirect-name>
=====
Application-Assurance Group 1 http-error-redirect <redirect-name>
=====
description : <description-string>
template : <template-id>
 : text description of template
participant-id : <string>
http-host : <http-host-name>
error code : <http-error-code> custom-msg-size : <msg size>
admin status : Up
=====
Grp:Part Error Redirects Redirects Not Sent
 Code Sent > Custom Out ofFile Error
 size ResourceType

1:1 404 1250 52 10 10
1:56789 404 2000 952 81 01

Total 3250 1004 91 1 1

=====
*A:cses-E11>

```

## http-redirect

|                    |                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-redirect</b> <i>redirect-name</i> [ <b>detail</b> ]                                                              |
| <b>Context</b>     | show>app-assure>group                                                                                                    |
| <b>Description</b> | This command displays application assurance http-redirect statistics and status information.                             |
| <b>Parameters</b>  | <i>redirect-name</i> — Specifies the name of the http-redirect policy.<br><b>detail</b> — Displays detailed information. |
| <b>Output</b>      | The following table describes the show command output fields:                                                            |

**Table 22 Show HTTP Redirect Output Fields**

| Label            | Description                                                                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template         | Specifies HTTP redirect template id information. Each HTTP redirect template returns a specific HTTP redirect message such as HTTP 302 or Javascript and can optionally use macro substitution. |
| Redirect URL     | Specifies the address the subscriber will be redirected to.                                                                                                                                     |
| Captive Redirect | Specifies Yes if captive redirect is used and No if captive redirect is not used.                                                                                                               |
| Redirect HTTPS   | Specifies Yes if redirect https is used and No if redirect https is not used.                                                                                                                   |
| VLAN ID          | Specifies the AA interface VLAN id used for captive redirect.                                                                                                                                   |
| Admin Status     | Specifies the administrative status (Up/Down) of the HTTP redirect policy.                                                                                                                      |
| AQP Ref          | Specifies Yes if the HTTP redirect policy is referenced in AQP, and No if it is not.                                                                                                            |

### Sample Output

```
*A:7750# show application-assurance group 1 http-redirect "redirect-portal"

=====
Application Assurance Group 1 HTTP Redirect redirect-portal
=====
Description : (Not Specified)
Template : 5
 : Redirect supporting macro substitution using HTTP 302
Redirect URL : http://172.16.70.100/Redirect/redirect-
portal.html?RequestedURL=$URL
Captive Redirect : Yes
 Redirect HTTPS : Yes
 VLAN ID : 20
```

```
Admin Status : Up
AQP Ref : Yes
```

```

Summary Statistics

```

| Grp:Part | Redirects<br>Sent | Client Resets<br>Sent | Redirects<br>Not Sent |
|----------|-------------------|-----------------------|-----------------------|
| 1:1      | 0                 | 0                     | 0                     |
| 1:2      | 0                 | 0                     | 0                     |
| 1:3      | 0                 | 0                     | 0                     |
| Total    | 0                 | 0                     | 0                     |

```
=====
```

## error-codes

- Syntax** **error-codes**
- Context** show>app-assure>http-redirect
- Description** This command displays http-error-redirect error-codes.
- Output** The following output example shows HTTP error redirect error code information, and [Table 23](#) describes the fields.

### Example Output

```
*A:Dut-C>show application-assurance http-error-redirect error-codes
=====
Application-Assurance http-error-redirect error-codes
=====
```

| Code | Description                   | Default custom-msg-size |
|------|-------------------------------|-------------------------|
| 400  | Bad Request                   | 1024                    |
| 401  | Unauthorized                  | 1024                    |
| 402  | Payment Required              | 1024                    |
| 403  | Forbidden                     | 1024                    |
| 404  | Not Found                     | 1024                    |
| 405  | Method Not Allowed            | 1024                    |
| 406  | Not Acceptable                | 1024                    |
| 407  | Proxy Authentication Required | 1024                    |
| 408  | Request Timeout               | 1024                    |
| 409  | Conflict                      | 1024                    |
| 410  | Gone                          | 1024                    |
| 411  | Length Required               | 1024                    |
| 412  | Precondition Failed           | 1024                    |
| 413  | Payload Too Large             | 1024                    |
| 414  | URI Too Long                  | 1024                    |
| 415  | Unsupported Media Type        | 1024                    |
| 416  | Range Not Satisfiable         | 1024                    |
| 417  | Expectation Failed            | 1024                    |
| 421  | Misdirected Request           | 1024                    |



|     |                                 |      |
|-----|---------------------------------|------|
| 422 | Unprocessable Entity            | 1024 |
| 423 | Locked                          | 1024 |
| 424 | Failed Dependency               | 1024 |
| 425 | Too Early                       | 1024 |
| 426 | Upgrade Required                | 1024 |
| 427 | Unassigned                      | 1024 |
| 428 | Precondition Required           | 1024 |
| 429 | Too Many Requests               | 1024 |
| 430 | Unassigned                      | 1024 |
| 431 | Request Header Fields Too Large | 1024 |
| 451 | Unavailable For Legal Reasons   | 1024 |
| 500 | Internal Server Error           | 1024 |
| 501 | Not Implemented                 | 1024 |
| 502 | Bad Gateway                     | 1024 |
| 503 | Service Unavailable             | 1024 |
| 504 | Gateway Timeout                 | 1024 |
| 505 | HTTP Version Not Supported      | 1024 |
| 506 | Variant Also Negotiates         | 1024 |
| 507 | Insufficient Storage            | 1024 |
| 508 | Loop Detected                   | 1024 |
| 509 | Unassigned                      | 1024 |
| 510 | Not Extended                    | 1024 |
| 511 | Network Authentication Required | 1024 |
| 730 | Custom Error Code               | 1024 |
| 731 | Custom Error Code               | 1024 |
| 735 | Custom Error Code               | 1024 |

=====

**Table 23** Show Application Assurance HTTP Redirect Error Codes Output Fields

| Label                                 | Description                                 |
|---------------------------------------|---------------------------------------------|
| Description                           | Describes the error                         |
| Default                               | Indicates what the default is for the error |
| custom-msg-size (Custom Message Size) | The size of the message                     |

## template

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>template</b>                                                         |
| <b>Context</b>     | show>app-assure>http-redirect                                           |
| <b>Description</b> | This command displays http-error-redirect template information.         |
| <b>Output</b>      | The following is an example show output for the <b>policer</b> command. |

### Sample Output

```
*A:cses-E11>show application-assurance http-error-redirect template
```

```

=====
Application-Assurance http-error-redirect templates
=====
ID Description

1 Template suited for Barefruit landing server. Includes participant-id.
2 Template suited for Xerocole landing server.
=====
*A:cses-E11>

```

## template

|                    |                                                               |
|--------------------|---------------------------------------------------------------|
| <b>Syntax</b>      | <b>template</b>                                               |
| <b>Context</b>     | show>app-assure>http-notif                                    |
| <b>Description</b> | This command displays http-notification template information. |

## template

|                    |                                                           |
|--------------------|-----------------------------------------------------------|
| <b>Syntax</b>      | <b>template</b>                                           |
| <b>Context</b>     | show>app-assure>http-redirect                             |
| <b>Description</b> | This command displays http-redirect template information. |

## protocol

|                    |                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>protocol</b> [ <i>protocol-name</i> ]<br><b>protocol</b> [ <i>protocol-name</i> ] <b>detail</b>                                                          |
| <b>Context</b>     | show>app-assure                                                                                                                                             |
| <b>Description</b> | This command displays application-assurance policy protocols loaded from the isa-aa.tim file.                                                               |
| <b>Parameters</b>  | <i>protocol-name</i> — Displays all protocols from the isa-aa.tim file.<br><b>detail</b> — Displays detailed information about the specified protocol name. |
| <b>Output</b>      | The following is an example show output for the <b>protocol</b> command.                                                                                    |

### Sample Output

```

A:ALU-ABC>show>app-assure# protocol
=====
Application Assurance Protocols
=====
Protocol : Description

```

```

 aim_oscar : America Online Oscar Instant Messaging.
 aim_oscar_file_xfer : America Online Oscar File Transfer.
 aim_oscar_video_voice : America Online Oscar Video and Voice
 Traffic.
 aim_toc : America Online Talk to Oscar Instant
 Messaging.
 bittorrent : BitTorrent peer to peer protocol.
...
A:ALU-ABC>show>app-assure#

A:ALU-ABC>show>app-assure# protocol tftp
=====
Application Assurance Protocols
=====
 Protocol : Description

 tftp : IETF RFC 1350: Trivial File Transfer
 Protocol.
=====
A:ALU-ABC>show>app-assure#

```

## radius-accounting-policy

|                    |                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>radius-accounting-policy</b> [ <i>rad-acct-plcy-name</i> ]<br><b>radius-accounting-policy</b> <i>rad-acct-plcy-name</i> <b>associations</b><br><b>radius-accounting-policy</b> <i>rad-acct-plcy-name</i> <b>statistics</b>             |
| <b>Context</b>     | show>app-assure                                                                                                                                                                                                                           |
| <b>Description</b> | This command displays RADIUS accounting policy information.                                                                                                                                                                               |
| <b>Parameters</b>  | <i>rad-acct-plcy-name</i> — Specifies the RADIUS accounting policy.<br><b>associations</b> — Specifies to show what contexts are associated with this policy.<br><b>statistics</b> — Specifies to show statistics related to this policy. |

## threshold-crossing-alert

|                    |                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>threshold-crossing-alert</b> [ <b>detail</b> ]                                              |
| <b>Context</b>     | show>app-assure                                                                                |
| <b>Description</b> | This command displays information about threshold crossing alerts.                             |
| <b>Output</b>      | The following output example shows application assurance threshold crossing alert information. |

### Sample Output

```

show application-assurance threshold-crossing-alert
=====
Grp:Part Type Name Entry Dir

1 error-drop N/A N/A to-sub
1 error-drop N/A N/A from-sub
1 frag-drop-ooo N/A N/A to-sub
1 overload-drop N/A N/A from-sub
1 overload-drop N/A N/A to-sub
1 gtp-filter gtpFilter def-action from-sub
1 gtp-filter gtpfilter max-payload from-sub
1 gtp-filter gtpfilter def-action from-sub
1 gtp-filter red 2 to-sub
1 gtp-filter red def-action from-sub
1 sctp-filter blue ppid-range to-sub
1 sctp-filter red 1 from-sub
1 sctp-filter red 2 to-sub
1 sctp-filter red ppid-range from-sub
1 sctp-filter red def-action to-sub
1 sctp-filter red def-action from-sub
1 session-filter blue def-action from-sub
1 session-filter red 1 from-sub
1 session-filter red 2 to-sub
1 session-filter red def-action from-sub
1 tcp-validate green N/A to-sub
2:50 error-drop N/A N/A to-sub
2:32656 error-drop N/A N/A from-sub
2:32656 policer 12345679801234567890123456789012 N/A from-sub
2:32656 policer red N/A from-sub

No. of TCAs: 24
=====

```

```

show application-assurance threshold-crossing-alert detail
=====
Application Assurance Threshold Crossing Alerts
=====

tcp-validate "green" to-sub

Group:Part : 1 Trigger on : denied-traffic
High watermark : 30 Low watermark : 20
Last raised : N/A Last cleared : N/A
State : cleared

```

## version

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>version</b>                                                                        |
| <b>Context</b>     | show>app-assure                                                                       |
| <b>Description</b> | This command displays the versions of the isa-aa.tim used by the CPM and the AA ISAs. |
| <b>Output</b>      | The following is an example show output for the <b>version</b> command.               |

**Sample Output**

```
A:ALU>show>app-assure# version
=====
Versions of isa-aa.tim in use
=====
CPM : TiMOS-M-7.0.R4
1/1 : TiMOS-I-7.0.R1
2/1 : TiMOS-I-7.0.R1
3/2 : TiMOS-I-7.0.R1
=====
A:ALU>show>app-assure#
```

**mda**

|                    |                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mda</b> [ <i>slot</i> [ <i>/mda</i> ]] [ <i>detail</i> ]                                                                                                                                                |
| <b>Context</b>     | show                                                                                                                                                                                                       |
| <b>Description</b> | This command displays MDA information.<br><br>If no command line options are specified, a summary output of all MDAs is displayed in table format.                                                         |
| <b>Parameters</b>  | <i>slot</i> — The slot number for which to display MDA information.<br><i>mda</i> — The MDA number in the slot for which to display MDA information.<br><b>detail</b> — Displays detailed MDA information. |
| <b>Output</b>      | <a href="#">Table 24</a> describes MDA output fields.                                                                                                                                                      |

**Table 24** Show MDA Output Fields

| Label             | Description                      |
|-------------------|----------------------------------|
| Slot              | The chassis slot number.         |
| MDA               | The MDA slot number.             |
| Provisioned type  | The MDA type provisioned.        |
| Equipped type     | The MDA type actually installed. |
| Admin State       | Up — Administratively up.        |
|                   | Down — Administratively down.    |
| Operational State | Up — Operationally up.           |
|                   | Down — Operationally down.       |

**Sample Output**

```

show mda
=====
MDA Summary
=====
Slot Mda Provisioned Type Admin Operational
 Mda Equipped Type (if different) State State

2 1 m20-lgb-xp-sfp up up
 2 isa-aa up up/active
 isa-ms
=====

```

## aa-sub-using

- Syntax** **aa-sub-using**  
**aa-sub-using app-profile-name**
- Context** show>service
- Description** This command displays application subscriber information.
- Parameters** *app-profile-name* — Specifies the application profile name.
- Output** The following is an example show output for the **aa-sub-using** command.

### Sample Output

```

*B:Dut-C# show service aa-sub-using
=====
Aa-Subscribers
=====
aa-sub-type aa-sub-name app-profile-name

esm-mac diameter_esm-000100000001 app-prof-~%;&+-!~?
esm-mac diameter_esm-000100000002 app-prof-~%;&+-!~?
esm-mac diameter_esm-000100000003 app-prof-~%;&+-!~?
esm-mac diameter_esm-000100000004 app-prof-~%;&+-!~?
=====

```

## sap-using app-profile

- Syntax** **sap-using app-profile app-profile-name**
- Context** show>service
- Description** This command displays information about SAPs using the specified application profile.
- Parameters** *app-profile-name* — Specifies an existing application profile name created in the **config>app-assure>group>policy** context.
- Output** The following is an example show output for the **sap-using app profile** command.

Sample Output

```
*A:ALA-48# show service sap-using app-profile test
=====
Service Access Point Using Application Profile 'test'
=====
PortId SvcId Ing. Ing. Egr. Egr. Adm Opr
 QoS Fltr QoS Fltr

1/1/18:0 89 1 none 1 none Up Down

Number of SAPs : 1

=====
*A:ALA-48#
```

sap-using aarp

- Syntax** **sap-using aarp** *aarp-id*
- Context** show>service
- Description** This command displays SAP information for a specific AARP ID.
- Parameters** *aarp-id* — Specifies the AARP ID.

**Values** 1 to 65535

sap-using transit-policy

- Syntax** **sap-using transit-policy ip** *transit-ip-policy*  
**sap-using transit-policy prefix** *transit-prefix-policy*
- Context** show>service
- Description** This command displays SAP information for a specific transit IP policy or transit prefix policy.
- Parameters** *transit-ip-policy* — Specifies the transit IP policy ID.

**Values** 1 to 65535

*transit-prefix-policy* — Specifies a transit prefix policy ID.

**Values** 1 to 65535

sdp-using aarp

- Syntax** **sdp-using aarp** *aarp-id*
- Context** show>service

---

**Description** This command displays SDP information for a specific AARP instance ID.

**Parameters** *aarp-id* — Specifies the AARP instance ID.

**Values** 1 to 65535

## sdp-using app-profile

**Syntax** **sdp-using app-profile** *app-profile-name*

**Context** show>service

**Description** This command displays the SDP and associated services diverted to Application Assurance using a specific app profile name.

## sdp-using transit-policy

**Syntax** **sdp-using transit-policy ip** *transit-ip-policy*  
**sdp-using transit-policy prefix** *transit-prefix-policy*

**Context** show>service

**Description** This command displays SDP information for an IP transit IP policy or a transit prefix policy.

**Parameters** *ip-policy-id* — Specifies an transit IP policy ID.

**Values** 1 to 65535

*transit-prefix-policy* — Specifies a transit prefix policy ID.

**Values** 1 to 65535

## subscriber-using app-profile

**Syntax** **subscriber-using app-profile** *app-profile-name*

**Context** show>service

**Description** This command displays the subscribers and associated services diverted to Application Assurance using a specific app profile name.

**Output**

### Sample Output

```
*A:Dut-C# show service aa-sub-using
=====
Aa-Subscribers
=====
```



| aa-sub-type              | aa-sub-name               | app-profile-name  |
|--------------------------|---------------------------|-------------------|
| esm-mac                  | diameter_esm-000100000001 | app-prof-~%;&+-!? |
| esm-mac                  | diameter_esm-000100000002 | app-prof-~%;&+-!? |
| ....                     |                           |                   |
| esm-mac                  | diameter_esm-000100000064 | app-prof-~%;&+-!? |
| -----                    |                           |                   |
| Number of ESM subs       |                           | : 0               |
| Number of ESM mac subs   |                           | : 100             |
| Number of SAP subs       |                           | : 0               |
| Number of Spoke-Sdp subs |                           | : 0               |
| Number of Transit subs   |                           | : 0               |
| Total number of aa-subs  |                           | : 100             |
| -----                    |                           |                   |

### 3.5.2.2 Tools Commands

#### aarp

|                    |                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>aarp</b> <i>aarpld</i> <b>event-history</b> [ <b>clear</b> ]                                                                                                                                       |
| <b>Context</b>     | tools>dump>application-assurance                                                                                                                                                                      |
| <b>Description</b> | This command dumps application-assurance AARP information for a specified instance.                                                                                                                   |
| <b>Parameters</b>  | <i>aarpld</i> — Specifies the AARP ID.<br><b>Values</b> 1 to 65535<br><b>event-history</b> — Dumps historical information for the instance.<br><b>clear</b> — Clears the event history after reading. |

#### group

|                    |                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>group</b> <i>aa-group-id</i> <b>resources</b>                                                                                                                                                                    |
| <b>Context</b>     | tools>dump>application-assurance                                                                                                                                                                                    |
| <b>Description</b> | This command dumps application-assurance information within a group.                                                                                                                                                |
| <b>Parameters</b>  | <i>aa-group-id</i> — Specifies the AA group identifier.<br><b>Values</b> <i>aa-group-id</i> : partition:aa-group-id[:partition-id]<br>aa-group-id: 1 to 255<br><b>resources</b> — Specifies the AA group resources. |
| <b>Output</b>      | The following output displays group resources information.                                                                                                                                                          |

**Sample Output**

```
*A:Dut-C# tools dump application-assurance group 1 resources
```

```
=====
Application-Assurance Group 1 Resource Usage and Limits
=====
```

```
Partitioned : No
AA-Sub-Scale : residential
Minimum-ISA-Generation : 1
```

```

mda mda-type Status aa-sub aa-sub flow-records ip transit-prefix-entries capacity quarantined
 stats current limit addresses ipv4 v4-rm ipv6 v6-rm cost aa-sub

5/1 isa2-aa up/active 9 162 0 20480 0 0 0 0 9 1
Mda Limit 1024 32768 n/a n/a 16384 0 0 0 0 n/a 100

```

```

Resource Current Limit

Control Certificate Profiles : 0 20
Control DNS IP Cache : 0 128
Control DNS IP Cache Domain Entries : 0 4096
Control DNS IP Cache Entries : 0 65536
Control Event Logs : 0 1
Control Event Log Entries : 0 100000
Control GTP Filter : 0 128
Control HTTP Enrichment : 0 128
Control HTTP Error Redirect : 0 1
Control HTTP Notification : 0 8
Control HTTP Redirect : 0 128
Control IP Prefix Lists : 0 1000
Control IP Prefix Lists Entries : 0 24000
Control SCTP Filter : 0 128
Control Session Filter : 0 300
Control Session Filter Entries : 0 6000
Control URL Filter : 0 4
Control URL List : 0 3
Control URL List Entries (standard) : 0 450
Control URL List Entries (extended) : 0 2000
Control IP Port Lists : 0 100
Control IP Port Lists Entries : 0 3200
Control TCP Validate : 0 128
Control TCP Optimizer : 0 128
Control Multi-path TCP Proxies : 0 4

Policer System Level Single Bucket BW Policers : 0 128
Policer System Level Flow Count Limit Policers : 0 128
Policer System Level Flow Rate Limit Policers : 0 128
Policer Subscriber Level Single Bucket BW Policers : 0 5000
Policer Subscriber Level Dual Bucket BW Policers : 0 5000
Policer Subscriber Level Flow Count Limit : 0 5000
Policer Subscriber Level Flow Rate Limit : 0 5000
Policer All Policer Types For Group : 0 5000
Policer Time-Of-Day Overrides For Group : 0 384

Policy Protocols : 247 -
Policy Custom Protocols : 0 10
Policy Custom Protocol Expressions : 0 10
Policy Charging Groups : 0 32
```

---

|            |                                             |     |      |
|------------|---------------------------------------------|-----|------|
| Policy     | Application Groups                          | : 1 | 32   |
| Policy     | Applications                                | : 1 | 500  |
| Policy     | Application Filters                         | : 0 | 2500 |
| Policy     | Application Filter Expressions              | : 0 | 2500 |
| Policy     | Application Service Options Characteristics | : 0 | 32   |
| Policy     | Application Service Options Values          | : 0 | 256  |
| Policy     | Application Profiles                        | : 0 | 100  |
| Policy     | Application QoS Policies                    | : 0 | 1000 |
| Policy     | AQP ASO Matches                             | : 0 | 2000 |
| Policy     | AQP Subscriber Matches                      | : 0 | 100  |
| Policy     | Subscriber HTTP URL Parameters              | : 0 | -    |
| -----      |                                             |     |      |
| Statistics | Subscriber Statistics                       | : 0 | 512  |
| Statistics | Subscriber Statistics Exported by RADIUS    | : 0 | 64   |
| Statistics | Special Study Protocol Subscribers          | : 0 | 100  |
| Statistics | Special Study Application Subscribers       | : 0 | 100  |

---

## group

|                    |                                                                                |                                                        |            |
|--------------------|--------------------------------------------------------------------------------|--------------------------------------------------------|------------|
| <b>Syntax</b>      | <b>group</b> <i>aa-group-id</i> [: <i>partition-id</i> ]                       |                                                        |            |
| <b>Context</b>     | tools>dump>application-assurance                                               |                                                        |            |
| <b>Description</b> | This command dumps application-assurance information within a group/partition. |                                                        |            |
| <b>Parameters</b>  | <i>aa-group-id</i> — Specifies the AA group identifier.                        |                                                        |            |
|                    | <b>Values</b>                                                                  |                                                        |            |
|                    | <i>aa-group-id</i> :                                                           | partition: <i>aa-group-id</i> [: <i>partition-id</i> ] |            |
|                    |                                                                                | <i>aa-group-id</i>                                     | 1 to 255   |
|                    |                                                                                | <i>partition-id</i>                                    | 1 to 65535 |

## aa-anl-list

|                    |                                                                                                                                                                        |                                                                                                           |  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|--|
| <b>Syntax</b>      | <b>aa-anl-list</b> [ <b>congested-only</b> ] [ <b>sort-type</b> { <b>top-by-subs</b>   <b>top-by-rate</b> }] [ <i>isa mda-id</i> ]<br><b>aa-anl-list summary</b>       |                                                                                                           |  |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                            |                                                                                                           |  |
| <b>Description</b> | This command displays the list of active ANLs detected by AA along with the associated conditions (for example, congestion, measured rate, and number of subscribers). |                                                                                                           |  |
| <b>Parameters</b>  | <b>congested-only</b> — Specifies only congested ANLs.<br><b>sort-type</b> — Filters by the specified sub-type.                                                        |                                                                                                           |  |
|                    | <b>Values</b>                                                                                                                                                          |                                                                                                           |  |
|                    |                                                                                                                                                                        | <b>top-by-subs</b> — Displays the top ANLs sorted by measured ANL bandwidth.                              |  |
|                    |                                                                                                                                                                        | <b>top-by-rate</b> — Displays the top ANLs sorted by those ANLs that have the most number of subscribers. |  |

*mda-id* — Specifies the slot and MDA in the format *slot/mda*.

**Values**      *slot*—1 to 10  
                 *mda*—1 or 2

**summary** — Displays summary information.

**Output**      The following output displays aa-anl-list information.

### Sample Output

```
A:Dut-C# tools dump application-assurance group 120:10 aa-anl-list
=====
Application-Assurance Access Network Location List: Group 120:10, ISA 3/1
=====
Type Location Congestion State Rate (kbps) Subscribers

AP-MAC+VLAN 23:89:be:c2:64:50+1034 RTT Limits Exceeded 21961 113
AP-MAC+VLAN 83:2d:3d:73:c4:9a+4090 RTT Limits Exceeded 15963 86
AP-MAC+VLAN f2:ee:cc:47:71:f7+0034 Not Congested 6147 12
=====
```

## aa-sub

**Syntax**      **aa-sub dsm mac** *mac-address* [**snapshot**]  
                 **aa-sub esm** *sub-ident-string*  
                 **aa-sub esm-mac** *esm-mac-name*  
                 **aa-sub transit** *transit-aasub-name*

**Context**      tools>dump>app-assure>group

**Description**      This command displays AA subscriber information for a specific ISA.

**Parameters**      *esm-mac-name* — Specifies the ESM MAC name; a maximum of 32 characters.  
                 *mac-address* — Specifies the MAC address in xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format.  
                 **snapshot** — Displays snapshot statistics.  
                 *sub-ident-string* — Specifies the AA subscriber identifier string, up to 32 characters.  
                 *transit-aasub-name* — Specifies the AA transit subscriber name, up to 32 characters.

**Output**      The following output display AA subscriber information.

### Sample Output

```
A:Dut-C# tools dump application-assurance group 120:10 aa-
sub dsm mac 00:01:02:00:00:00 summary
=====
Application-Assurance Subscriber Summary (realtime)
=====
```

```
MAC : 00:01:02:00:00:00 (dsm)
ISA assigned : 3/1
Group : 120:10
App-Profile : AppPro1
HTTP URL Parameters : (Not Specified)
Access Network Location : 04:7d:be:fb:64:a8+0243 (Not Congested)
ANL Type : AP-MAC+VLAN
Last HTTP Notified Time : N/A
```

```

Traffic Octets Packets Flows

From subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows 0 0 0
To subscriber:
 Admitted 0 0 0
 Denied 0 0 0
 Active flows 0 0 0
Flow counts:
 Short duration 0 0 0
 Med duration 0 0 0
 Long duration 0 0 0
Total flow duration : 0 seconds
```

```

Application Service Options (ASO)
```

```

Characteristic Value Derived from

Char1 val10 default
=====
```

## aa-sub-list

- Syntax** **aa-sub-list** [**filter-by-type** *sub-type*] [**isa** *mda-id*] **quarantined-only**  
**aa-sub-list** [**filter-by-type** *sub-type*] [**isa** *mda-id*] **policers-exceeded**  
**aa-sub-list summary**
- Context** tools>dump>app-assure>group
- Description** This command displays the AA subscriber list for a specific ISA.
- Parameters** **filter-by-type** *sub-type* — Filters by the specified sub-type.
- Values** dsm, esm, esm-mac, sap, spoke-sdp, transit
- mda-id** — Specifies the slot and MDA in the format *slot/mda*.
- Values** *slot*—1 to 10  
*mda*—1 or 2
- summary** — Displays summary information.
- quarantined-only** — Displays the AA subscribers that are under quarantine.

**policers-exceeded** — Displays subscribers that have exceeded policer resources.

**Output** The following output displays AA subscriber list information.

### Sample Output

```
*A:Dut-C# tools dump application-assurance group 1 aa-sub-list quarantined-only
=====
Application-Assurance Sub List (quarantined): Group 1, ISA 3/1
=====
```

| Type      | AA-Sub<br>(Quarantined Since)              | App Profile<br>(Last Quarantine Event) | Part<br>Id |
|-----------|--------------------------------------------|----------------------------------------|------------|
| esm       | Sub1<br>(01/30/2018 14:25:22)              | app-profile-1<br>(01/30/2018 15:27:3)  | 0          |
| spoke-Sdp | 1000:150<br>(01/30/2018 13:25:22)          | app-profile-2<br>(01/30/2018 16:27:3)  | 0          |
| esm-mac   | Sub3-000102030405<br>(01/30/2018 12:25:22) | app-profile-1<br>(01/30/2018 17:27:3)  | 0          |
| transit   | t1<br>(01/30/2018 11:25:22)                | app-profile-4<br>(01/30/2018 18:27:3)  | 0          |

```

Number of AA Subscribers : 4
```

```
*A:Dut-C# tools dump application-assurance group 1 aa-sub-list summary
=====
Application-Assurance Subscriber Summary for Group 1, ISA 5/2
=====
```

|              | all | esm | sap | spoke-<br>sdp | transit | dsm | esm-mac |
|--------------|-----|-----|-----|---------------|---------|-----|---------|
| Total        | 0   | 0   | 0   | 0             | 0       | 0   | 0       |
| Overrides    | 0   | 0   | 0   | 0             | 0       | 0   | 0       |
| Pol Exceeded | 0   | 0   | 0   | 0             | 0       | 0   | 0       |
| Congested    | 0   | 0   | 0   | 0             | 0       | 0   | 0       |
| Quarantined  | 0   | 0   | 0   | 0             | 0       | 0   | 0       |

```

Total number of aa-subs found : 0
Total number of aa-subs with overrides found : 0
Total number of aa-subs with policer resources exceeded found : 0
Total number of congested aa-subs found : 0
Total number of quarantined aa-subs found : 0
=====
```

## admit-deny-stats

**Syntax** **admit-deny-stats**

**Context** tools>dump>app-assure>group

**Description** This command displays application-assurance admit-deny statistics.

**Output** The following output is an example of AA admit-deny statistics information.

### Sample Output

```
tools dump application-assurance group 1 admit-deny-stats
=====
Application-Assurance Group 1 Admit-Deny Statistics
=====

Packet Validation Statistics
 Admitted Sub-To-Net Denied Sub-To-Net Admitted Net-To-Sub Denied Net-To-Sub
 (Packets) (Packets) (Packets) (Packets)

Error
 0 0 0 0
Fragments: Out-Of-Order
 0 0 0 0
Fragments: All
 0 0 0 0
Overload
 N/A 0 N/A 0

TCP Validation Statistics
 Admitted Sub-To-Net Denied Sub-To-Net Admitted Net-To-Sub Denied Net-To-Sub
 (Packets) (Packets) (Packets) (Packets)

2 0 0 0 0
net 14 1 15 1

```

## app-group

**Syntax** **app-group** [*app-group-name*] **count** [**detail**]

**Context** tools>dump>app-assure>group

**Description** This command displays per-subscriber per-app-group statistics.

## application

**Syntax** **application** [*application-name*] **count** [**detail**]

**Context** tools>dump>app-assure>group

**Description** This command displays per-subscriber per-application statistics.

## charging-group

**Syntax** **charging-group** [*charging-group-name*] **count** [**detail**]

**Context** tools>dump>app-assure>group

**Description** This command displays per-subscriber per-charging-group statistics.

## summary

**Syntax** **summary**

**Context** tools>dump>app-assure>group

**Description** This command displays subscriber summary information.

## aa-sub-search

**Syntax** **aa-sub-search** *search-type granularity* [**direction** *direction*] [**max-count** *max-count*]

**Context** tools>dump>app-assure>group

**Description** This command displays AA aa-sub information.

**Parameters** *search-type* — Specifies the type of search.

**Values** top

*granularity* — Specifies the granularity of the search.

**Values** bytes, packets, flows

**direction** *direction* — Specifies the network/subscriber direction.

**Values** from-sub, to-sub, both

**max-count** *max-count* — Specifies the maximum flows to display.

**Values** 1 to 100

**Output** The following output display AA aa-sub information.

### Sample Output

```
A:Dut-C# tools dump application-assurance group 74 aa-sub-search top bytes
=====
Application-Assurance aa-sub search for Group 74: Top 10 by bytes (both)
=====
Entry isa SubType SubName
 From-sub-count To-sub-count Group:Partition Interval (UTC)
1 3/2 esm-mac "diameter_esm-000100000001"
 40 42 74:40346 "01/13/2017 14:39:18"
2 3/2 esm-mac "diameter_esm-000100000002"
 40 42 74:40346 "01/13/2017 14:39:18"
3 3/2 esm-mac "diameter_esm-000100000003"
 40 42 74:40346 "01/13/2017 14:39:18"
4 3/2 esm-mac "diameter_esm-000100000004"
 40 42 74:40346 "01/13/2017 14:39:18"
```



|    |     |         |                             |                                |
|----|-----|---------|-----------------------------|--------------------------------|
| 5  | 3/2 | esm-mac | "diameter_esm-000100000005" |                                |
|    | 40  |         | 42                          | 74:40346 "01/13/2017 14:39:18" |
| 6  | 3/2 | esm-mac | "diameter_esm-000100000006" |                                |
|    | 40  |         | 42                          | 74:40346 "01/13/2017 14:39:18" |
| 7  | 3/2 | esm-mac | "diameter_esm-000100000007" |                                |
|    | 40  |         | 42                          | 74:40346 "01/13/2017 14:39:18" |
| 8  | 3/2 | esm-mac | "diameter_esm-000100000008" |                                |
|    | 40  |         | 42                          | 74:40346 "01/13/2017 14:39:18" |
| 9  | 3/2 | esm-mac | "diameter_esm-000100000009" |                                |
|    | 40  |         | 42                          | 74:40346 "01/13/2017 14:39:18" |
| 10 | 3/2 | esm-mac | "diameter_esm-00010000000a" |                                |
|    | 40  |         | 42                          | 74:40346 "01/13/2017 14:39:18" |

Total number of aa-subs found: 10

## dns-ip-cache

|                    |                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dns-ip-cache isa mda-id [url file-url]</b>                                                                                                                                                         |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                                                           |
| <b>Description</b> | This command displays the list of IP addresses stored in a DNS IP cache.                                                                                                                              |
| <b>Parameters</b>  | <b>isa mda-id</b> — Specifies the DNS IP cache for a particular ISA-AA card.<br><b>url file-url</b> — Specifies the URL for the file to direct the search output to. The file may be local or remote. |

### Values

|                        |              |                                                                                                                                                        |
|------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| local-url   remote-url | local-url    | [<cflash-id>/][<file-path>]                                                                                                                            |
|                        |              | 200 chars max, including cflash-id<br>directory length 99 chars max each                                                                               |
|                        | remote-url   | [{ftp:// tftp://}<login>:<pswd>@<remote-locn>/<br>][<file-path>]<br>255 chars max<br>directory length 99 chars max each                                |
|                        | remote-locn  | [ <hostname>   <ipv4-address>   <ipv6-address> ]                                                                                                       |
|                        | ipv4-address | a.b.c.d                                                                                                                                                |
|                        | ipv6-address | x:x:x:x:x:x:x[-interface]<br>x:x:x:x:x:x.d.d.d[-interface]<br>x - [0..FFFF]H<br>d - [0..255]D<br>interface - 32 chars max, for link<br>local addresses |
|                        | cflash-id    | flash slot ID                                                                                                                                          |

**Output** Table 25 describes the command output fields.

**Table 25 Tools DNS IP Cache Output Fields**

| Label              | Description                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-address         | Indicates the IP address stored in the DNS IP cache. The address is added into the cache if the DNS response meets the DNS IP cache match criteria (domain name and DNS server address).      |
| creationTime       | Indicates the time at which the entry was created. The entry is created by a DNS response meeting the DNS IP cache match criteria (domain name and DNS server address).                       |
| lastUpdated(UTC)   | Indicates the time at which the entry was last updated, either from a new IP flow (fully classified) using the same IP address or a new DNS response meeting the DNS IP cache match criteria. |
| numDNSResponses    | Indicates the number of DNS responses including this IP address meeting the DNS IP cache match criteria.                                                                                      |
| lastMatchTime(UTC) | Indicates the last time the IP address matched an app-filter with a server address DNS IP cache criteria.                                                                                     |
| numTimesMatched    | Indicates the number of times the IP address matched an app-filter with a server address DNS IP cache.                                                                                        |

### Sample Output

```
*A:7750# tools dump application-assurance group 1 dns-ip-
cache "Default DNS IP Cache"
isa 3/2
=====
Application-Assurance dns-ip-cache "Default DNS IP Cache"
Current Time: "01/21/2015 16:44:00" (UTC)
 group: 1
 isa: 3/2
 admin state: no shutdown
 max-entries: 150
=====
ip-address creationTime (UTC) lastUpdated(sec)
numDNSResponses lastMatchTime(UTC) numTimesMatched
2001:db8:3d40:3::3fa8:3d59 "01/21/2015 16:42:49" 71 5
"01/21/2015 16:42:49" 0
2001:db8:3d40:3::3fa8:3d0b "01/21/2015 16:42:49" 71 1
"01/21/2015 16:42:49" 0
2001:db7:3d40:3::3fa8:3d2b "01/21/2015 16:42:49" 71 1
"01/21/2015 16:42:49" 0
192.168.74.203 "01/21/2015 16:42:36" 84 67
"01/21/2015 16:42:36" 0
192.168.124.91 "01/21/2015 16:42:36" 84 15
"01/21/2015 16:42:36" 0
```

|                         |                          |    |
|-------------------------|--------------------------|----|
| 192.168.124.97          | "01/21/2015 16:42:36" 84 | 15 |
| "01/21/2015 16:42:36" 0 |                          |    |
| 192.168.86.136          | "01/21/2015 16:42:36" 84 | 5  |
| "01/21/2015 16:42:36" 0 |                          |    |
| 192.168.74.176          | "01/21/2015 16:42:36" 84 | 67 |
| "01/21/2015 16:42:36" 0 |                          |    |
| 192.168.86.99           | "01/21/2015 16:42:36" 84 | 11 |
| "01/21/2015 16:42:36" 0 |                          |    |

## event-log

**Syntax** **event-log** *log-event url file-url*  
**event-log** *log-event isa mda-id [url file-url]*

**Context** tools>dump>app-assure>group

**Description** This command displays application-assurance event-log information.

## flow-record-search

**Syntax** **flow-record-search aa-sub** {*esm sub-ident-string* | **sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id* | **transit** *transit-aasub-name* | **mobile** {*imsi imsi-msisdn* | **msisdn** *imsi-msisdn* | **imei** *imei*} **apn** *apn-name* | **dsm** *mac mac-address* | **esm-mac** *esm-mac-name*} [**protocol** *protocol-name*] [**application** *app-name*] [**app-group** *app-group-name*] [**flow-status** *flow-status*] [**start-flowid** *start-flowid*] [**classified** *classified*] [**server-ip** *ip-address*] [**server-port** *port-num*] [**client-ip** *ip-address*] [**bytes-tx** *kbytes*] [**flow-duration** *minutes*] [**max-count** *max-count*] [**search-type** *search-type*] [*url file-url*]

**flow-record-search isa** *mda-id* [**protocol** *protocol-name*] [**application** *app-name*] [**app-group** *app-group-name*] [**flow-status** *flow-status*] [**start-flowid** *start-flowid*] [**classified** *classified*] [**server-ip** *ip-address*] [**server-port** *port-num*] [**client-ip** *ip-address*] [**bytes-tx** *kbytes*] [**flow-duration** *minutes*] [**max-count** *max-count*] [**search-type** *search-type*] [*url file-url*]

**Context** tools>dump>app-assure>group

**Description** This command dumps application-assurance flow-records matching the specified criteria for a specific AA subscriber.

**Parameters** **application** *app-name* — Displays flows for the specified application name.

**app-group** *app-group-name* — Displays flows for the specified application group.

**bytes-tx** *kbytes* — Display flows with the specified minimum kilobytes.

**Values** 0 to 4294967295

**classified** *classified* — Specifies the starting flow ID.

**Values** yes, no

**client-ip** *ip-address* — Display flows with the specified client IP address.

**Values**      *ipv4-address* - a.b.c.d  
                  *ipv6-address* - x:x:x:x:x:x:x (eight 16-bit pieces)

**dsm mac** *mac-address* — Displays flows for the specified subscriber.

**esm sub-ident-string** — Displays flows for the specified subscriber.

**esm-mac** *esm-mac-name* — Displays flows for the specified ESM MAC.

**flow-duration** *minutes* — Display flows with the specified minimum duration in minutes.

**Values**      0 to 4294967295

**flow-status** *flow-status* — Displays only flows that are active or closed.

**Values**      active, closed

**max-count** *max-count* — Specifies the maximum count of flows to display.

**Values**      1 to 4294967295

**protocol** *protocol-name* — Displays flows for the specified protocol.

**sap** *sap-id* — Displays flows for the specified SAP.

**search-type** *search-type* — Specifies the level of detail displayed for flows that match the search criteria.

**Values**      default — Displays some per flow information.  
                  count — Displays the number of matching flows.  
                  detail — Displays all per flow information available.

**server-ip** *ip-address* — Display flows with the specified server IP address.

**Values**      *ipv4-address* - a.b.c.d  
                  *ipv6-address* - x:x:x:x:x:x:x (eight 16-bit pieces)

**server-port** *port-num* — Display flows with the specified server port number.

**Values**      0 to 65535

**spoke-sdp** *sdp-id:vc-id* — Displays flows for the specified spoke SDP.

**start-flowid** *start-flowid* — Specifies the starting flow ID.

**Values**      0 to 4294967295

**transit** *transit-aasub-name* — Displays flows for the specified transit subscriber.

**url** *file-url* — Specifies the URL for the file to direct the search output to. The file may be local or remote.

**Values**

local-url | remote-url

local-url      [<flash-id>]/[<file-path>]  
                  200 chars max, including cflash-id  
                  directory length 99 chars max each

remote-url [{ftp://|tftp://}<login>:<pswd>@<remote-  
locn>/] [<file-path>]  
255 chars max  
directory length 99 chars max each

remote- [ <hostname> | <ipv4-address> | <ipv6-  
locn address> ]

ipv4-address a.b.c.d

ipv6-address x:x:x:x:x:x:x[-interface]  
x:x:x:x:x:d.d.d.d[-  
interface]  
x - [0..FFFF]H  
d - [0..255]D  
interface - 32 chars max, for  
link  
local addresses

cflash-id flash slot ID

**Output** The following example displays flow record search information.

### Sample Output

```
*A:Dut-C# tools dump application-assurance group 74:40346 flow-record-search aa-
sub esm-mac "diameter_esm-000100000002"
=====
Application-Assurance flow record search, Version 1.0
Search Start Time: "01/13/2017 14:30:50" (UTC)
Search Criteria:
 group[:partition]: 74:40346
 aa-sub: diameter_esm-000100000002 (esm-mac)
 protocol name: none specified
 application name: none specified
 app-group name: none specified
 flow-status: none specified
 start-flowId: none specified
 classified: none specified
 server-ip: none specified
 server-port: none specified
 client-ip: none specified
 bytes-tx: none specified
 flow-duration: none specified
 max-count: none specified
 search-type: default
=====
FlowId Init Src-ip Dst-ip Ip-prot Src-prt Dst-prt Protocol
Application Pkts-tx Bytes-tx Pkts-disc Bytes-disc Time-ofp(UTC)
Time-olp(UTC)
124 yes 192.168.200.2 200.1.1.3 icmp 0 0 "non_tcp_udp"
"ICMP" 1 42 0 0 "01/13/2017 14:27:06"
"01/13/2017 14:27:06"
300 no 192.168.200.2 200.1.1.3 icmp 0 0 "non_tcp_udp"
```

```
"ICMP" 1 42 0 0 "01/13/2017 14:27:30"
"01/13/2017 14:27:30"
```

load-balance

|                    |                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>load-balance</b> [ <b>service</b> <i>service-id</i> ]                                                                             |
| <b>Context</b>     | tools>perform>app-assure>group                                                                                                       |
| <b>Description</b> | This command rebalances AA subscribers between ISAs within a group, in case imbalance occurs such as with the addition of new cards. |
| <b>Parameters</b>  | <b>service</b> <i>service-id</i> — Specifies the service                                                                             |
|                    | <b>Values</b> 1 to 2147483648                                                                                                        |

http-host-recorder detail

|                    |                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-host-recorder detail</b> [ <b>isa</b> <i>mda-id</i> ] <b>url</b> <i>file-url</i>                                                                                                                                                                                              |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command saves the http host values recorded by the tool into a file. The http-host-recorder is configured using debug commands.                                                                                                                                                  |
| <b>Parameters</b>  | <b>isa</b> <i>mda-id</i> — Specifies the AA ISA.                                                                                                                                                                                                                                      |
|                    | <b>Values</b> slot 1 to 10, mda 1 to 2                                                                                                                                                                                                                                                |
|                    | <b>url</b> <i>file-url</i> — Specifies the URL for the file to direct the http-host-recorder output to.                                                                                                                                                                               |
|                    | <b>Values</b>                                                                                                                                                                                                                                                                         |
|                    | <b>local-url:</b> <cflash-id>/[<file-path>]<br>200 chars max, including cflash-id<br>directory length 99 chars max each                                                                                                                                                               |
|                    | <b>remote-url:</b> [{ftp:// tftp://}<login>:<pswd>@<remote-locn>]/[<file-path>]<br>255 chars max<br>directory length 99 chars max each                                                                                                                                                |
|                    | <b>remote-locn:</b> <hostname>   <ipv4-address>   <ipv6-address> ]<br>ipv4-address a.b.c.d<br>ipv6-address x:x:x:x:x:x[-interface]<br>x:x:x:x:x:d.d.d.d[-interface]<br>x - [0..FFFF]H<br>d - [0..255]D<br>interface 32 chars max, for link local addresses<br>cflash-id flash slot ID |

## http-host-recorder status

|                    |                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-host-recorder status</b> [ <i>isa mda-id</i> ]                                                                                                                                                                                                                        |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                                                                                                                                   |
| <b>Description</b> | This command displays the current status of the http-host-recorder with current-time, start-time, stop-time, sample-rates, filters, buffer as well as number of bytes and flows recorded for the specified AA ISA. The http-host-recorder is configured using debug commands. |
| <b>Parameters</b>  | <b>isa mda-id</b> — Specifies the AA ISA<br><b>Values</b> slot 1 to 10, mda 1 to 2                                                                                                                                                                                            |

## http-host-recorder top

|                    |                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-host-recorder top</b> <i>granularity</i> [ <b>max-count</b> <i>max-count</i> ] [ <i>isa mda-id</i> ]                                                                                                                                                                                                     |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | This command configures dump application-assurance http-host-recorder information.                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>granularity</i> — Specifies if the output is sorted by bytes or flows.<br><b>Values</b> bytes, flows<br><b>max-count</b> <i>max-count</i> — Specifies the maximum count of flows to display.<br><b>Values</b> 1 to 25<br><i>isa mda-id</i> — Specifies the AA ISA<br><b>Values</b> slot 1 to 10<br>mda 1 to 2 |

## http-host-recorder granularity

|                    |                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-host-recorder top</b> <i>granularity</i> [ <b>max-count</b> <i>max-count</i> ] [ <i>isa mda-id</i> ]                                                                                                                 |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                                                                                  |
| <b>Description</b> | This command displays by bytes or flows top http-host recorded by the tool on a particular AA ISA.                                                                                                                           |
| <b>Parameters</b>  | <i>granularity</i> — Specifies if the output is sorted by bytes or flows.<br><b>Values</b> bytes, flows<br><b>max-count</b> <i>count-value</i> — Specifies the maximum number of values to display.<br><b>Values</b> 1 to 25 |

**isa mda-id** — Specifies the AA ISA  
**Values** slot 1 to 10, mda 1 to 2

policer

**Syntax** **policer** *policer-name* **day** *day* **time** *time-of-day*  
**Context** tools>dump>app-assure>group  
**Description** This command displays rates for the policer for a specific day and time.  
**Parameters** *policer-name* — Specifies an existing policer name up to 256 characters in length.  
**day** *day* — Specifies a day to display policer rates.  
**Values** sunday, monday, tuesday, wednesday, thursday, friday, saturday  
**time** *time-of-day* — Specifies a time of day (in hours and minutes) to display policer rates.  
**Values** hh : 0 to 24  
mm : 0, 15, 30, 45

port-recorder detail

**Syntax** **port-recorder detail** [**flow-count** *flows*] [**byte-count** *kbytes*] [**isa mda-id**] **url** *file-url*  
**Context** tools>dump>app-assure>group  
**Description** This command saves the port recorded by the tool into a file. The port-recorder is configured using debug commands.  
**Parameters** **flow-count** *flows* — Match ports with flow count greater than the specified value.  
**Values** slot 1 to 4294967295  
**bytes-count** *kbytes* — Match ports with bytes count greater than the specified value.  
**Values** slot 1 to 4294967295  
**isa mda-id** — Specifies the AA ISA  
**Values** slot 1 to 10, mda 1 to 2  
**url** *file-url* — Specifies the URL for the file to direct the port-recorder output to.  
**Values**  
**local-url:** <cflash-id>/[<file-path>]  
200 chars max, including cflash-id  
directory length 99 chars max each



|                     |                                                              |                                        |  |
|---------------------|--------------------------------------------------------------|----------------------------------------|--|
| <b>remote-url:</b>  | [{ftp:// tftp://}<login>:<pswd>@<remote-locn>/][<file-path>] |                                        |  |
|                     | 255 chars max                                                |                                        |  |
|                     | directory length 99 chars max each                           |                                        |  |
| <b>remote-locn:</b> | <hostname>   <ipv4-address>   <ipv6-address> ]               |                                        |  |
|                     | ipv4-address                                                 | a.b.c.d                                |  |
|                     | ipv6-address                                                 | x:x:x:x:x:x:x[-interface]              |  |
|                     |                                                              | x:x:x:x:x:x:d.d.d.d[-interface]        |  |
|                     |                                                              | x - [0..FFFF]H                         |  |
|                     |                                                              | d - [0..255]D                          |  |
|                     | interface                                                    | 32 chars max, for link local addresses |  |
|                     | cflash-id                                                    | flash slot ID                          |  |

port-recorder status

|                    |                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>port-recorder status</b> [ <i>isa mda-id</i> ]                                                                                                                                                                                                                     |
| <b>Context</b>     | tools>dump>app-assure>group                                                                                                                                                                                                                                           |
| <b>Description</b> | This command displays the current status of the port-recorder with current-time, start-time, stop-time, sample-rates as well as number of bytes and flows for UDP and TCP traffic on the specified AA ISA card. The port-recorder is configured using debug commands. |
| <b>Parameters</b>  | <b>isa mda-id</b> — Specifies the AA ISA                                                                                                                                                                                                                              |
|                    | <b>Values</b> slot 1 to 10, mda 1 to 2                                                                                                                                                                                                                                |

port-recorder top

|                    |                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>port-recorder top</b> <i>granularity</i> [ <b>max-count</b> <i>max-count</i> ] [ <b>isa mda-id</b> ] |
| <b>Context</b>     | tools>dump>app-assure>group                                                                             |
| <b>Description</b> | This command displays by bytes or flows the top ports recorded by the tool on a particular AA ISA.      |
| <b>Parameters</b>  | <b>granularity</b> — Specifies if the output is sorted by bytes or flows.                               |
|                    | <b>Values</b> bytes, flows                                                                              |
|                    | <b>max-count</b> <i>count-value</i> — Specifies the maximum number of values to display.                |
|                    | <b>Values</b> 1 to 25                                                                                   |
|                    | <b>isa mda-id</b> — Specifies the AA ISA                                                                |
|                    | <b>Values</b> slot 1 to 10, mda 1 to 2                                                                  |

---

## traffic-capture

|                    |                                                                                    |
|--------------------|------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>traffic-capture detail url</b> <i>file-url</i><br><b>traffic-capture status</b> |
| <b>Context</b>     | tools>dump>app-assure>group                                                        |
| <b>Description</b> | This command displays application-assurance traffic-capture information.           |

## aarp

|                    |                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>aarp aarpld force-evaluate</b>                                                                                                                                                   |
| <b>Context</b>     | tools>perform>app-assure                                                                                                                                                            |
| <b>Description</b> | This command performs Application Assurance Redundancy Protocol instance operations.                                                                                                |
| <b>Parameters</b>  | <b>aarpld</b> — Specifies an integer that identifies an AARP instance<br><b>Values</b> 1 to 65535<br><b>force-evaluate</b> — Forces a re-evaluation of the preferred AARP instance. |

## group

|                    |                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>group aa-group-id load-balance</b> [ <b>service</b> <i>service-id</i> ]                                                                                                                                                                                                                            |
| <b>Context</b>     | tools>perform>app-assure                                                                                                                                                                                                                                                                              |
| <b>Description</b> | This command performs application assurance group operations.                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <b>aa-group-id</b> — Specifies the application assurance group ID.<br><b>Values</b> 1 to 255<br><b>load-balance</b> — Load balances subscribers within the group.<br><b>service service-id</b> — Load balances the specified service.<br><b>Values</b> 1 to 2148278381, svc-name (up to 64 char max.) |

## aa-sub

|               |                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>aa-sub esm</b> <i>sub-ident-string</i><br><b>aa-sub esm-mac</b> <i>esm-mac-name</i><br><b>aa-sub sap</b> <i>sap-id</i><br><b>aa-sub spoke-id</b> <i>sdp-id:vc-id</i><br><b>aa-sub transit</b> <i>transit-aasub-name</i> |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | tools>perform>app-assure>group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command performs application assurance group aa-sub operations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <p><b>esm</b> <i>sub-ident-string</i> — Specifies an existing subscriber identification string.</p> <p><b>esm-mac</b> <i>esm-mac-name</i> — Specifies an existing subscriber MAC.</p> <p><b>sap</b> <i>sap-id</i> — Specifies the physical port identifier portion of the SAP definition.</p> <p><b>spoke-id</b> <i>sdp-id:vc-id</i> — Specifies the spoke SDP ID and VC ID.</p> <p><b>Values</b>      1 to 17407<br/>                  1 to 4294967295</p> <p><b>transit</b> <i>transit-aasub-name</i> — Specifies an existing transit subscriber name string up to 32 characters in length.</p> |

## clear-quarantine

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>clear-quarantine</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | tools>perform>app-assure>group>aa-sub                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | This command clears the specified AA subscriber from the quarantine state. If the specified AA subscriber is not in a quarantined state, an error message is generated. When this command is successfully executed, an SNMP trap is raised indicating that the AA-subscriber is no longer quarantined. If the quarantine table is full and the automatic detection algorithm identifies a new subscriber to be quarantined, the oldest quarantined AA subscriber is removed, a trap is raised and the newly identified AA subscriber is quarantined. |

## quarantine

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>quarantine</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | tools>perform>app-assure>group>aa-sub                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command places the specified AA subscriber into the quarantine state. If the specified AA subscriber is already in a quarantined state, an error message is generated. If the quarantine table is full, the command generates an error message when the user tries to manually quarantine an AA subscriber. The user can manually <b>clear-quarantine</b> any quarantined AA subscriber to make space for the new AA subscriber. When this command is successfully executed, an SNMP trap is raised indicating that the AA-subscriber is now quarantined. |

## seen-ip

|               |                                                      |
|---------------|------------------------------------------------------|
| <b>Syntax</b> | <b>seen-ip transit-ip-policy</b> <i>ip-policy-id</i> |
|---------------|------------------------------------------------------|

**seen-ip transit-ip-policy *ip-policy-id* clear**

|                    |                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------|
| <b>Context</b>     | tools>dump>app-assure                                                                           |
| <b>Description</b> | This command dumps application-assurance seen-ip information for a specified transit-ip policy. |
| <b>Parameters</b>  | <i>ip-policy-id</i> — An integer that identifies a transit IP profile entry.                    |
|                    | <b>Values</b> 1 to 65535                                                                        |
|                    | <b>clear</b> — Clears the seen IP information after reading.                                    |

### 3.5.2.3 Clear Commands

#### group

|                    |                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>group <i>aa-group-id</i> cflowd</b><br><b>group <i>aa-group-id</i> event-log</b><br><b>group <i>aa-group-id</i> statistics</b><br><b>group <i>aa-group-id</i> status</b><br><b>group <i>aa-group-id</i> [:partition] gtp</b>                                                                                                                            |
| <b>Context</b>     | clear>app-assure                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command clears application assurance group statistics or status.                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <i>aa-group-id</i> — Clears data for the specified AA ISA group.<br><b>cflowd</b> — Clears application assurance cflowd statistics.<br><b>event-log</b> — Clears application assurance event log.<br><b>statistics</b> — Clears application assurance system and subscriber statistics.<br><b>status</b> — Clears application assurance status statistics. |

#### radius-accounting-policy

|                    |                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>radius-accounting-policy <i>rad-acct-plcy-name</i> [server <i>server-index</i>] statistics</b>                                            |
| <b>Context</b>     | clear>app-assure                                                                                                                             |
| <b>Description</b> | This command clears application assurance RADIUS accounting statistics for the specified policy.                                             |
| <b>Parameters</b>  | <i>policy-name</i> — The name of the policy. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces. |

*server-index* — The index for the RADIUS server.

**Values**      1 to 5 (a maximum of 5 accounting servers)

### 3.5.2.4    Debug Commands

#### group

**Syntax**      **group** *aa-group-id[:partition-id]*

**Context**      debug>app-assure

**Description**    This command configures application-assurance within a group/partition debugging.

**Parameters**    *aa-group-id[:partition-id]* — Specifies the existing application assurance group and partition id.

**Values**

|                           |                                     |
|---------------------------|-------------------------------------|
| <i>aa-group-id:parti*</i> | : <i>aa-group-id[:partition-id]</i> |
| <i>aa-group-id</i>        | [1..255]                            |
| <i>partition-id</i>       | [1..65535]                          |

#### traffic-capture

**Syntax**      [no] **traffic-capture**

**Context**      debug>app-assure>group

**Description**    This command configures debugging for traffic capture.

#### match

**Syntax**      [no] **match**

**Context**      debug>app-assure>group>traffic-capture

**Description**    This command configures debugging for traffic match criteria.

#### application

**Syntax**      **application** {**eq** | **neq**} *application-name*  
**no application**

---

|                    |                                                      |
|--------------------|------------------------------------------------------|
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match         |
| <b>Description</b> | This command configures debugging on an application. |

## client-ip

|                    |                                                                      |
|--------------------|----------------------------------------------------------------------|
| <b>Syntax</b>      | <b>client-ip {eq   neq} <i>ip-address</i></b><br><b>no client-ip</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                         |
| <b>Description</b> | This command configures debugging of a client IP.                    |

## client-port

|                    |                                                                        |
|--------------------|------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>client-port {eq   neq} <i>port-num</i></b><br><b>no client-port</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                           |
| <b>Description</b> | This command configures debugging of a client port.                    |

## dst-ip

|                    |                                                                |
|--------------------|----------------------------------------------------------------|
| <b>Syntax</b>      | <b>dst-ip {eq   neq} <i>ip-address</i></b><br><b>no dst-ip</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                   |
| <b>Description</b> | This command configures debugging on a destination IP address. |

## dst-port

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dst-port {eq   neq} <i>port-num</i></b><br><b>no dst-port</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                     |
| <b>Description</b> | This command configures debugging on a destination port.         |

## ip-addr1

|               |                                              |
|---------------|----------------------------------------------|
| <b>Syntax</b> | <b>ip-addr1 {eq   neq} <i>ip-address</i></b> |
|---------------|----------------------------------------------|

---

**no ip-addr1**

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match       |
| <b>Description</b> | This command configures debugging on IP address 1. |

**ip-addr2**

|                    |                                                                    |
|--------------------|--------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-addr2 {eq   neq} <i>ip-address</i></b><br><b>no ip-addr2</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                       |
| <b>Description</b> | This command configures debugging on IP address 2.                 |

**ip-protocol-num**

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-protocol-num {eq   neq} <i>protocol-id</i></b><br><b>no ip-protocol-num</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                                      |
| <b>Description</b> | This command configures debugging on an IP protocol number.                       |

**port1**

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>Syntax</b>      | <b>port1 {eq   neq} <i>port-num</i></b><br><b>no port1</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match               |
| <b>Description</b> | This command configures debugging on port 1.               |

**port2**

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>Syntax</b>      | <b>port2 {eq   neq} <i>port-num</i></b><br><b>no port2</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match               |
| <b>Description</b> | This command configures debugging on port 2.               |

## server-ip

|                    |                                                                      |
|--------------------|----------------------------------------------------------------------|
| <b>Syntax</b>      | <b>server-ip</b> {eq   neq} <i>ip-address</i><br><b>no server-ip</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                         |
| <b>Description</b> | This command configures debugging on a server IP address.            |

## server-port

|                    |                                                                        |
|--------------------|------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>server-port</b> {eq   neq} <i>port-num</i><br><b>no server-port</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                           |
| <b>Description</b> | This command configures debugging on a server port.                    |

## src-ip

|                    |                                                                |
|--------------------|----------------------------------------------------------------|
| <b>Syntax</b>      | <b>src-ip</b> {eq   neq} <i>ip-address</i><br><b>no src-ip</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                   |
| <b>Description</b> | This command configures debugging on a source IP address.      |

## src-port

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>src-port</b> {eq   neq} <i>port-num</i><br><b>no src-port</b> |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match                     |
| <b>Description</b> | This command configures debugging on a source port.              |

## mirror-source

|                    |                                                       |
|--------------------|-------------------------------------------------------|
| <b>Syntax</b>      | [no] <b>mirror-source</b> <i>service-id</i>           |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>match          |
| <b>Description</b> | This command configures debugging on a mirror source. |



## record

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>record</b>                                      |
| <b>Context</b>     | debug>app-assure>group>traffic-capture             |
| <b>Description</b> | This command configures traffic recording options. |

## cut-through-packets

|                    |                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>cut-through-packets</b> <i>cut-through-packets</i>                                                                                                 |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>record                                                                                                         |
| <b>Description</b> | This command records cut-through packet conditions.                                                                                                   |
| <b>Parameters</b>  | <i>cut-through-packets</i> — Indicates whether to capture cut-through only packets or cut-through and other packets, or to exclude them all together. |
| <b>Values</b>      | exclude, include, only                                                                                                                                |
| <b>Default</b>     | include                                                                                                                                               |

## limit

|                    |                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>limit</b> { <b>all-packet-matches</b>   <b>first-session-match</b> }                                                                                            |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>record                                                                                                                      |
| <b>Description</b> | This command records limit conditions.                                                                                                                             |
| <b>Parameters</b>  | <b>all-packet-matches</b> — Records all the packets matching the condition.<br><b>first-session-match</b> — Records only the first session matching the condition. |

## start

|                    |                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>start</b> { <b>immediate</b>   <b>on-new-session</b> }                                                                                                               |
| <b>Context</b>     | debug>app-assure>group>traffic-capture>record                                                                                                                           |
| <b>Description</b> | This command records limit conditions.                                                                                                                                  |
| <b>Parameters</b>  | <b>immediate</b> — Start recording immediately for new or existing flows or sessions.<br><b>on-new-session</b> — Only start recording record for new flows or sessions. |

---

## shutdown

|                    |                                                         |
|--------------------|---------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                    |
| <b>Context</b>     | debug>app-assur>group>traffic-capture                   |
| <b>Description</b> | This command administratively disables traffic capture. |

## isa-aa-group

|                    |                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>isa-aa-group</b> <i>aa-group-id</i> { <b>all</b>   <b>unknown</b> }<br><b>no isa-aa-group</b> <i>aa-group-id</i>                                                                                                                                                                                                                          |
| <b>Context</b>     | debug>mirror-source                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command configures an AA ISA group as a mirror source for this mirror service. Traffic is mirrored after AA processing takes place on AA ISAs of the group, therefore, any packets dropped as part of that AA processing are not mirrored.                                                                                              |
| <b>Parameters</b>  | <b>all</b> — Specifies that all traffic after AA processing will be mirrored.<br><b>unknown</b> — Specifies that all traffic during the identification phase (may match policy entry or entries that have mirror action configured) and traffic that had been identified as unknown_tcp or unknown_udp after AA processing will be mirrored. |

## persistence

|                    |                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>persistence</b> [ <i>persistence-client</i> ]<br><b>no persistence</b>                                                                                 |
| <b>Context</b>     | debug>system                                                                                                                                              |
| <b>Description</b> | This command displays persistence debug information.                                                                                                      |
| <b>Parameters</b>  | <i>persistence-client</i> — Use the <b>application-assurance</b> keyword to display persistence debug information.<br><b>Values</b> application-assurance |

## http-host-recorder

|                    |                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] http-host-recorder</b>                                                                                                                                     |
| <b>Context</b>     | debug>app-assur>group                                                                                                                                              |
| <b>Description</b> | This command enables the http-host-recorder feature on a particular group:partition.<br>The <b>no</b> form of the command disables the http-host-recorder feature. |

## filter

|                    |                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>filter</b>                                                                                                                        |
| <b>Context</b>     | debug>app-assur>group>http-host-recorder                                                                                             |
| <b>Description</b> | This command configures recorder filter settings. This command specifies the filtering parameter for the http-host-recorder feature. |

## default-filter-action

|                    |                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-filter-action</b> <i>default-action</i>                                                                                                                                               |
| <b>Context</b>     | debug>app-assur>group>http-host-recorder>filter                                                                                                                                                  |
| <b>Description</b> | This command configures the recorder filter default action to either record or no-record. This parameter applies to http-host values not matching any expressions defined in the filter context. |
| <b>Parameters</b>  | <i>default-action</i> — Specifies the default action.<br><b>Values</b> record, no-record                                                                                                         |

## expression

|                    |                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>expression</b> <i>expr-index</i> <i>expr-type</i> <b>eq</b> <i>expr-string</i> { <b>record</b>   <b>no-record</b> }<br><b>no expression</b> <i>expr-index</i>                                                                                                                                   |
| <b>Context</b>     | debug>app-assur>group>http-host-recorder>filter                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command configures the recorder filter expressions.                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>expr-index</i> — Specifies the expression index value.<br><b>Values</b> 1 to 4<br><i>expr-type</i> — Specifies the expression type.<br><b>Values</b> http-host<br><i>expr-string</i> — Specifies the HTTP host filter expression string.<br><b>Values</b> format *<expression>\$ (33 chars max) |

## record

|                |                                                                             |
|----------------|-----------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>record</b> { <b>all-hosts</b>   <b>http-host-app-filter-candidates</b> } |
| <b>Context</b> | debug>app-assur>group>http-host-recorder>filter                             |

**Description** This command configures which http-host are selected for the http-host-recorder. It is either any http-host values going through the AA ISA or the http-host corresponding to flows not matching a string based app-filter.

For the feature to work it is required to configure at least one app-filter to catch the HTTP protocol signature.

**Parameters** **all-hosts | http-host-app-filter-candidates** — Specifies which hosts the recorder will record

**Values** all-hosts, http-host-app-filter-candidates

**Default** http-host-app-filter-candidates

## rate

**Syntax** **rate** *sample-rate*  
**no rate**

**Context** debug>app-assure>group>http-host-recorder  
debug>app-assure>group>port-recorder

**Description** This command configures the sampling rate for the recorded http host, a sampling rate of 10 will sample one out of 10 http-host.

**Parameters** *sample-rate* — Specifies the sample rate.

**Values** 1 to 10000

**Default** 100

**Output** The following configuration records http-host entries ending with “.com” as a result of the expression filter configuration. It will not record any other HTTP host values since the default-filter-action set to no-record. The http-host entries analyzed by the recorder in the first place are http-host-app-filter-candidates.

### Sample Output

```
7750# show debug
debug
 application-assurance
 group 1:1
 http-host-recorder
 filter
 default-filter-action no-record
 expression 1 http-host eq "*.com$" record
 record http-host-app-filter-candidates
 exit
 rate 100
 no shutdown
 exit
 exit
exit
```

---

exit

## shutdown

|                    |                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                        |
| <b>Context</b>     | debug>app-assure>group>http-host-recorder<br>debug>app-assure>group>port-recorder                                                           |
| <b>Description</b> | This commands allows to stop or start the http-host-recorder. To reset the recorded values execute shutdown followed by <b>no</b> shutdown. |

## port-recorder

|                    |                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] port-recorder</b>                                                                                                                   |
| <b>Context</b>     | debug>app-assure>group                                                                                                                      |
| <b>Description</b> | This commands allows to stop or start the http-host-recorder. To reset the recorded values execute shutdown followed by <b>no</b> shutdown. |

## application

|                    |                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] application <i>application-name</i></b>                                                                                                                              |
| <b>Context</b>     | debug>app-assure>group>port-recorder                                                                                                                                         |
| <b>Description</b> | This commands specifies the applications used as input by the port-recorder. Applications responsible for unknown or unidentified traffic are meant to be used by this tool. |
| <b>Output</b>      | The following sample configuration records TCP and UDP port numbers for the application "Unidentified TCP".                                                                  |

### Sample Output

```
7750# show debug
debug
 application-assurance
 group 1:1
 port-recorder
 application "Unidentified TCP"
 rate 100
 no shutdown
 exit
 exit
 exit
exit
```



## 4 IP Tunnels

### 4.1 IP Tunnels Overview

This section discusses IP Security (IPsec), GRE tunneling, and IP-IP tunneling features supported by the MS-ISA. In these applications, the MS-ISA/MS-ISA2 functions as a resource module for the system, providing encapsulation and (for IPsec) encryption functions. The IPsec encryption functions provided by the ISA are applicable for many applications including mobile backhaul, encrypted SDPs, video wholesale, site-to-site encrypted tunnel, and remote access VPN concentration.

Figure 37 shows an example of an IPsec deployment, and the way this would be supported inside a 7750 SR. GRE and IP-IP tunnel deployments are very similar. IP tunnels have two flavors GRE/IP-IP, in all but a few area the information for IP Tunnels applies to both types.

**Figure 37 7750 SR IPsec Implementation Architecture**

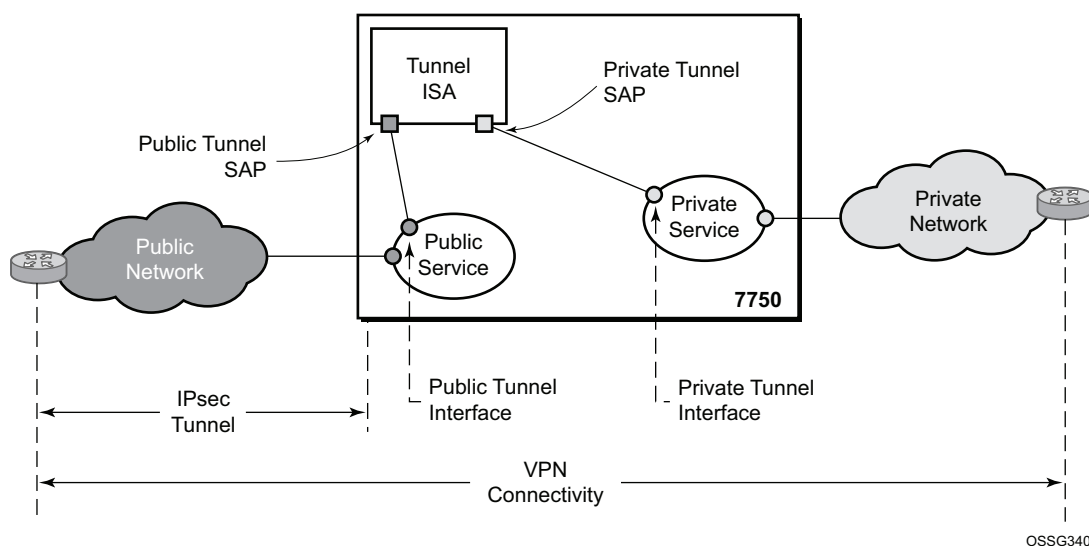


Figure 37, the public network is typically an “insecure network” (for example, the public Internet) over which packets belonging to the private network in the diagram cannot be transmitted natively. Inside the 7750 SR, a public service instance (IES or VPRN) connects to the public network and a private service instance (typically a VPRN) connects to the private network.

The public and private services are typically two different services, and the ISA is the only “bridge” between the two. Traffic from the public network may need to be authenticated and encrypted inside an IPsec tunnel to reach the private network. In this way, the authenticity/confidentiality/integrity of accessing the private network can be enforced. If authentication and confidentiality are not important then access to the private network may alternatively be provided through GRE or IP-IP tunnels.

The ISA provides a variety of encryption features required to establish bi-directional IPsec tunnels including:

Control Plane:

- Manual Keying
- Dynamic Keying: IKEv1/v2
- IKEv1 Mode: Main and Aggressive
- Authentication: Pre-Shared-Key /xauth with RADIUS support/X.509v3 Certificate/EAP
- Perfect Forward Secrecy (PFS)
- DPD
- NAT-Traversal
- Security Policy
- DH-Group: 1/2/5/14/15/19/20/21

Data Plane:

- ESP (with authentication) Tunnel mode
- Authentication Algorithm: MD5/SHA1/SHA256/SHA384/SHA512/AES-XCBC
- Encryption Algorithm: DES/3DES/AES128/AES192/AES256/AES-GCM128/AES-GCM192/AES-GCM256/AES-GMAC128/AES-GMAC192/AES-GMAC256
- Anti-Replay Protection
- N:M IPsec ISA card redundancy

SR OS will use a configured authentication algorithm for Pseudorandom Function (PRF). IPsec features are supported on the 7750 SR, the 7450 ESS running in mixed mode, and VSR.

There are two types of tunnel interfaces and SAPs:

- Public tunnel interface: configured in the public service; outgoing tunnel packets have a source IP address in this subnet
- Public tunnel SAP: associated with the public tunnel interface; a logical access point to the ISA card in the public service



- Private tunnel interface: configured in the private service; can be used to define the subnet for remote access IPsec clients.
- Private tunnel SAP: associated with the private tunnel interface, a logical access point to the ISA card in the private service

Traffic flows to and through the ISA card as follows:

- In the upstream direction, the encapsulated (and possibly encrypted) traffic is forwarded to a public tunnel interface if its destination address matches the local or gateway address of an IPsec tunnel or the source address of a GRE or IP-IP tunnel. Inside the ISA card, encrypted traffic is decrypted, the tunnel header is removed, the payload IP packet is delivered to the private service, and from there, the traffic is forwarded again based on the destination address of the payload IP packet.
- In the downstream direction, unencapsulated/clear traffic belonging to the private service is forwarded into the tunnel by matching a route with the IPsec/GRE/IP-IP tunnel as next-hop. The route can be configured statically, learned by running OSPF on the private tunnel interface (GRE tunnels only), learned by running BGP over the tunnel (IPsec and GRE tunnels only), or learned dynamically during IKE negotiation (IPsec only). After clear traffic is forwarded to the ISA card, it is encrypted if required, encapsulated per the tunnel type, delivered to the public service, and from there, the traffic is forwarded again based on the destination address of the tunnel header.

## 4.1.1 Tunnel ISAs

A tunnel-group is a collection of ISAs (each having mda-type **isa-tunnel**) or MS-ISA2s (mda-type **isa2-tunnel**) configured to handle the termination of one or more IPsec, GRE and/or IP-IP tunnels. Two example tunnel-group configurations are shown below:

```
config isa
 tunnel-group 1 create
 primary 1/1
 backup 2/1
 no shutdown
 exit
```

```
config isa
 tunnel-group 2 create
 multi-active
 mda 3/1
 mda 3/2
 no shutdown
```

A GRE, IP-IP, or IPsec tunnel belongs to only one tunnel group. There are two types of tunnel groups:

- A single-active tunnel-group can have one tunnel-ISA designated as primary and optionally one other tunnel-ISA designated as backup. If the primary ISA fails the affected failed tunnels are re-established on the backup (which is effectively a cold standby) if it is not already in use as a backup for another tunnel-group.
- A multi-active tunnel-group can have multiple tunnel-ISAs designated as primary. This is only supported on the 7750 SR-7/SR-12/SR-12E/c-12/SR-1e/SR-2e/SR-3e, 7450 ESS in mixed mode, or the VSR. Only one ISA is supported on VSR.

The **show isa tunnel-group** command allows the operator to view information about all configured tunnel groups. This command displays the following information for each tunnel-group: group ID, primary tunnel-ISAs, backup tunnel-ISAs, active tunnel-ISAs, admin state and oper state.

There are three thresholds that are used to monitor memory usage in a tunnel ISA:

- max-threshold: when the memory usage of an ISA exceeds this threshold, any new IKE states will be rejected
- high-watermark: when the memory usage of an ISA exceed this threshold, a trap will be generated
- low-watermark: when the memory usage of an ISA fall below this threshold, a clear trap will be generated

These three thresholds are fixed, not configurable.

A tunnel-group has an **isa-scale-mode**, which defines the maximum number of all tunnels (all types combined) which can be established on each ISA of the tunnel group. This is currently fixed at 32,000 tunnels per ISA. This value is different on vSR and vSIM, refer to the corresponding User Guides for details.

#### 4.1.1.1 Public Tunnel SAPs

A VPRN or IES service (the delivery service) must have at least one IP interface associated with a public tunnel SAP to receive and process the following types of packets associated with GRE, IP-IP and IPsec tunnels:

- GRE (IP protocol 47)
- IP-IP (IP protocol 4)
- IPsec ESP (IP protocol 50)

- IKE (UDP)

The public tunnel SAP type has the format **tunnel-tunnel-group.public:index**, as shown in the following CLI example.

```
*A:Dut-C>config>service# info

customer 1 create
 description "Default customer"
exit
ies 1 customer 1 create
 interface "public" create
 address 192.168.12.1/24
 tos-marking-state untrusted
 sap tunnel-1.public:200 create
 exit
 exit
 no shutdown
exit
vprn 2 customer 1 create
 route-distinguisher 10.1.1.1:65007
 interface "greTunnel" tunnel create
 address 10.0.0.1/24
 dhcp
 no shutdown
 exit
 sap tunnel-1.private:210 create
 ip-tunnel "toCel" create
 dest-ip 10.0.0.2
 gre-header
 source 10.251.12.88
 remote-ip 10.251.12.2
 backup-remote-ip 10.251.12.22
 delivery-service 1
 no shutdown
 exit
 exit
 no shutdown
exit

*A:Dut-C>config>service#
```

#### 4.1.1.2 Private Tunnel SAPs

The private service must have an IP interface to a GRE, IP-IP, or IPsec tunnel in order to forward IP packets into the tunnel, causing them to be encapsulated (and possibly encrypted) per the tunnel configuration and to receive IP packets from the tunnel after the encapsulation has been removed (and decryption). That IP interface is associated with a private tunnel SAP.

The private tunnel SAP has the format **tunnel-tunnel-group.private:index**, as shown in the following CLI example where a GRE tunnel is configured under the SAP.

```
*A:Dut-A# show ip tunnel
=====
IP Tunnels
=====
TunnelName SapId SvcId Admn
Local Address DlvrySvcId Oper
OperRemoteAddress

tun-1-gre-tunnel tunnel-1.private:1 201 Up
192.168.1.2 1201 Up
192.168.3.2

IP Tunnels: 1
=====
```

4.1.1.3 IP Interface Configuration

In the configuration example of the previous section the IP address 10.0.0.1 is the address of the GRE tunnel endpoint from the perspective of payload IP packets. This address belongs to the address space of the VPRN 1 service and will not be exposed to the public IP network carrying the GRE encapsulated packets. An IP interface associated with a private tunnel SAP does not support unnumbered operation.

It is possible to configure the IP MTU (M) of a private tunnel SAP interface. This sets the maximum payload IP packet size (including IP header) that can be sent into the tunnel – for example, it applies to the packet size before the tunnel encapsulation is added. When a payload IPv4 packet that needs to be forwarded into the tunnel is larger than M bytes the payload packet is IP fragmented (prior to tunnel encapsulation) if the DF bit is clear, otherwise the packet is discarded. When a payload IPv6 packet that needs to be forwarded into the tunnel is larger than M bytes the packet is discarded if its size is less than 1280 bytes otherwise it is forwarded and encapsulated intact.

#### 4.1.1.4 GRE and IP-IP Tunnel Configuration

To bind an IP/GRE or IP-IP tunnel to a private tunnel SAP, the **ip-tunnel** command should be added under the SAP. To configure the tunnel as an IP/GRE tunnel, the **gre-header** command must be present in the configuration of the **ip-tunnel**. To configure the tunnel as an IP-IP tunnel, the **ip-tunnel** configuration should have the **no gre-header** command. When configuring a GRE or IP-IP tunnel, the **dest-ip** command specifies an IPv4 or IPv6 address (private) of the remote tunnel endpoint. A tunnel can have up to 16 dest-ip addresses. If any of the dest-ip addresses are not contained by a subnet of the local private endpoint then the tunnel will not come up. In the CLI sub-tree under **ip-tunnel**, there are commands to configure the following:

- The source address of the GRE or IP-IP tunnel- This is the source IPv4 address of GRE or IP-IP encapsulated packets sent by the delivery service. It must be an address in the subnet of the associated public tunnel SAP interface.
- The remote IP address - If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE or IP-IP encapsulated packets sent by the delivery service.
- The backup remote IP address- If the remote IP address of the tunnel is not reachable then this is the destination IPv4 address of GRE or IP-IP encapsulated packets sent by the delivery service.
- The delivery service- This is the id or name of the IES or VPRN service where GRE or IP-IP encapsulated packets are injected and terminated. The delivery service can be the same service where the private tunnel SAP interface resides.
- The DSCP marking in the outer IP header of GRE encapsulated packets- If this is not configured then the default is to copy the DSCP from the inner IP header to the outer IP header.

A private tunnel SAP can have only one ip-tunnel sub-object (one GRE or IP-IP tunnel per SAP).

The **show ip tunnel** command displays information about a specific IP tunnel or all configured IP tunnels. The following information is provided for each tunnel:

- service ID that owns the tunnel
- private tunnel SAP that owns the tunnel
- tunnel name, source address
- remote IP address
- backup remote IP address
- local (private) address
- destination (private) address
- delivery service

- dscp
- admin state
- oper state
- type (GRE or IP-IP)

The following is an example of the output of the **show ip tunnel <tunnel-name>** command.

```
A:config>service>vprn>if>sap>ip-tunnel# show ip tunnel "ipv6-gre"
=====
IP Tunnel Configuration Detail
=====
Service Id : 1 Sap Id : tunnel-1.private:1
Tunnel Name : ipv6-gre
Description : None
GRE Header : Yes Delivery Service : 2
GRE Keys Set : False
GRE Send Key : N/A GRE Receive Key : N/A
Admin State : Up Oper State : Up
Source Address : 2001:db8::1:2:3:4
Remote Address : 3ffe:1::2
Backup Address : (Not Specified)
Oper Remote Addr : 3ffe:1::2
DSCP : ef
Reassembly : inherit
Clear DF Bit : false IP MTU : max
Encap IP MTU : 1400
Pkt Too Big : true
Pkt Too Big Numb*: 100 Pkt Too Big Intvl: 10 secs
Oper Flags : None
Last Oper Changed: 02/09/2015 15:22:38
Host MDA : 1/2

Target Address Table

Destination IP IP Resolved Status

172.16.1.2 Yes
2001:db8::2 Yes

=====
IP Tunnel Statistics: ipv6-gre
=====
Errors Rx : 0 Errors Tx : 0
Pkts Rx : 0 Pkts Tx : 0
Bytes Rx : 0 Bytes Tx : 0
Key Ignored Rx : 0 Too Big Tx : 0
Seq Ignored Rx : 0
Vers Unsup. Rx : 0
Invalid Chksum Rx : 0
Key Mismatch Rx : 0
=====
=====
```

```
Fragmentation Statistics
=====
Encapsulation Overhead : 44
Pre-Encapsulation
 Fragmentation Count : 0
 Last Fragmented Packet Size : 0
Post-Encapsulation
 Fragmentation Count : 0
 Last Fragmented Packet Size : 0
=====
=====
```

#### 4.1.1.5 IP Fragmentation and Reassembly for IP Tunnels

An IPsec, GRE or IP-IP tunnel packet that is larger than the IP MTU of some interface in the public network must either be discarded (if the Do Not Fragment (DF) bit is set in the outer IP header) or fragmented. If the tunnel packet is fragmented, then it is up to the destination tunnel endpoint to reassemble the tunnel packet from its fragments. Starting in Release 10, IP reassembly can be enabled for all the IPsec, GRE, and IP-IP tunnels belonging to a tunnel-group. For IP-IP and GRE tunnels, the reassembly option is also configurable on a per-tunnel basis so that some tunnels in the tunnel-group can have reassembly enabled, and others can have the extra processing disabled. When reassembly is disabled for a tunnel, all received fragments belonging to the tunnel are dropped.

To avoid public network fragmentation of IPsec, GRE, or IP-IP packets belonging to a particular tunnel, one possible strategy is to fragment IPv4 payload packets larger than a specified size M at entry into the tunnel (before encapsulation and encryption if applicable). The size M is configurable using the **ip-mtu** command under the **ip-tunnel** or **ipsec-tunnel/tunnel-template** configuration.

If the payload IPv4 packets are all M bytes or less in length then it is guaranteed that all resulting tunnel packets will be less than M+N bytes in length, if N is the maximum overhead added by the tunneling protocol. If M+N is less than the smallest interface IP MTU in the public network, fragmentation will be avoided. In some cases, some of the IPv4 payload packets entering a tunnel may have their DF bit set. And if desired, the SR OS supports the option (also configurable on a per-tunnel basis) to clear the DF bit in these packets so that they can be fragmented.

The system allows users to configure an **encapsulated-ip-mtu** for a given tunnel under an **ip-tunnel** or **ipsec-tunnel/tunnel-template** configuration. This represents the maximum size of the encapsulated tunnel packet. After encapsulation, if the IPv4 or IPv6 tunnel packet size exceeds the configured **encapsulated-ip-mtu**, then the system will fragment the packet against the **encapsulated-ip-mtu**.

The following is a description of system behavior about fragmentation:

- Private Side — If the size, before encapsulation, of the IPv4 or IPv6 packet entering the tunnel is larger than the ip-mtu configured under ip-tunnel or ipsec-tunnel/tunnel template:
  - IPv4 payload packet:
    - If the DF bit is not set in the packet or if the **clear-df-bit** command is configured, then the system fragments the packet against the ip-mtu configured under ip-tunnel or ipsec-tunnel/tunnel-template.
    - Otherwise, the system drops the packet and sends back an ICMP error Fragmentation required and DF flag set, with the suggested MTU set as the ip-mtu.
  - IPv6 payload packet:
    - If the packet size >1280 bytes, the system drops the packet and sends back an ICMPv6 Packet Too Big (PTB) message with the suggested MTU set as the ip-mtu.
    - If the packet size ≤1280 bytes, the system will forward the packet into the tunnel.
- Public Side — This applies to both ESP and IKE packets, IPv4 and IPv6.
  - If the ESP/IKE packet is larger than the encapsulated-ip-mtu, then the system fragments the packet against the encapsulated-ip-mtu.

#### 4.1.1.6 TCP MSS Adjustment

The system supports the Transmission Control Protocol (TCP) Maximum Segment Size (MSS) adjustment feature for the following types of tunnels on the ISA:

- IPsec
- IPinIP/GRE
- L2TPv3 (data packet only)

The intent of TCP MSS adjustment is to avoid IP-level fragmentation for TCP traffic encapsulated in a tunnel by updating the MSS option value in the TCP SYN packet with an appropriate value. This feature is useful when there is tunnel encapsulation that is not known by a TCP host, and the extra tunnel encapsulation overhead might cause IP-level fragmentation.

The system supports TCP MSS adjustment on both the public and private sides.

On the public side, when the ISA receives a tunnel packet (such as ESP), after decryption or decapsulation, if the payload packet is a TCP SYN packet, then the ISA replaces the MSS option with a configured value if the configured MSS value is smaller than the received MSS value or when there is no MSS option:



- If **public-tcp-mss-adjust auto** is configured, then:  
new MSS value = public\_side\_MTU – tunnel\_overhead – TCP fixed header – IP fixed header  
where
  - public\_side\_MTU = **encapsulated-ip-mtu**  
If **encapsulated-ip-mtu** is not configured, which means there is no post-encap fragmentation on ISA, then TCP MSS adjust is disabled.
  - TCP fixed header = 20
  - IP fixed header = 20 (IPv4) or 40 (IPv6)
- If a specific MSS value such as **public-tcp-mss-adjust new\_mss\_value** is configured, then the new MSS value sets to the *new\_mss\_value*

Notes:

- The **public-tcp-mss-adjust auto** command only applies to IPsec and IPinIP/GRE tunnels
- For an IPsec tunnel, the tunnel\_overhead is the maximum overhead of the corresponding CHILD\_SA
- For an IPinIP tunnel, the tunnel\_overhead is 0
- For a GRE tunnel, the tunnel\_overhead is length of GRE header

The private side is similar to the public side. The system processes the received TCP SYN packet on the private side if the TCP MSS adjust is enabled. However, there is no **auto** parameter for **private-tcp-mss-adjust** command.

## 4.1.2 Operational Conditions

A tunnel group that is in use cannot be deleted. In single-active mode, changes to the primary ISA are allowed only when the tunnel group is in a shutdown state. Changing the configured backup ISA (or adding a backup ISA) is allowed at any time unless the ISA is currently active for this tunnel group. When the backup ISA is active, changing the primary ISA is allowed without shutting down the tunnel group.

Changes can be made to the following:

- the mode from multi-active to single-active
- the primary ISA that is in single-active mode
- the active MDA number value that is in multi-active mode
- enabling or disabling the **ipsec-responder-only** configuration

In multi-active mode, if the active member ISA goes down, the system replaces it with a backup ISA. However, if a backup ISA is not available, the tunnel group is placed in an operationally down state. A multi-active tunnel group with MC-IPsec enabled cannot be changed into single active-mode unless it is first removed from the MC-IPsec configuration.

The public interface address can be changed at any time; however, if changed, any static tunnels that were configured to use the public interface address require a configuration changes accordingly. Otherwise, the tunnels are in an operationally down state until their configuration is corrected. The public service cannot be deleted while tunnels are associated.

A tunnel group ID or tag cannot be changed. To remove a tunnel-group instance, it must be in a shutdown state and all IPsec tunnels and IPsec GWs that terminated on the tunnel group must be removed first.

The security policy cannot be changed while an IPsec tunnel is administratively up and using the security policy.

The tunnel local gateway address, peer address, local ID, and public or private service ID parameters cannot be changed while the IPsec GW or IPsec tunnel is administratively up.

Each IPsec GW or IPsec tunnel has an administrative state. When the administrative state is down, tunnels cannot be set up.

Each IPsec GW and IPsec tunnel has an operation state. The operational state can have three possible values:

- oper-up — All configuration and related information are valid and fully ready for tunnel setup.
- oper-down — Some critical configuration information is missing or not ready. Tunnels cannot be set up.
- limited — Not all configuration information is ready to become fully operationally up. When IPsec GW is in a limited state, it is possible that a new tunnel cannot be established; however, the established tunnel is not impacted. When the IPsec tunnel is in a limited state, reconnection may fail.
  - IPsec GWs or IPsec tunnels can enter the limited state due do the following reasons, among others:
    - a Certificate Authority (CA) profile in the configured trust-anchor-profile goes down after the IPsec GW or IPsec tunnel becomes operationally up
    - an entry in a configured certificate profile goes down after the IPsec GW or IPsec tunnel becomes operationally up

#### 4.1.2.1 Dynamic Configuration Change Support for IPsec Gateway

All dynamic IPsec tunnels (dynamic LAN-to-LAN tunnels and remote-access tunnels) that terminate on the same IPsec GW share the same configuration (**config>service>sap>ipsec-gw**). The SR OS provides dynamic configuration change capability to modify certain IPsec GW configurations without impacting existing tunnels.

The following IPsec GW configurations are dynamically configurable without shutting down the IPsec GW:

- Change the pre-shared-key
- Change the reference of the ike-policy
- Change the reference of the tunnel-template
- Enable or change reference of the radius-authentication-policy
- Enable or change reference of the radius-accounting-policy
- Enable, disable, or change reference of the ts-negotiation
- Enable, disable, or change reference of the client-db
- Change configurations in the **config>service>sap>ipsec-gw>cert** context
- Change configurations in the **config>service>sap>ipsec-gw>dhcp** context
- Change configurations in the **config>service>sap>ipsec-gw>dhcp6** context
- Change configurations in the **config>service>sap>ipsec-gw>local-address-assignment** context

Existing tunnels are not impacted by dynamic configuration changes. The system uses new configurations for new tunnel negotiations. The system continues to use previous configurations that created the tunnels for on-going operations (such as rekeying) of the existing tunnel.

### 4.1.3 QoS Interactions

The ISA can interact with the queuing functions on the IOM through the ingress/egress QoS provisioning in the IES or IP VPN service where the IPsec session is bound. Multiple IPsec sessions can be assigned into a single IES or VPRN service. In this case, QoS defined at the IES or VPRN service level, is applied to the aggregate traffic coming out of or going into the set of sessions assigned to that service.

In order to keep marking relevant in the overall networking design, the ability to translate DSCP bit marking on packets into DSCP bit markings on the IPsec tunneled packets coming out of the tunnel is supported.

### 4.1.4 OAM Interactions

The ISA is IP-addressed by an operator-controlled IP on the public side. That IP address can be used in Ping and Traceroute commands and the ISA can either respond or forward the packets to the CPM.

For static LAN-to-LAN tunnel, in multi-active mode, a ping requests to public tunnel address would not be answered if the source address is different from the remote address of the static tunnel.

The private side IP address is visible. The status of the interfaces and the tunnels can be viewed using show commands.

Traffic that ingresses or egresses an IES or VPRN service associated with certain IPsec tunnels can be mirrored like other traffic.

Mirroring is allowed per interface (public) or IPsec interface (private) side. A filter mirror is allowed for more specific mirroring.

---

## 4.1.5 Redundancy

In single-active mode, every tunnel group can be configured with primary and backup ISAs. An ISA can be used as a backup for multiple IPsec groups. The ISAs are cold standby such that upon failure of the primary the standby resumes operation after the tunnels re-negotiate state. While the backup ISA can be shared by multiple tunnel groups only one tunnel group can fail to a single ISA at one time (no double failure support).

In multi-active mode, the active-mda-number value determines the number of ISA MDAs that will be active for this tunnel group, and tunnels are spread across all active ISA MDAs. Additional ISA MDA in this tunnel group will be in cold standby.

IPsec also supports dead peer detection (DPD).

BFD can be configured on the private tunnel interfaces associated with GRE tunnels and used by the OSPF, BGP or static routing that is configured inside the tunnel.

SR OS also supports multi-chassis IPsec redundancy, which provides 1:1 stateful protection against ISA failure or chassis failure

## 4.1.6 Statistics Collection

Input and output octets and packets per service queue are used for billing end customers who are on a metered service plan. Since multiple tunnels can be configured per interface the statistics can include multiple tunnels. These can be viewed in the CLI and SNMP.

Reporting (syslog, traps) for authentication failures and other IPsec errors are supported, including errors during IKE processing for session setup and errors during encryption or decryption.

A session log indicates the sort of SA setup when there is a possible negotiation. This includes the setup time, teardown time, and negotiated parameters (such as encryption algorithm) as well as identifying the service a particular session is mapped to, and the user associated with the session.

## 4.1.7 Security

The ISA module provides security utilities for IPsec-related service entities that are assigned to interfaces and SAPs. These entities (such as card, isa-tunnel module, and IES or VPRN services) must be enabled in order for the security services to process. The module only listens to requests for security services from configured remote endpoints. In the case of a VPN concentrator application, these remote endpoints could come from anywhere on the Internet. In the cases where a point-to-point tunnel is configured, the module listens only to messages from that endpoint.

### 4.1.7.1 GRE Tunnel Multicast Support

GRE tunnels support unicast and multicast IP packets as payload. From a multicast prospective, a GRE tunnel IP interface (associated with a private tunnel SAP) can be configured as an IGMP interface and/or as a PIM interface; MLD is not supported. The following multicast features are supported:

- IGMP versions 1, 2 and 3
- IGMP import policies
- IGMP host tracking
- Static IGMP membership
- Configurable IGMP timers
- IGMP SSM translation
- Multicast CAC
- Per-interface, per-protocol (IGMP/PIM) multicast group limits
- MVPN support (draft-rosen)
- MVPN support (BGP-MPLS)
- PIM-SM and SSM operation
- PIM BFD support
- Configurable PIM timers
- Configurable PIM priority
- PIM tracking support
- PIM ECMP (bandwidth or hash-based)
- Static multicast route

### 4.1.7.2 IPv6 over IPv4 GRE Tunnel

IPv6 payload packets can be delivered over an IPv4 GRE tunnel. In this scenario the two endpoints of the GRE tunnel have IPv4 addresses and the VPRN or IES SAP interface to the tunnel is an IPv6 only or dual-stack IPv4/IPv6 interface. IPv6 over IPv4 GRE tunneling allows IPv6 islands to be connected over an IPv4 only transport infrastructure.

In order to configure a tunnel to carry IPv6 payload the tunnel must be configured with at least one **dest-ip** that contains an IPv6 address (global unicast and/or link local). A tunnel can have up to 16 **dest-ip** addresses (IPv4 and IPv6 together). For a tunnel to come operationally up all the **dest-ip** addresses must be part of locally configured subnets (associated with the private tunnel interface).

In order to forward IPv6 traffic through a tunnel supporting IPv6 payload a dynamic routing protocol (such as BGP or OSPFv3) can be configured to run inside the tunnel (by associating the protocol with the private tunnel interface) or else an IPv6 static route next-hop equal to a **dest-ip** of the tunnel can be used.

IPv6 payload packets larger than 1280 bytes (the minimum IPv6 MTU) and also larger than the configured **ip-mtu** value of the tunnel are always discarded. If the **icmp6-generation** and **packet-too-big** commands are configured under the tunnel, then ICMPv6 Packet-Too-Big messages are generated and sent back to the originating host when discards occur due to the private side IP MTU being exceeded.

### 4.1.8 IKEv2

IKEv2, defined in RFC 4306, *Internet Key Exchange (IKEv2) Protocol*, is the second version of the Internet Key Exchange Protocol. The main driver of IKEv2 is to simplify and optimize IKEv1. An IKE\_SA and a CHILD\_SA can be created with only four IKEv2 message exchanges. IKEv2 is supported with the following features:

- static LAN-to-LAN tunnel
- dynamic LAN-to-LAN tunnel
- remote-access tunnel
- pre-shared-key authentication, certificate authentication, EAP (remote-access tunnel only)
- liveness check
- IKE\_SA rekey
- CHILD\_SA rekey (full Traffic-Selector support including protocol and port range)

### 4.1.8.1 IKEv2 Traffic Selector and TS-List

The SR OS IKEv2 implementation supports the following traffic selectors:

- IPv4/IPv6 address range
- IP protocol ID
- protocol port range

Port range (including OPAQUE ports) is supported for the following protocols:

- TCP
- UDP
- SCTP
- ICMP
- ICMPv6
- MIPv6

With ICMP and ICMPv6, the system treats the most significant 8 bits of the IKEv2 TS port value as the ICMP message type and the least significant 8 bits as ICMP code.

With MIPv6, the system treats the most significant 8 bits of the IKEv2 TS port value as the mobility header type.

With ICMP, ICMPv6, and MIPv6, the port value in TS<sub>i</sub> is the value that the tunnel initiator can send, and the port value in TS<sub>r</sub> is the value that the tunnel responder can send.

The SR OS supports OPAQUE as a TS port selector. An OPAQUE port means that the corresponding CHILD\_SA only accepts packets that are supposed to have port information but do not, such as when a packet is a non-initial fragment.

The system allows users to configure a TS-list for each IPsec gateway, applied to both IKEv2 remote access tunnels and dynamic LAN-to-LAN tunnels. Each TS-list contains a local part and a remote part, with each part containing up to 32 entries. Each entry can contain address ranges or subnets, protocols, and port range configurations.

The local part of the TS-list represents the traffic selector for the local system, while the remote part is for the remote peer. If a TS-list is applied on an IPsec gateway, and the system is the tunnel responder, then the local part is TS<sub>r</sub> and the remote part is TS<sub>i</sub>.

Combinations of address range, protocol, and port range are not allowed to overlap between entries in the same TS-list.



The system performs traffic selector narrowing as follows.

1. For each TS in the received TSi/TSr, independent address, protocol, and port narrowing is performed. The resulting TS-set is the combination of the address, protocol, and range intersections.
2. The collected TS-set is used as the TSi/TSr.

For a remote access tunnel, TSi narrowing results in an intersection between the following three TSis:

- the TSi received from the client
- the remote part configuration of the TS-list
- a generated TS based on the assigned internal address
  - address — the assigned internal address
  - protocol — any
  - port range — any

The following is an example of a dynamic LAN-to-LAN tunnel.

The configured TS-list local part is as follows:

- Entry 1: 10.10.1.0 → 10.10.1.20, udp, port 100 → 200
- Entry 2: 10.20.1.0 → 10.20.1.20, udp, port 300 → 400

The peer proposes the following TSr:

- Entry 1: 10.10.1.1 → 10.10.1.5, udp, port 110 → 150
- Entry 2: 10.10.1.6 → 10.10.1.10, udp, port 180 → 210
- Entry 3: 10.10.1.15 → 10.10.1.28, udp, port 120 → 160
- Entry 4: 10.20.1.15 → 10.20.1.28, tcp, port 250 → 450

The intersections for the proposed entries are as follows:

- Entry 1: 10.10.1.1 → 10.10.1.5, udp, port 110 → 150
- Entry 2: 10.10.1.6 → 10.10.1.10, udp, port 180 → 200
- Entry 3: 10.10.1.15 → 10.10.1.20, udp, port 120 → 160
- Entry 4: 10.20.1.15 → 10.20.1.20, tcp, port 300 → 400

The resulting TSr system return would be:

- 10.10.1.1 → 10.10.1.5, udp, port 110 → 150
- 10.10.1.6 → 10.10.1.10, udp, port 180 → 200

- 10.10.1.15 → 10.10.1.20, udp, port 120 → 160
- 20.20.1.15 → 20.20.1.20, tcp, port 300 → 400

If more than 32 entries are returned, the system will reject ts-negotiation and return `TS_UNACCEPTABLE` to the peer.

For dynamic LAN-to-LAN tunnels, the system can automatically create a reverse route in a private VRF to route clear traffic into the tunnel. The reverse route is created based on the address range part of the narrowed `TSi` of the `CHILD_SA`. If there are multiple `TSs` in the `TSi` that have overlapping address ranges, the system will create one or more minimal subnet routes that can cover all address ranges in the `TSi`. If the auto-created reverse route overlaps with an existing reverse route that points to the same tunnel, the system will choose the route with the larger subnet. If the existing route points to a different tunnel, then `CHILD_SA` creation fails.

For RADIUS authentication, such as **psk-radius**, **cert-radius**, or EAP, the RADIUS server can optionally return a TS-list name via the VSA `Alc-IPsec-Ts-Override` in the access-accept message, which overrides the TS-list name configured via the CLI.

In the event of a `CHILD_SA` rekey, if the system is a rekey initiator, it will send the current in-use TS to the peer and expect the peer to return the same TS. If the system is a rekey responder, the system will do the same narrowing as was done during `CHILD_SA` creation.

Configuration of a TS-list can be changed without shutting down the IPsec gateway, although the new TS-list only applies to the subsequent rekey or to the new `CHILD_SA` creation, and does not affect established `CHILD_SAs`.

#### 4.1.8.2 IKEv2 Fragmentation

In some cases, an IKEv2 message can be large, like an `IKE_AUTH` message with certificate payload. This will likely cause the IKEv2 packet to be fragmented into a few smaller IP packets. However, in some deployments, there could be devices or network policing, rate limiting or even dropping UDP fragments. In these cases, the SR OS supports fragmenting IKEv2 messages on the protocol level, as specified in RFC 7383, Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation.

This feature is enabled by configuring the **ikev2-fragment** command in the `ike-policy` context with an MTU. The specified MTU is the maximum size of IKEv2 packet.

The system only enables IKEv2 fragmentation for a given tunnel when the **ikev2-fragment** is configured and the peer also announces its support via sending a `IKEV2_FRAGMENTATION_SUPPORTED` notification.

---

## 4.1.9 SHA2 Support

According to RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*, the following SHA2 variants are supported for authentication or pseudo-random functions:

Use HMAC-SHA-256+ algorithms for data origin authentication and integrity verification in IKEv1/2, ESP:

- AUTH\_HMAC\_SHA2\_256\_128
- AUTH\_HMAC\_SHA2\_384\_192
- AUTH\_HMAC\_SHA2\_512\_256

For use of HMAC-SHA-256+ as a PRF in IKEv1/2:

- PRF\_HMAC\_SHA2\_256
- PRF\_HMAC\_SHA2\_384
- PRF\_HMAC\_SHA2\_512

## 4.1.10 IPsec Client Lockout

An optional lockout mechanism can be enabled to block malicious clients and prevent them from using invalid credentials to consume system resources, as well as to prevent malicious users from guessing credentials such as a pre-shared key. This mechanism can be enabled by using the **lockout** command.

If the number of failed authentication attempts from a particular IPsec client exceeds a configured threshold during a specified time interval, the client will be blocked for a configurable period of time. If a client is blocked, the system will drop all IKE packets from the source IP address and port.

The following authentication failures are counted as failed authentication attempts:

- IKEv1
  - **psk**: failed to verify the HASH\_I payload in main mode
  - **plain-psk-xauth**:
    - failed to verify the HASH\_I payload in main mode
    - RADIUS access-reject received
- IKEv2
  - **psk**: failed to verify the AUTH payload in the auth-request packet

- **psk-radius:**
  - failed to verify the AUTH payload in the auth-request packet
  - RADIUS access-reject received
- **cert:**
  - failed to verify the AUTH payload in the auth-request packet
  - failed to verify the peer's certification to configured trust-anchors
- **cert-radius:**
  - failed to verify the AUTH payload in the auth-request packet
  - failed to verify the peer's certification to configured trust-anchors
  - RADIUS access-reject received
- **eap:** RADIUS access-reject received

Other failures, such as being unable to assign an address, are not counted.

The AUTH failure counter is reset by either a successful authentication before the client is blocked, the expiration of a block timer, or the expiration of the duration timer.

If multiple IPsec clients behind a NAT device share the same public IP address, a limit for the maximum number of clients or ports behind the same IP address can be configured. If the number of ports exceeds the configured limitation, all ports from that IP address are blocked.

The **clear ipsec logout** command can also be used to manually clear a logout state for the specified clients.

## 4.1.11 IPsec Tunnel CHILD\_SA Rekey

SR OS supports CHILD\_SA rekeying for both IKEv1 and IKEv2. The following are the behaviors for the rekey:

- IKEv1 or IKEv2 CHILD\_SA rekey initiator:
  - Outbound: The system immediately switches to the new security association (SA) after a new SA is created.
  - Inbound: The old SA is kept for three minutes after the new SA is created. Then, it is removed, and upon removal:
    - IKEv1: The system will not send a delete message upon removal.
    - IKEv2: The systems send a delete message upon removal.
- IKEv1 or IKEv2 CHILD\_SA rekey responder:

- Outbound: The system keeps using the old SA for 25 seconds after the new SA is created before switching to the new SA. If a delete message of the old SA is received before 25 seconds, the system removes the old SA and will start using new SA.
- Inbound: The old SA is kept for rest of its lifetime. However, if a delete message is received to close the corresponding outbound SA, then the system removes the corresponding inbound SA before its lifetime expires. The system sends a delete message when the old SA lifetime expires.

If the old SA lifetime expires before the 25 seconds or three minutes mentioned above, the old SA is removed upon expiration and the system sends a delete message.

## 4.1.12 Multiple IKE/ESP Transform Support

For IPsec tunnels or IPsec gateways, the SR OS allows users to configure up to four IKE transform and four IPsec transform configurations for IKE and ESP traffic.

IKE transform parameters are configured in the **config>ipsec>ike-transform** and referenced in the **ike-policy**, while IPsec transform parameters are configured in the **config>ipsec>ipsec-transform** context and referenced in the tunnel template for dynamic tunnels and under **config>service>vpn>interface>sap>ipsec-tunnel>dynamic-keying** for static tunnels.

IKE transform includes the following configurations:

- IKE encryption algorithm
- IKE authentication algorithm
- Diffie-Hellman group
- IKE SA lifetime

IPsec transform includes the following configurations:

- ESP encryption algorithm
- ESP authentication algorithm
- Diffie-Hellman group for CHILD SA rekey with PFS
- CHILD SA lifetime

If multiple **ike-transform** and **ipsec-transform** parameters are configured for IPsec gateways and IPsec tunnels, the system uses the configured transforms to negotiate with the peer. This negotiation allows IPsec gateways and IPsec tunnels to support peers with different crypto algorithms.

## 4.2 X.509v3 Certificate Overview

X.509v3 is an ITU-T standard which consists of a hierarchical system of Certificate Authorities (CAs) that issue certificates that bind a public key to particular entity's identification. The entity's identification could be a distinguished name or an alternative name such as FQDN or IP address.

An end entity is an entity that is not CA. For example an end entity can be a web server, a VPN client, or a VPN gateway.

A CA issues a certificate by signing an entity's public key with its own private key. A CA can issue certificates for an end entity as well as for another CA. In the case when a CA certificate is issued by itself (signed by its own private key), then this CA is called the root CA. Thus, an end entity's certificate could be issued by the root CA or by a subordinate CA (this is issued by another subordinate CA or root CA). When there are multiple CA involved, it is called a chain of CAs.

A PKI also includes the mechanism for revoking certificates due to reasons such as a compromised private key.

The certificate can be used for different purposes. One purpose is authentication. Typically certificate authentication functions as following:

- The system trusts a CA as trust anchor CA (which typically is a root CA). This means that all certificates issued by a trust anchor CA, or the certificates issued by a sub CA issued by the trust anchor CA, are consider trusted.
- A peer to be authenticated presents its certificate along with a signature over some shared data between the peer and system, which is signed by using a private key.
- The signature is verified by using the public key in the certificate. And the certificate itself is verified that is issued by the trust anchor CA or a sub-CA in a chain up to the trust anchor CA. The system can also check if the peer's certificate has been revoked. Only when all these verifications succeed, then the certificate authentication succeeds.

### 4.2.1 SR OS X.509v3 Certificate Support

SR OS PKI implementation supports the following features:

- Supported ECDSA curves:
  - secp256r1
  - secp384r1

- secp521r1
- Certificate Enrollment:
  - Locally generated RSA/DSA/ECDSA key
  - Off-line enrollment via PKCS#10
  - On-line enrollment via CMPv2
- Support CA chain
- Certificate revocation check:
  - CRL for both EE (End Entity) and CA certificate
  - OCSP for EE certificate only

## 4.2.2 Local Storage

The SR OS requires the following objects to be stored locally as file:

- CA Certificate
- CRL
- System's own certificate
- System's own key

All above objects must be imported before they can be used by the SR OS. This is performed by using the **admin certificate import** command. The import process converts the format of input file to DER, encrypts the key file and saves it in cf3:/system-pki directory.

The imported file can also be exported as one to use in the specified format by means of the **admin certificate export** command.

The **admin certificate import** and **admin certificate export** command supports following formats:

- Certificates can be import/export by using following formats:
  - PKCS#12
  - PKCS#7 (DER and PEM)
  - PEM
  - DER

If there are multiple certificates in the file, only the first one will be used.

- Key pair can be import/export by using following formats:
  - PKCS#12 (must along with certificate)

- PEM
- DER
- CRL can be import/export by using following formats:
  - PKCS#7 (DER and PEM)
  - PEM
  - DER
- PKCS#12 file can be encrypted with a password

### 4.2.3 CA-Profile

In SR OS, CA-related configuration is stored in a CA-profile which contains following configurations:

- Name and description
- CA's Certificate — An imported certificate
- CA's CRL— An imported CRL
- Revocation check method — Specifies the way CA check the revocation status of the certificate it issued.
- CMPv2 — A CMPv2 server related configurations
- OCSP— An OCSP responder related configurations

When user enables a ca-profile (no shutdown), system will load the specified CA certificate and CRL into memory. And following checks are performed:

- For CA certificate:
  - All non-optional fields defined in section 4.1 of RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, must exist and conform to the RFC 5280 defined format.
  - Check the version field to see if its value is 0x2.
  - Check the Validity field to see that if the certificate is still in validity period.
  - X509 Basic Constraints extension must exist and CA Boolean must be True.
  - If Key Usage extension exists, then at least keyCertSign and cRLSign should be asserted.

For CRL:

- All non-optional fields defined in section 5.1 of RFC 5280 must exist and conform to the RFC 5280 defined format.



- If the version field exists, the value must be 0x1.
- The delta CRL Indicator must not exist (Delta CRL is not supported).
- CRL must be signed by the configured CA certificate.

CRL, by default, is required to enable ca-profile, but it could be optional by changing the revocation check method configuration. For the revocation check method configuration, refer to [Certificate Revocation Check](#).

## 4.2.4 CA Chain Computation

In case of verifying a certificate with a CA or a chain of CAs, the system needs to identify the issuer CA of the certificate in question. The SR OS will look through all configured ca-profiles to find the issuer CA. The following is the method system used to find the issuer CA:

- The issuer CA's certificate subject must match the issuer field of the certificate in question.
- If present, the authority key identifier of the certificate in question must match the subject key identifier of the issuer CA's certificate
- If present, the key usage extension of the issuer CA's certificate must permit certificate signing.

## 4.2.5 Certificate Enrollment

The SR OS supports two certificate enrollment methods:

- Off-line method via PKCS#10
- On-line method via CMPv2

The off-line method works as follows:

1. Generate a key pair via the command **admin certificate gen-keypair**

For example:

**admin certificate gen-keypair cf3:/segw.key size 2048 type rsa**

2. Generate a PKCS#10 certificate signing request with the key generated in the step mentioned above via the **admin certificate gen-local-cert-req** command.

For example:

**admin certificate gen-local-cert-req keypair cf3:/segw.key subject-dn**

**C=US,ST=CA,O=ALU,CN=SeGW domain-name segw-1.alu.com file cf3:/segw.pkcs10**

The user specifies the subject of certificate request and optionally can also specify a FQDN and/or an IP address as SubjectAltName.

3. Import the key file via the **admin certificate import** command

For example:

```
admin certificate import type key input cf3:/segw.key output segw.key format de
```

4. Since the key is imported, remove the key file generated in the first step for security reasons.

5. Send the PKCS#10 file to CA via an offline method such as E-MAIL.

6. CA signs the request, and returns the certificate.

7. Import the result certificate the **admin certificate import** command.

For example:

```
admin certificate import type cert input cf3:/segw.cert output segw.cert format pem
```

For CMPv2-based enrollment, refer to [Certificate Management Protocol Version 2 \(CMPv2\)](#).

## 4.2.6 Certificate Revocation Check

A revocation check is a process to see if a certificate has been revoked by the issuer CA.

The SR OS supports two methods for certificate revocation check:

- CRL
- OCSP

CRL can be used for both EE and CA certificate checks, while OCSP could only be used for an EE certificate.

With an IPsec application, users can configure multiple check methods with a priority order for an EE certificate. With the **status-verify** command in the **ipsec-gw/ipsec-tunnel** configuration context, a primary method, a secondary method and a default result can be configured. The primary and secondary method can be either OCSP or CRL. The default result is either **good** or **revoked**. If the system cannot get an answer from the primary method, then it will fall back to the secondary method. If secondary method also does not return an answer, then the system will use the default result.

By default, the system uses CRL to check the revocation status of a certificate, whether it is an end entity certificate or a CA certificate. This makes CRL a mandatory configuration in the **ca-profile**.

The **revocation-check** command in the **ca-profile** can change this behavior, with **revocation-check crl-optional** configured:

When a user enables the **ca-profile** (**no shutdown**), the system will try to load the configured CRL (specified by the **crl-file** command). But, if the system fails to load it for following reasons, then the system will still keep **ca-profile oper-up**, but treat the CRL as non-existent.

- The CRL file does not exist.
- The CRL is not properly encoded, possibly due to an interrupted file transfer.
- The CRL is not signed by the CA certificate configured in the CA profile.
- The wrong CRL version.
- The CRL expired or is not yet valid.

If the system needs to use the CRL of a specific **ca-profile** to check revocation status of an end entity certificate and CRL is non-existent due to the above reasons, then the system will treat it as unable to get an answer from CRL and fall back to the secondary status-verify method or default-result configured under the **ipsec-gw/ipsec-tunnel**.

If the system needs to check the revocation of a CA certificate in certificate chain, and if the CRL is non-existent due to the above reasons, then the system will skip checking the revocation status of the CA certificate. For example, the CA1 is issued by CA2, if CA2's **revocation-check** is **crl-optional** and CA2's CRL is non-existent, then the system will not check CA1 certificate's revocation status and consider it as good.

The user must disable the **ca-profile** to change the revocation-check configuration.

For details about OCSP, refer to [OCSP](#).

## 4.2.7 Certificate/CRL Expiration Warning

The system can optionally generate a warning message before a certificate or a CRL expires. The amount of time before expiration is configurable via two system-wide CLI commands (**certificate-expiration-warning** and **crl-expiration-warning**). The warning messages can also be optionally repeated at a configured interval. For details of the warning messages, refer to the corresponding command descriptions.

If a configured EE certificate expires, the system will not bring down an established ipsec-tunnel/ipsec-gw down, however future certificate authentication will fail.

If a CA certificate expires, the system will bring the ca-profile operationally down. This will not affect established tunnels, however future certificate authentication that uses the ca-profile will fail.

## 4.2.8 Certificate/CRL/Key Cache

Configured certificates, CRLs, and keys are cached in memory before they are used by the system.

- Every certificate/CRL/Key has one cache copy system-wide.
- For a CA certificate and CRL, the cache will be created when there is a ca-profile and when a **no shutdown** is performed, and removed.
- For an ipsec-tunnel or ipsec-gw using legacy **cert** and **key** configurations, the cache will be created only when the first tunnel using it is in a **no shutdown** state, and it will be cleared when the last tunnel that used it is **shutdown**.
- For an ipsec-tunnel or ipsec-gw using **cert-profile**, the cache will be created when the first **cert-profile** using it is in a **no shutdown** state, and removed when the last cert-profile that used it is **shutdown**.
- If a certificate or key is configured with both a **cert-profile** and legacy **cert** or **key** command, then the cache will be created when the first object (a **ipsec-gw**, **ipsec-tunnel** or **cert-profile**) using it is in a **no shutdown** state and removed the last object using it is **shutdown**.

In order to update a certificate or key without a **shutdown ca-profile** or **ipsec-tunnel/ipsec-gw**, there is a CLI command (**admin certificate reload**) to manually reload the certificate and key cache. For details about reload, refer to the command description for **admin certificate reload**.

## 4.2.9 Auto CRL Update

The SR OS provides an automatic mechanism to update a CRL file. The system will try to download the CRL from a list of configured HTTP URLs and replace existing CRL file when a qualified CRL is successfully downloaded. A qualified CRL is a valid CRL signed by the CA and is more recent than the existing CRL. To determine if a downloaded CRL is more recent than an existing CRL, the system will compare the This-Update field of the CRL first. If they are the same, the system will compare the CRL number extension if present.

The configured HTTP URL must point to a DER-encoded CRL file.

This feature supports two types of downloading schedules:

- **Periodic** — The system will download a CRL periodically at the interval configured via the **periodic-update-interval** command. For example, if the **periodic-update-interval** is 1 day, then the system will download CRL every 1 day. The minimal periodic-update-interval is 1 hour.
- **Next-update-based** — The system will download a CRL at the time = `Next_Update_time_of_current_CRL` minus pre-update-time. For example, if the Next-Update of current CRL is 2015-06-30 06:00 and pre-update-time is 1 hour, then the system will start the download at 2015-06-30, 05:00.

The system allows up to eight URLs to be configured for a given ca-profile. When downloading begins, URLs will be tried in order, and the first successfully downloaded qualified CRL will be used to update existing CRL. If the downloading fails or the downloaded CRL is not qualified, the system will move to the next URL in the list. If all URLs in the list fail to return a qualified URL, then:

- In case of next-update-based schedule, the system will wait for a configured retry-interval before retry from the first URL in the list again.
- In case of periodic schedule, the system will wait until the next scheduled time.

Upon executing a **no shutdown** of a ca-profile, if the auto-crl-update is enabled, then in case configures CRL file does not exist or is expired or invalid, then the system will start downloading right away.

The system also provides an **admin** command (**admin certificate crl-update ca <ca-profile-name>**) for users to manually trigger downloading. However, it requires a shutdown of the **auto-crl-update** command (**no auto-crl-update**).

HTTP transport can be over either IPv4 or IPv6.

This feature supports Base/Management/VPN routing instance. VPLS management is not supported. In the case of VPN, the HTTP server port can only be 80 or 8080.

## 4.2.10 IPsec Client Database

The IPsec client database is a database configured in the (**config>ipsec>client-db**) CLI context, which can be used to authenticate and authorize IKEv2 dynamic LAN-to-LAN tunnels.

Each client database contains one or more client entries. When the system receives a new tunnel request, it performs a look up in the associated database of the IPsec gateway (**ipsec-gw**). If there is match, the system optionally could use credentials configured in the matched client entry to authenticate the peer. If the authentication succeeds, then, optionally, the matched entry could also return certain IPsec parameters such as the private service ID which can be used for tunnel setup.

If the client database lookup failed to return a match result, then the system can either fall back to the **ipsec-gw** level configuration or fail the tunnel setup. The action to take depends on the CLI configuration.

The system supports one of the following as matching input:

- The peer's tunnel IP address
- The peer's IDi
- A combination of both

The above matching input is defined in the **match-list** context in the client-db configuration. Each client entry contains client matching criteria that corresponds to the match list. The system correlates matching input with the client matching criteria of each client entry in the client-db configuration. The system supports the following matching method:

- For the peer's IDi:
  - Any: any IDi
  - IPv4/IPv6 prefix: Matches the peer's address type IDi to a configured prefix. It is considered a match if the IDi falls within the prefix.
  - FQDN: Matches the peer's FQDN type IDi to a string. This supports a complete string match or a suffix string match.
  - RFC822: Matches the peer's RFC 822 type IDi to a string This supports a complete string match or suffix string match.
- For the peer's tunnel IP address:
  - Matches the peer's tunnel address to a configured prefix. It is a match if the IDi fall within the prefix.
  - IPv4 Any: Matches any IPv4 address.
  - IPv6 Any: Matches any IPv6 address.

Each client entry has a client index (an integer). This is different from a client identification. if there are multiple matched entries in a lookup, the client entry with smallest client index will be used.

The client entry supports following types of credentials:

- Pre-shared key

If the credential is not configured in the matched entry, then the credential configured under the ipsec-gw context will be used.

A client entry could optionally return the following IPsec parameters:

- A private service id
- A private interface name
- A tunnel-template id
- A Ts list

The returned parameter overrides the configuration of the ipsec-gw level.

There is only one client-db for each ipsec-gw, but different ipsec-gw configurations can use the same client-db.

Note that the **encapsulated-ip-mtu** command in the client-db returned tunnel-template will not be applied to the IKE packet fragmentation. The **encapsulated-ip-mtu** command configured in the **configure>ipsec>tunnel-template** context is used instead. However, the client-db returned encapsulated IP MTU value still applies to the ESP packet fragmentation.

Note that:

- A client entry in a shutdown state will be skipped while the system performs the matching process.
- If the configuration returned by client-db is invalid, the system will fail the tunnel setup.
- The reference of the client-db under the ipsec-gw context can be changed without shutting down ipsec-gw
- Shutting down a referenced client-db without shutting down ipsec-gw is allowed and the established tunnel will not be impacted. The system will use the configuration on the ipsec-gw level for new a tunnel request while the client-db is shutdown if a fallback is configured.
- Adding a new client in a referenced client-db without shutting down ipsec-gw or client-db is allowed.
- Removing a client in the referenced client-db without shutting down ipsec-gw or client-db is allowed. However, the shutdown of the client to be removed is required.
- Changing an existing client of a referenced client-db without shutting down ipsec-gw or client-db is allowed. However, the shutdown of the client to be removed is required.

## 4.3 Using Certificates For IPsec Tunnel Authentication

The SR OS supports X.509v3 certificate authentication for IKEv2 tunnel (LAN-to-LAN tunnel and remote-access tunnel). The SR OS also supports asymmetric authentication. This means the SR OS and the IKEv2 peer can use different methods to authenticate. For example, one side could use pre-shared-key and the other side could use a certificate.

The SR OS supports certificate chain verification. For a static LAN-to-LAN tunnel or ipsec-gw, there will be a configurable trust-anchor-profile which specifies the expecting CAs that should be present in the certificate chain before reaching the root CA (self-signed CA) configured in the system.

The SR OS's own key and certificate are also configurable per tunnel or ipsec-gw.

When using certificate authentication, the SR OS will use the subject of the configured certificate as its ID by default.



**Note:** IPsec application is subject to FIPS restrictions; for more information please refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*.

### 4.3.1 IKEv2 Digital Signature Authentication

RFC 7427 *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)* defines a new IKEv2 AUTH payload method which not only indicates the type of public key, but also the hash algorithm that used to generate the signature; it also includes a new IKEv2 notification: SIGNATURE\_HASH\_ALGORITHMS, which is used to signal support of RFC 7427 and a list of support hash algorithms to a peer.

RFC 7427 is the default way to perform certificate authentication for IKEv2. The system negotiates its support with the peer as follows:

- Sending:
  - As tunnel initiator: Includes SIGNATURE\_HASH\_ALGORITHMS in the IKE\_SA\_INIT request.
  - As tunnel responder: Includes SIGNATURE\_HASH\_ALGORITHMS in IKE\_SA\_INIT response only if the received IKE\_SA\_INIT request includes it.



- Includes the following hash algorithms in SIGNATURE\_HASH\_ALGORITHMS:
  - SHA1/SHA2-256/SHA2-384/SHA2-512
- Receiving:
  - If the peer does not include SIGNATURE\_HASH\_ALGORITHMS in the IKE\_SA\_INIT packet, then it does not support RFC 7427 and the system will use an RSA Digital Signature for the RSA key(value 1), and DSS Digital Signature (value 3) for the DSA key to generate the AUTH payload.



**Note:** If the ECDSA key is selected in the cert-profile entry, then the tunnel setup fails in the system.

- If the peer sends SIGNATURE\_HASH\_ALGORITHMS, then the system uses RFC 7427 and the strongest hash algorithms that is supported by both sides to generate the AUTH payload. If there is no common hash algorithms supported by both sides, the system will fallback to RSA Digital Signature (Auth Method value 1) or DSS Digital Signature (Auth Method value 3).



**Note:** If the selected key is an RSA key, then there are certain cases that have a short RSA key with long hash algorithm. The system will fall back to RSA Digital Signature for RSA key (value 1) even when both sides send SIGNATURE\_HASH\_ALGORITHMS and there are common hash algorithms.

- To verify the received digital signature of the AUTH payload, the peer must use one of the algorithms in the SIGNATURE\_HASH\_ALGORITHMS that the system sends. Otherwise, the tunnel setup will fail.

The system will continue to use CAs in received cert-request payloads to select the cert-profile entry; if the selected entry is an RSA key, then the system needs to decide to whether use PKCS#1-1.5 or RSASS-PSS to generate the signature by using the value set by the **config>ipsec>cert-profile>entry>rsa-signature** command.

---

## 4.4 Trust-Anchor Profile

Since Release 12.0R1, the SR OS supports multiple trust-anchors per ipsec-tunnel/ipsec-gw. Users can configure a trust-anchor-profile that includes up to eight CAs. The system will build a certificate chain by using the certificate in the first certificate payload in the received IKEv2 message. If any of configured trust-anchor CAs in the trust-anchor-profile appears in the chain, then authentication is successful. Otherwise authentication is failed.

The SR OS will only support processing of up to 16 hashes for the trust-anchor list from other products. If the remote end is sending more than 16, and a certificate match is in the > 16 range the tunnel will remain down with authentication failure.

The legacy **trust-anchor** command under ipsec-gw/ipsec-tunnel was deprecated in Release 15.0.R1.

## 4.5 Cert-Profile

Since Release 12.0R1, the SR OS supports sending different certificate/chain according to the received IKEv2 certificate-request payload. This is achieved by configuring a cert-profile which allows up to eight entries. Each entry includes a certificate and a key and optionally also a chain of CA certificates.

The system will load cert/key in cert-profile into memory and build a chain: compare-chain for the certificate configured in each entry of cert-profile upon no shutdown of the cert-profile. These chains will be used in IKEv2 certificate authentication. If a chain computation cannot be completed for a configured certificate, then the corresponding compare-chain will be empty, or only partially computed.

Because there could be multiple entries configured in the cert-profile, the system needs to pick the cert/key in the correct entry that the other side expects to receive. This is achieved by a lookup of the CAs within the received cert-request payload in the compare-chain and then picking the first entry that there is a cert-request CA appearing in its chain. If there is no such cert, the system picks the first entry in the cert-profile. The first entry is the 1st configured entry in cert-profile. The entry-id of first entry does not have to be "1".

For example, there are three CA listed in certificate-request payload: CA-1, CA-2 and CA-3, and there are two entries configured in the cert-profile like following:

```
cert-profile "cert-profile-1"
 entry 1
 cert "cert-1"
 key "key-1"
 entry 2
 cert "cert-2"
 key "key-2"
 send-chain
 ca-profile "CA-1"
 ca-profile "CA-2"
```

The system will build two compare-chains: chain-1 for cert-1 and chain-2 for cert-2. Assume CA-2 appears in chain-2, but CA-1 and CA-3 do not appear in either chain-1 or chain-2. Then the system will pick entry 2.

After a cert-profile entry is selected, the system generates the AUTH payload by using the configured key in the selected entry. The system will also send the cert in the selected entry as "certificate" payload to the peer.

---

If a chain is configured in the selected entry, then one certificate payload is needed for each certificate in the configured chain. The first certificate payload in the IKEv2 message will be the signing certificate, which is configured by the **cert** command in the chosen cert-profile entry. With the above example, the system will send three certificate payloads: cert-2, CA-1,CA-2.

The following CA chain-related enhancements are supported

- The no-shut of a ca-profile will trigger a re-computation of compute-chain in related cert-profiles. The system will also generate a new log-1 to indicate a new compute-chain has been generated; the log includes the ca-profile names on the new chain. Another log-2 will be generated if the send-chain in a cert-profile entry is not in compute-chain due to this ca-profile change. Another log is generated if the hash calculation for a certificate under a ca-profile has changed.
- When no-shutting a cert-profile, the system now allows the CAs in the send-chain, not in the compute-chain. The system will also generate log-2 as above.
- The system now allows changes of the configuration of send-chain without shutdown of cert-profile.

## 4.6 Certificate Management Protocol Version 2 (CMPv2)

CMPv2, RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)* is a protocol between a Certificate Authority (CA) and an end entity. It provides multiple certificate management functions like certificate enrollment, certificate update, etc.

The SR OS supports following CMPv2 operations:

- Initial Registration — The process the SR OS uses to enroll a certificate with a certain CA for the first time.
  - Public/Private key pair must be pre-provisioned before enrollment by means of local generation or other methods.
  - Users can optionally include a certificate or certificate chain in the extraCerts field of the initial registration request.
- Key Pair Update — A process for SR OS to update an existing certificate due to reason like refreshes key/cert before it expires or any other reason
- Certificate Update — A process where an initialized SR OS system obtains additional certificates.
- Polling — In some cases, the CA may not return the certificate immediately for reasons such as **request processing need manual intervention**. In such cases, the SR OS supports polling requests and responds as described in Section 5.3.22, Polling Request and Response, in RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*.

The following lists some implementation details:

- HTTP is the only supported transport protocol for CMPv2. HTTP 1.1 and 1.0 are supported and configurable.
- All CMPv2 messages sent by SR OS consist of only one PKI Message. The size of the sequence for PKI Messages are 1 in all cases.
- Both the password-based MAC and the public key-based signature CMPv2 message protection are supported.
- SR OS only allows one outstanding ir/cr/kur request for each CMPv2 server. The means that no new requests are allowed if a pending request is present.

## 4.7 OCSP

Online Certificate Status Protocol (OCSP) (RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*) is used by SR OS applications to determine the (revocation) state of an identified certificate. Unlike CRL, which relies on checking against an off-line file, OCSP provides timely, on-line information regarding the revocation status of a certificate.

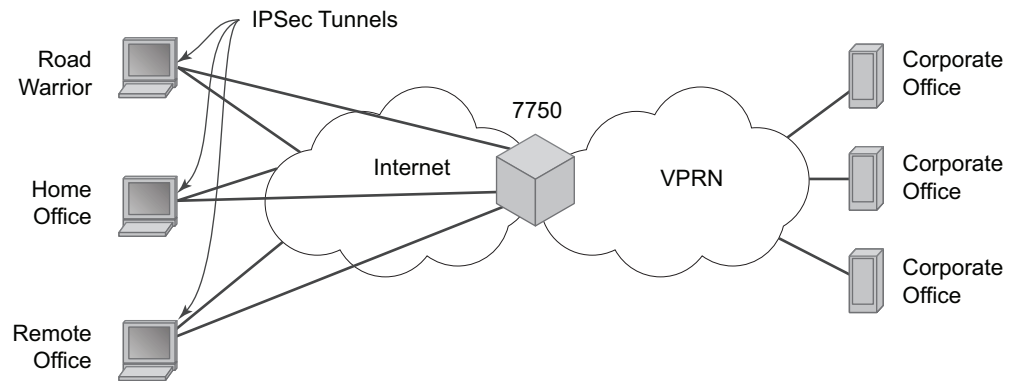
IPsec is the only supported application to use OCSP. With introduction of OCSP, the system supports both CRL and OCSP as the certificate revocation status checking method. For a given ipsec-tunnel or ipsec-gw, the user could configure a primary method, a secondary method and a default result to achieve a hierarchical fallback mechanism. If the primary method fails to return a result, the system will fall back to the secondary method. If the secondary method fails, the fall back proceeds to a default result.

The following lists implementation details:

- Only an OCSP client function is supported.
- HTTP is the only supported transport protocol.
- OCSP server access via management routing instance is not supported.
- SR OS does not sign an OCSP Request.
- The OCSP response must be signed. The system will verify the response by using the signer's certificate included in the response. If there is no such certificate, the CA certificate in the ca-profile will be used.
- If a nextUpdate exists in the OCSP response, the system will check the current time  $\leq$  nextUpdate. If yes, then the response is valid, otherwise the response is considered unreliable. The system will move to next revocation checking method.
- The revocation status result from a valid OCSP response will be cached in the system.
- OCSP can only be used to verify the revocation status of the end-entity certificate. CRL is still needed for CA certificate's status verification.

## 4.8 Video Wholesale Example

**Figure 38** Video Wholesale Configuration



OSSG182

As satellite headend locations can be costly, many municipal and second tier operators cannot justify the investment in their own ground station in order to offer triple play features. However, it is possible for a larger provider or a cooperative of smaller providers to unite and provide a video headend. Each retail subscriber can purchase content from this single station, and receive it over IP. However, encryption is required so the signal cannot be understood if intercepted. A high speed encrypted tunnel is preferred over running two layers of double video protection which is cumbersome and computationally intensive.

## 4.9 Multi-Chassis IPsec Redundancy Overview

This section applies to the 7750 SR, the 7450 ESS running in mixed mode, and VSR.

Multi-Chassis IPsec redundancy (MC-IPsec) provides a 1:1 (active/standby) IPsec stateful failover mechanism between two chassis.

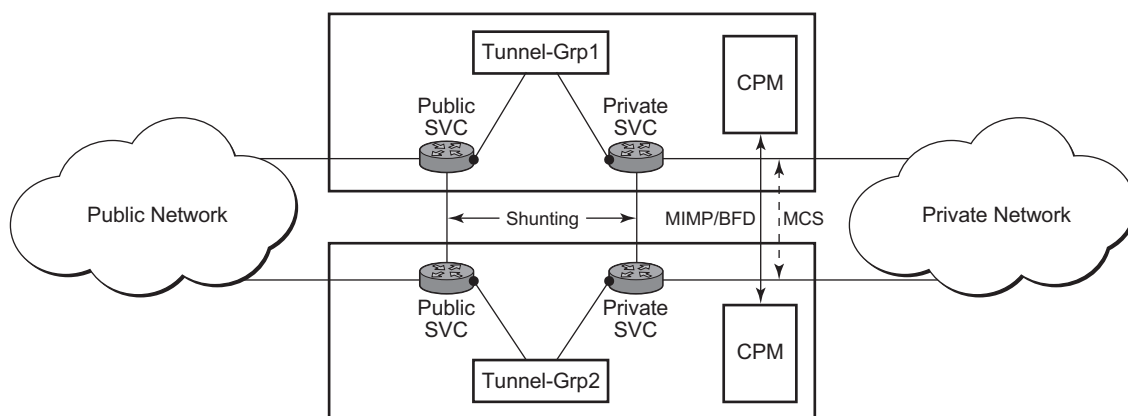
- This feature provides protection against MS-ISA failure and chassis failure.
- MC-IPsec is supported for all types of IKEv2 tunnels, include static LAN-to-LAN, dynamic LAN-to-LAN and remote-access tunnel
- This feature is supported only on multi-active tunnel-groups.
- The granularity of failover is per tunnel-group, which means a specific tunnel-group could failover to standby chassis independent of other tunnel-groups on the master chassis.
- The following components are included in this feature:
  - Master Election: MIMP (MC-IPsec Mastership Protocol) runs between chassis to elect master, MIMP run for each tunnel-group independently
  - Synchronization: MCS (Multi-Chassis Synchronization) sync IPsec states between chassis
  - Routing:
    - MC-IPsec aware routing attract traffic to the master chassis
    - Shunting support
    - MC-IPsec aware VRRP

### 4.9.1 Architecture

The overall MC-IPsec redundancy architecture is displayed in [Figure 39](#).



**Figure 39 MC-IPsec Architecture**



al\_0099

## 4.9.2 MC-IPsec Mastership Protocol (MIMP)

With MIMP enabled, there is a master chassis and a backup chassis. The state of the master or standby is per tunnel-group. For example (Table 26), chassis A and B, for tunnel-group 1, A is master, B is standby; for tunnel-group 2, A is standby, B is master.

**Table 26 Master and Backup Chassis Example**

|                | Master | Standby |
|----------------|--------|---------|
| Tunnel Group 1 | A      | B       |
| Tunnel Group 2 | B      | A       |

All IKEv2 negotiation and ESP traffic encryption/decryption only occurs on the master chassis. If the backup chassis receives such traffic, if possible, it will shunt them to the master.

There will be a mastership election protocol (MIMP) running between the chassis to elect the master. This is an IP-based protocol to avoid any physical topology restrictions.

A central BFD session could be bound to MIMP to achieve fast chassis failure detection.

---

### 4.9.2.1 MIMP Protocol States

There are five MIMP states:

1. discovery
2. notEligible
3. eligible
4. standby
5. master

discovery

- Upon MC-IPsec is enabled for the tunnel-group, for example:
  - System starts up.
  - no shutdown MC-IPsec peer.
  - no shutdown MC-IPsec tunnel-group.
- Functionally, this means blackhole traffic to the MS-ISA and no shunting.
- If the peer is reached before the discovery-interval (configurable) has expired, then the state will be changed to whatever the MIMP decides
- If the peer is not reached before the discovery-interval has expired, then the state will be changed to **eligible** or **notEligible** depending on the oper-status of the tunnel-group.

notEligible

- The tunnel-group is operationally down.
- Functionally, this means blackhole traffic to the MS-ISA and no shunting.

eligible

- The peer is not reachable or the associated BFD session is down but the tunnel-group is operationally up.
- Functionally, this means the MS-ISA processes traffic.

standby

- Peer is reachable, elected standby.
- Functionally, this means blackhole traffic to MS-ISA and shunting if possible.

master

- Peer is reachable, elected master.

- Functionally, this means the MS-ISA processes traffic.

#### 4.9.2.2 Election Logic

The following election logic is executed when MIMP packets are exchanged.

Calculate Master Eligibility:

1. Set masterEligible to TRUE if the local tunnel group is operationally up, otherwise FALSE.
2. Set peerMasterEligible to TRUE if the peer's tunnel group is operationally up, otherwise FALSE.

First elect based on eligibility:

1. If masterEligible and not peerMasterEligible, elect self master → DONE.
2. If not masterEligible and peerMasterEligible, elect peer master → DONE.
3. If not masterEligible and not peerMasterEligible, no master → DONE.

Then apply stickyness rules (mastership tends not to change)

1. If I was "acting master" and peer was not "acting master", then elect self master → DONE.
2. If I was not "acting master" and peer was "acting master", then elect peer master → DONE.

An "acting master" is either in MIMP state "master" or "eligible".

Then elect based on priority and number of active ISA:

1. If my priority is higher than peer, elect self master → DONE.
2. If peer priority is higher than mine, elect peer master → DONE.
3. If I have more active ISA than peer, elect self master → DONE.
4. If peer has more active ISA than me, elect peer master → DONE.

The tie breaker:

1. If the local chassis's MIMP source address is higher than the peer's, elect self master → DONE.
2. Elect peer master → DONE.

### 4.9.2.3 Protection Status

Each MC-IPsec-enabled tunnel-group has a “protection status”, which could be one of following:

- **notReady** — The tunnel-group is not ready for a switchover due to reasons such as no elected standby to takeover or there are pending IPsec states which need to be synced. If switchover occurs with this status, then there could be a significant traffic impact.
- **nominal** — The tunnel-group is in a better situation to switchover than notReady. However, traffic still may be impacted.

Protection status serves as an indication for the operator to decide the optimal time to perform a controlled switchover.

The **show redundancy multi-chassis mc-ipsec peer <ip-address> tunnel-group <tunnel-group-id>** command can be used to check current protection status.

### 4.9.2.4 Other Details

- Mastership election is per tunnel-group.
  - MIMP is running in the base routing instance.
  - MIMP will use the configured value of the **config>redundancy>multi-chassis>peer>source-address** command as the source address. If not configured, then system address will be used.
  - The priority range is from 0 to 255.
  - When an mc-ipsec tunnel-group enters standby from acting master, the tunnel-group will be restarted.
  - When a tunnel-group enters an admin shutdown state under the mc-ipsec configuration (add a tunnel-group to mc-ipsec configuration, or upon admin shutdown of an mc-ipsec enabled tunnel group):
    - All tunnels in the tunnel-group will be deleted/reinstalled to the MS-ISAs.
    - All IKE states associated with those tunnels are locally purged from the MS-ISAs.
    - No IKE messages are sent to the IKE peer.
- These behaviors occur regardless of the presence of a redundant chassis or the state of a redundant chassis.
- With MC-IPsec enabled:
    - auto-establish is blocked.

- For DPD configuration, only **no dpd** and **dpd** configurations with **reply-only** are allowed.

## 4.9.3 Routing

### 4.9.3.1 Routing in Public Service

A /32 route of the local tunnel address is created automatically for all tunnels on the MC-IPsec enabled tunnel-group.

This /32 route can be exported to a routing protocol by a route policy. The protocol type in route-policy is IPsec.

To attract traffic to the master chassis, a route metric of these /32 routes could be set according to the MIMP state, a metric from the master chassis is better than a metric from the standby chassis. There are three available states that can be used in the **from state** command in the route policy entry configuration:

- IPsec-master-with-peer
  - Corresponding MIMP states: master
- IPsec-master-without-peer
  - Corresponding MIMP states: eligible
- IPsec-non-master
  - Corresponding MIMP states: discovery/standby

However, if the standby chassis receives IPsec traffic, the traffic will be shunt to the master chassis by forwarding to a redundant next-hop. The redundant next-hop is an IP next-hop in the public routing instance.

### 4.9.3.2 Routing in Private Services

For static LAN-to-LAN tunnels, the static route with the IPsec tunnel as the next-hop could be exported to a routing protocol by a route policy. The protocol type remains **static**. For dynamic LAN-to-LAN tunnels, the reverse-route could be exported to a routing protocol by a route policy. The protocol type is **ipsec**. For remote-access tunnel, the private interface route could be exported to a routing protocol by a route policy.

Similar to routing in public services, the route metric of the above the routes could be set according to the MIMP state. Only a static route with an IPsec tunnel as the nexthop and reverse route has an MIMP state.

If the standby chassis receives IPsec traffic, the traffic will be shunt to the master chassis by forwarding to a redundant next-hop. The redundant next-hop is an IP next-hop in a private routing instance.

### 4.9.3.3 Other Details About Shunting

Shunting only works when tunnel-group is operationally up.

Shunting is not supported over auto-bind tunnels.

## 4.9.4 MC-IPsec Aware VRRP

In many cases, the public side is a Layer 2 network and VRRP is used to provide link or node protection. However, VRRP and MC-IPsec are two independent processes, each has its own mastership state, which means the VRRP master could be different from MC-IPsec master. This will result unnecessary shunting traffic.

To address this issue, MC-IPsec aware VRRP is introduced in SR OS Release 10.0R8, which add a new priority event in vrrp-policy: mc-ipsec-non-forwarding. If the configured tunnel-group enters non-forwarding (non-master) state, then the priority of associated VRRP instance will be set to the configured value. Delta priority is not supported for this type of event.

## 4.9.5 Synchronization

In order to achieve stateful failover, IPsec states are synced between chassis by using the MCS protocol.

- Only successfully created SA after a completed INITIAL EXCHANGES or CREATE\_CILD\_SA EXCHANGES is synced.
- Upon switchover, the new standby chassis will reboot the tunnel-group.
- The ESP sequence number is not synced.
- The CLI configuration is not synced.

---

The time must be the same on both chassis (using NTP/SNTP to sync to the same server is an option).

#### 4.9.5.1 Automatic CHILD\_SA Rekey

Because the ESP sequence number is not synced, a CHILD\_SA rekey for each tunnel will be initiated by the new master to reset the sequence number upon switchover.

### 4.9.6 Responder Only

With MC-IPsec, it is required that MC-IPsec pair could only act as IKEv2 responder (except for the automatic CHILD\_SA rekey upon switchover). To enable this behavior, configure the following command.

```
config>isa>tunnel-grp>
 ipsec-responder-only
```

Refer to [IPsec Deployment Requirements](#) section for details.

## 4.10 IPsec Deployment Requirements

The following information describes requirements to deploy SR OS IPsec features.

### IPsec General:

To avoid high CPU loads and some complex cases, the following are the requirements to configure IKEv2 lifetime:

1. The IKE\_SA lifetime on one side should be approximately twice as large as the other side. The CHILD\_SA lifetime on one side should be approximately two or three times larger than the other side.
2. With the previous rule, the lifetime of the side with smaller lifetime should not be too small:
  - IKE\_SA:  $\geq 86400$  seconds
  - CHILD\_SA:  $\geq 3600$  seconds
3. With first rule, on the side with the smaller lifetime, the IKE\_SA lifetime should be at least three times larger than CHILD\_SA lifetime.
4. The IKE protocol is the control plane of IPsec, thus, the IKE packet should be treated as high QoS priority in the end-to-end path of the public service.
  - On a public interface, a SAP ingress QoS policy should be configured to ensure the IKE packet is treated as high QoS priority.
5. The correct system time is required for certificate authentication to work properly.
6. The peer's DPD interval must be larger than 30 seconds and should not send a DPD request if it receives IKE or ESP traffic.

### MC-IPsec Specific:

1. The IKEv2 lifetime requirements from the previous **IPsec General** section should be applied with special care to MC-IPsec deployments.

In an MC-IPsec deployment where the MC-IPsec pair peers with single, non-redundant IKE clients, the IKEv2 lifetime requirements must be applied with the larger lifetimes configured on the MC-IPsec pair.

An MC-IPsec deployment where one MC-IPsec pair peers with another MC-IPsec pair is not recommended. MC-IPsec performs optimally when the multi-chassis pair peers with a single IKE entity. If such a peering (MC-to-MC) is created, the above IKEv2 lifetime requirements should still be followed. However, with one side nominated to be the primary rekey initiator and having the smaller configured lifetimes.



2. Responder-only configuration is a mandatory requirement for all types of tunnels on the MC-IPsec pair in the usual deployment scenario of a MC-IPsec pair peering with single, non-redundant IKE clients.
3. DPD on the peer side (following the DPD requirement in the above IPsec General section), **dpd interval 300 max-retries 3 reply-only** on the MC-IPsec side.
4. Dedicated, redundant, direct physical link between chassis with enough bandwidth for MCS and shunting traffic.  
  
MIMP/MCS and BFD for MC-IPsec traffic must be forwarded over resilient links so that a single IOM/IMM, MDA or port failure will not cause the MIMP to go down. Since this control traffic is forwarded in the base routing instance, the base routing instance links need to spread over multiple ports on multiple IOM/IMMs. Proper QoS configuration is needed to make sure the control traffic gets the highest priority.
5. A MC-IPsec switchover when the protection status is not nominal may result in unexpected behavior and traffic loss. A nominal state must be reached on both MC-IPsec chassis before a MC-IPsec switchover is triggered.
6. When using VRRP in the public service and a chassis failure occurs, the VRRP/ Layer 2 network should re-converge before the MC-IPsec switchover occurs. One way to speed up VRRP switchover is to bind a BFD session to VRRP.
7. The system time of the master and standby chassis must be the same. One way to achieve this is for both chassis to sync to an NTP or SNTP server.
8. The CLI configuration is not synchronized via MCS so the user must provision the same IPsec-related configurations on the master and standby chassis. This includes using the same IKE policy ID, tunnel template ID, public or private interface name, and so on.

## 4.11 IKEv2 Remote-Access Tunnel

Since 11.0R6, SR OS supports IKEv2 remote-access tunnel, the difference between a remote-access tunnel and LAN-to-LAN tunnel is remote-access tunnel allows client to request an internal address (and other attributes like DNS address) via IKEv2 configuration payload. The SR OS supports IKEv2 remote-access tunnel with following features:

- Authentication Methods:
  - Pre-Shared-Key with RADIUS (**psk-radius**) or without RADIUS (**psk**)
  - Certificate with RADIUS (**cert-radius**) or without RADIUS (**cert**)
  - EAP/EAP-Only with RADIUS
- Internal address assignment via IKEv2 configuration payload
- Address assignment support:
  - RADIUS server based
  - Local Address assignment
- RADIUS accounting to report address usage
- RADIUS disconnect message to remove tunnel
- NAT-Traversal support
- Support MC-IPsec

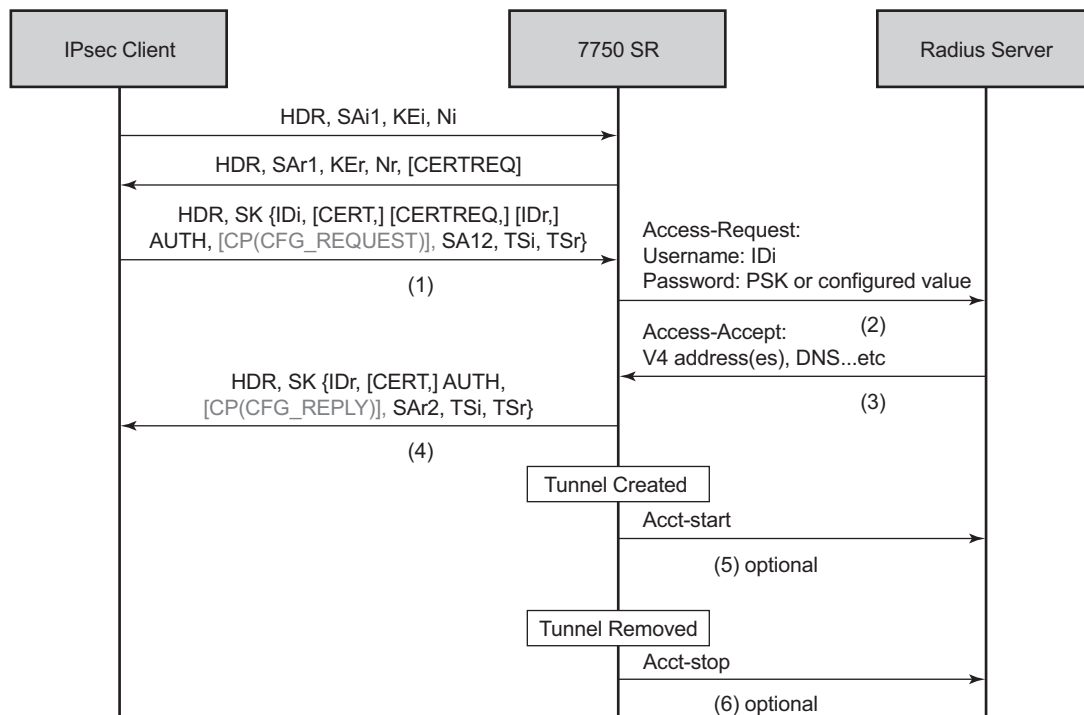
The SR OS only supports address assignments in first CHILD\_SA negotiation.

### 4.11.1 IKEv2 Remote Access Tunnel – RADIUS-Based PSK/Certificate Authentication

If the **auth-method** parameter in the **ike-policy** is configured as **psk-radius** or **cert-radius**, then the system will authenticate the client via PSK or certificate accordingly as like a LAN-to-LAN tunnel. The difference being that in the case of **psk-radius** or **cert-radius**, the system will also perform a RADIUS authentication or authorization and optionally send RADIUS accounting messages.

[Figure 40](#) displays a typical call flow for psk-radius and cert-radius.

**Figure 40** Call Flow for psk-radius/cert-radius



al\_0414

The Access-Request includes following attributes:

- Username: IDi
- User-Password: One of following value's hash according to section 5.2 of RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*.
  - Client's PSK if the psk-radius is configured (refer to the CLI).
  - Otherwise, a CLI configured key via the **password** command in the radius-authentication-policy; if password is not configured in this case, then system will not include User-Password attribute in access-request.
- Acct-Session-Id — Represents the IPsec tunnel session.  
The format is: local\_gw\_ip-remote\_ip:remote\_port-time\_stamp.  
For example: 172.16.100.1-192.168.5.100:500-1365016423.
- Other RADIUS attributes (dependent on the **config>ipsec>radius-auth-policy> include-radius-attribute** configuration).
  - Called-Station-Id: Local tunnel address.
  - Calling-station-Id: Remote tunnel address:port number.
  - Nas-Identifier: The system name.
  - Nas-Ip-Address: The system IP.

---

– Nas-port-id: The public tunnel SAP ID.

If the RADIUS authentication is successful, then the RADIUS sever will an send access-accept message back; otherwise, an access-reject message is sent back.

- The following are supported attributes in access-accept:
- Alc-IPsec-Serv-Id
- Alc-IPsec-Interface
- Framed-IP-Address
- Framed-IP-Netmask
- Alc-Primary-Dns
- Alc-Secondary-Dns
- Alc-IPsec-Tunnel-Template-Id
- Alc-IPsec-SA-Lifetime
- Alc-IPsec-SA-PFS-Group
- Alc-IPsec-SA-Encr-Algorithm
- Alc-IPsec-SA-Auth-Algorithm
- Alc-IPsec-SA-Replay-Window

Once the tunnel is successfully created, the system could optionally (depending on the configuration of the **radius-accounting-policy** under the **ipsec-gw** context), send an accounting-start packet to the RADIUS server, and also send an accounting-stop when the tunnel is removed. The user can also enable the **interim-update** option in the **radius-accounting-policy**.

The following are some attributes included in the acct-start/stop and interim-update:

- Acct-status-type
- Acct-session-id — The same as in the access-request
- Username

The following attributes are dependent on the **radius-acct-policy> include-radius-attribute** configuration:

- Frame-ip-address: the assigned internal address
- Calling-station-id
- Called-station-id
- Nas-Port-Id
- Nas-Ip-Addr
- Nas-Identifier

- Acct-Session-Time: tunnel session time, only in acct-stop packet.

For a complete list of supported attributes, refer to the *7750 SR and VSR RADIUS Attributes Reference Guide*.

The system also supports RADIUS disconnect messages to remove an established tunnel. If **accept-coa** (existing command) is enabled in the radius-server configuration, then the system will accept the disconnect-request message (RFC 5176, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*), and tear down the specified remote-access tunnel.

```
config>router>radius-server>server#
[no] accept-coa
```

For security reasons, the system will only accept a disconnect-request when **accept-coa** is configured **and** the disconnect-request comes from the corresponding server.

The target tunnel is identified by one of following methods:

- Acct-Session-Id
- Nas-Port-Id + Framed-Ip-Addr(Framed-Ipv6-Prefix) + Alc-IPsec-Serv-Id
- User-Name

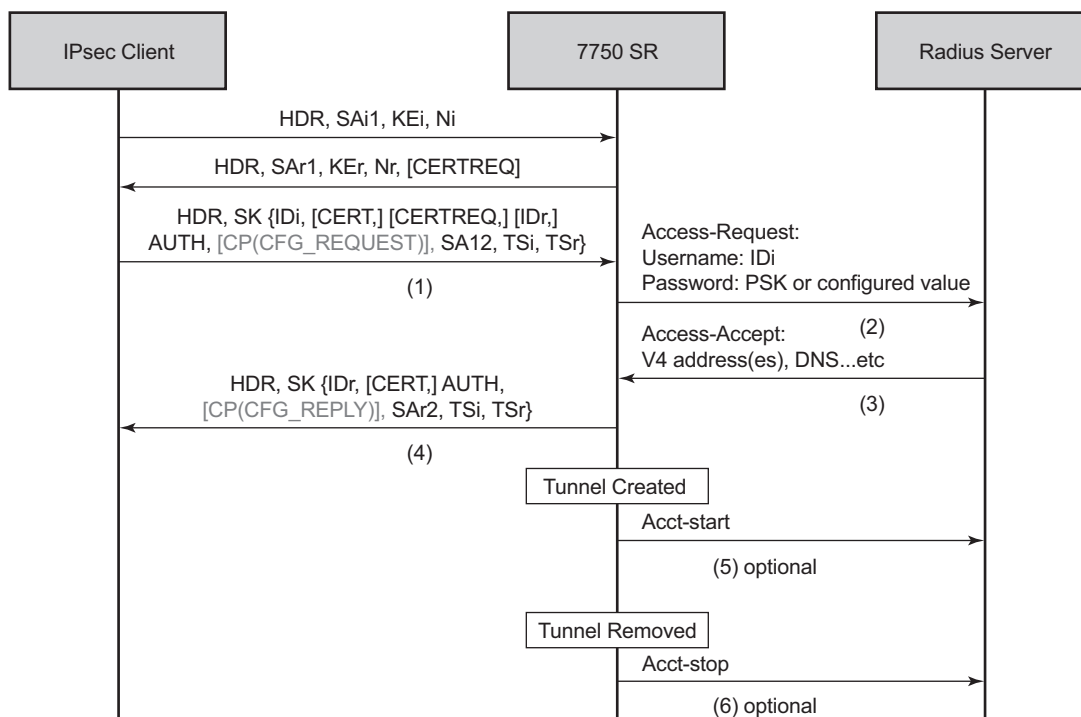
Refer to the *7750 SR and VSR RADIUS Attributes Reference Guide* for more details about disconnect message support.

By default, the system will only return what the client has requested in the CFG\_REQUEST payload. However, this behavior can be overridden by configuring **relay-unsolicited-cfg-attribute** in the **ike-policy**. With this configuration, the configured attributes returned from the source (such as the RADIUS server) will be returned to the client regardless if the client has requested it in the CFG\_REQUEST payload.

#### 4.11.1.1 IKEv2 Remote-Access Tunnel – EAP Authentication

The SR OS supports EAP authentication for a IKEv2 remote-access tunnel, in which case, the system acts as an authenticator between an IPsec client and a RADIUS server. It transparently forwards EAP messages between the IKEv2 session and RADIUS session. Thus, the actual EAP authentication occurs between the client and the RADIUS server.

[Figure 41](#) shows a typical call flow of EAP authentication.

**Figure 41** Typical Call Flow of EAP Authentication

al\_0414

EAP authentication is enabled by configuring **authentication eap**. Once enabled, after the received IKE\_AUTH request from the client, the system sends an EAP-Response/ID with IDi as the value in the access-request to AAA. AAA will return a method request and the system starts passing through between the client and AAA. (as shown in [Figure 41](#)).

The generation of the AUTH payload in the IKE\_AUTH response sent by the SR OS (message 4 in flow shown above) is dependent on the **own-auth-method** configuration:

- psk — The AUTH payload is present and generated by using PSK.
- cert — The AUTH payload is present and generated by the configured public and private key pairs as it does in certificate authentication. Any needed certificates will be also sent.
- eap-only — Neither AUTH nor CERT payload is present.

The RADIUS attributes in authentication and accounting packets are similar as psk-radius and cert-radius with following differences:

- RADIUS attributes support EAP-Message/Message-Authenticator /State attributes

- RADIUS attributes support Access-Challenge packet
- RADIUS attributes support MS-MPPE-Send-Key/ MS-MPPE-Recv-Key in access-accept. These two attributes are required for all EAP methods that generate MSK.

The system provides a method to support EAP and other authentication methods on the same **ipsec-gw** policy. This is enabled by configuring **auto-eap-radius** or **auto-eap** as the **auth-method** in the **ike-policy**.

With **auto-eap-radius**:

- If there is no AUTH payload in an IKE\_AUTH request, then the system uses EAP to authenticate the client and will also use **own-auth-method** to generate the AUTH payload.
- If there is an AUTH payload in the IKE\_AUTH request, the system will use **auto-eap-own-method** to generate the AUTH payload.
  - If the **auto-eap-method** is **psk**, then the system proceeds as auth-method: psk-radius.
  - If the **auto-eap-method** is **cert**, then the system proceeds as auth-method: cert-radius.
  - If **auto-eap-method** is **psk-or-cert**, then:
    - If the Auth Method field of the AUTH payload is PSK, then the system proceeds as **auth-method:psk-radius**.
    - If the Auth Method field of the AUTH payload is RSA or DSS, then the system proceeds as **auth-method:cert-radius**.

With **auto-eap**:

- If there is no AUTH payload in IKE\_AUTH request, then the system uses EAP to authenticate the client and will also use **own-auth-method** to generate AUTH payload.
- If there is an AUTH payload in the IKE\_AUTH request:
  - If the **auto-eap-method** is **psk**, then the system proceeds as auth-method: psk.
  - If the **auto-eap-method** is **cert**, then the system proceeds as auth-method: cert.
  - If the **auto-eap-method** is **psk-or-cert**, then:
    - If the Auth Method field of the AUTH payload is PSK, then the system proceeds as **auth-method psk**.
    - If the Auth Method field of the AUTH payload is RSA or DSS, then the system proceeds as **auth-method cert-auth**

The system will use auto-eap-own-method to generate the AUTH payload.

## 4.11.2 IKEv2 Remote-Access Tunnel – Authentication without RADIUS

To achieve authentication without RADIUS, auth-method need to configured as psk or cert-auth and local address assignment must be configured under ipsec-gw.

Figure 42 shows a typical call flow of certificate or PSK authentication without RADIUS.

**Figure 42** Typical Call Flow of Certificate or PSK Authentication without RADIUS

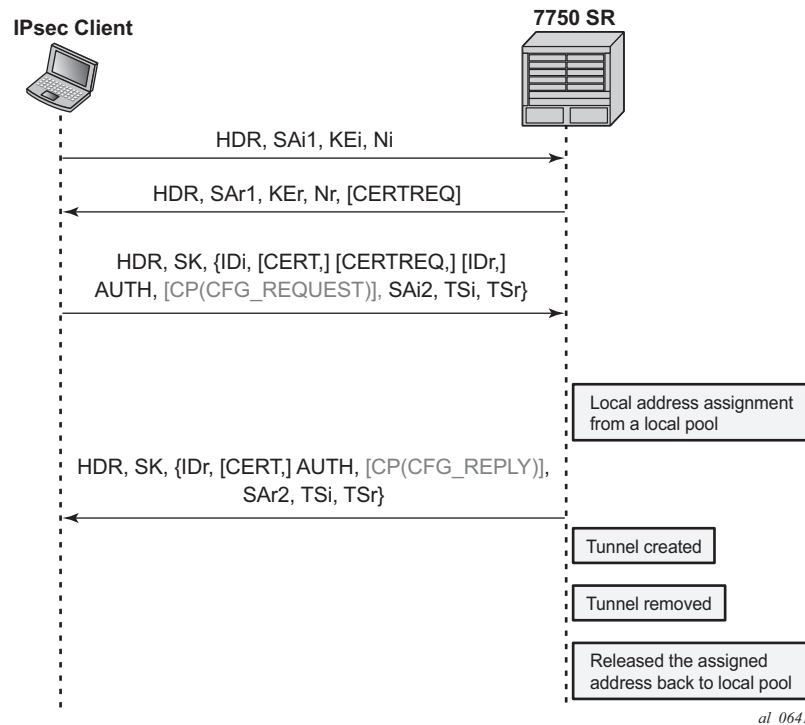
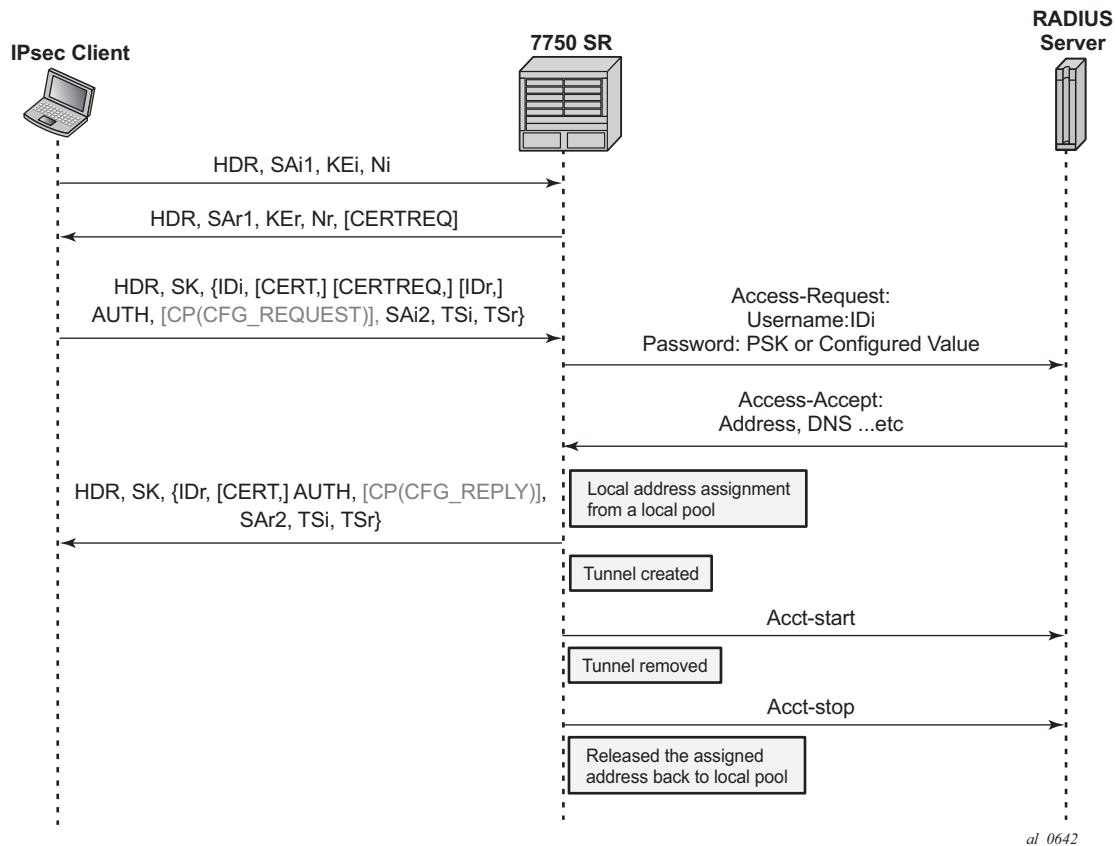


Figure 43 shows a typical call flow for EAP authentication.



**Figure 43 Typical Call Flow for EAP Authentication**



In this configuration, the **radius-authentication-policy** and **radius-accounting-policy** in the **ipsec-gwcontext** are ignored.

RADIUS disconnect messages are supported in this case. Only the following tunnel identification methods are supported:

- Nas-Port-Id + Framed-Ip-Addr(Framed-Ipv6-Prefix) + Alc-IPsec-Serv-Id
- User-Name

### 4.11.3 IKEv2 Remote-Access Tunnel – Address Assignment

The SR OS supports the following methods of address assignment for IKEv2 remote-access tunnels:

- RADIUS

- Local address assignment (LAA)
- DHCPv4/v6

For RADIUS-based address assignment, the address information is returned in an access-accept packet. This implies that RADIUS-based address assignment requires using an authentication method with RADIUS, such as **psk-radius**, **cert-radius**, or **eap**.

For LAA, the system gets an address from a pool defined in a local DHCPv4/v6 server. When a tunnel is removed, the assigned address is released back to the pool. If the local DHCPv4/v6 server is shut down, all existing tunnels that have an address from the server will be removed. If LAA is shut down, the current established tunnel that used LAA will stay up.

For DHCP-based address assignment, the system acts as a DHCP client on behalf of the IPsec client and requests an address from an external DHCP server via the standard DHCP exchange. In this case, the system also acts as a DHCP relay agent, which relays all DHCP packets between the DHCP server and the local DHCP client. DHCP renew and rebind are also supported.

### 4.11.3.1 DHCPv4 Address Assignment

The chaddr in the DHCPv4 header is generated by the SR OS:

- The first 2 bytes of the MAC address are 02:03
- The remaining 4 bytes are the hash result of IKEv2 IDi

The following options are included in the DHCPv4 packets sent by the SR OS:

- Option 82 circuit-id: *private-SAP-id* | *private-interface-name*; for example, tunnel-1.private:100 | priv-int
- Option 82 remote-id: IKEv2 IDi in text format
- Option 61 client-id: 1 byte that represents the IKEv2 IDi type plus the IKEv2 IDi in text format. The value of the first byte is as follows:
  - ID\_IPV4\_ADDR = 1
  - ID\_DER\_ASN1\_DN = 2
  - ID\_FQDN = 3
  - ID\_RFC822\_ADDR = 4
  - ID\_IPV6\_ADDR = 5

### 4.11.3.2 DHCPv6 Address Assignment

Because the system performs a DHCP relay function, all DHCPv6 packets sent or received are encapsulated in DHCPv6 relay-forward and relay-reply messages.

The following items are values of key fields and options in DHCPv6 packets sent by the system:

- Hop-count: 0
- Link address: configurable via the CLI
- Peer-address: auto-generated based on the IKEv2 IDi
- Option 1 Client Identifier
  - DUID type: 2
  - Enterprise ID: 6527
  - Value: 1 byte that represents the IKEv2 IDi type plus the IKEv2 IDi in text format. The value of the first byte is the same as that of the first byte in Option 61 for DHCPv4.
- Option 16 Vendor Class
  - Enterprise ID: 6527
  - Value: string “SROS IPsec”
- Option 18 Interface ID: *private-SAP-id* | *private-interface-name*; for example, tunnel-1.private:100 | priv-int
- Option 37 Remote Identifier
  - Enterprise ID: 6527
  - Value: IKEv2 IDi in text format

### 4.11.3.3 DHCPv4/v6 Usage Notes

- Using a local DHCP server on the same chassis for DHCP-based address assignment is not supported. The DHCP server must be external.
- IPsec DHCP Relay uses only the **gi-address** configuration found under the IPsec gateway and does not take into account **gi-address** with **src-ip-addr** configuration below other interfaces.
- The relay-proxy command (**config>service>vpn>if>dhcp>relay-proxy**) must be enabled on an interface that has a gateway IP address as the interface address in order for the interface to use a DHCPv4 address assignment. The system will ignore other DHCP or DHCPv6 configurations on the interface, with the exception of the relay-proxy configuration.

- If the DHCP server resides in a private service, and the **gi-address** is an address configured on the corresponding tunnel interface, then **relay-proxy** must be enabled on the corresponding private interface.
- If the DHCP server resides in a routing instance that is different from the private service, then there must be an interface (such as a loopback interface) in the routing instance that has the **gi-address** as the interface address, and **gi-address** must be routable for the DHCP server. Also, **relay-proxy** must be enabled on the interface in the routing instance.

The biggest difference between the LAA and DHCP-based methods is that LAA uses a local API to get an address from a local pool. There is no DHCP packet exchange for LAA, while a DHCP-based method uses standard DHCP packet exchange to request a packet from an external DHCP server.

Since there are three methods for address assignment, the following is the priority order (descending) of sources to choose in the event that more than one source is configured:

- LAA
- DHCP
- RADIUS

There is no fallback between the different sources.

LAA/DHCP can work with an authentication method that does not involve RADIUS, as well as with an authentication method that involves RADIUS. When using LAA/DHCP with an authentication method that involves RADIUS, the following applies.

- LAA/DHCP only happens after RADIUS is successfully authenticated.
- The address information returned by the RADIUS server will be ignored (even if LAA/DHCP is configured but is shut down).
- Non-address-related attributes in access-accept messages such as Alc-IPsec-Serv-Id and Alc-IPsec-Tunnel-Template-Id will still be accepted.
- RADIUS accounting is supported in this case, but the Framed-IP-Addr/Framed-IPv6-Prefix reported in the acct-request packet is the LAA/DHCP assigned address, not the address returned by the RADIUS server.
- RADIUS disconnect messages are supported.

For MC-IPsec:

- LAA — The configuration of **config>redundancy>multi-chassis>peer >sync local-dhcp-server** is not needed. This is because the assigned address will be synchronized as part of the IPsec tunnel states.
- DHCP:

- The DHCP packet exchange process only occurs on the master chassis.
  - The assigned address is synchronized to the standby chassis as part of the IPsec states. The standby chassis will not initiate any DHCP exchanges.
  - The configured DHCP server address (**ipsec-gw>dhcp>server**) should be the same on both chassis.
  - After an MC switchover:
    - The new master will not initiate any DHCP process unless it is time to renew an address or a tunnel goes down.
    - If a new master needs to renew an address or release an address, it will send the DHCP packet to the same DHCP server address that assigned the address on the old master, assuming the external DHCP server is still on, and the renew or release will be processed normally.
    - If the new master needs to assign an address for a new tunnel setup, it will send a DHCP discovery or solicit message to all configured DHCP server addresses and then pick the first offer or advertise to finish the DHCP process.
  - For DHCPv4, a gateway IP address is used by the server to forward a response back, so the gateway IP address must be an interface address of the router. For multi-chassis operation, if a DHCPv4 server resides in a private VPRN, there are two options:
    - Configure the same private interface address on both chassis and then use it as the gateway IP address. Configure MC-IPsec-aware routing to make sure that the DHCP response is directed to the master.
    - Configure different private interface addresses with the same subnet on both chassis. The gateway IP address is the private interface address of the local chassis. As well as the private subnet, two /32 private interface address routes from two chassis will also need to be advertised so that the DHCP response is routed to the correct chassis.
- If the DHCPv4 server does not reside in a private VPRN, then one method is to configure a loopback interface with a /32 address in the private subnet, and the loopback interface address will be used as the gateway IP address. Different addresses must be configured on the master and standby chassis.
- For DHCPv6, unlike DHCPv4, the link-address is not used for the server to forward responses back. The DHCPv6 server sends responses to the source address of the request. This typically is the egress interface address when the system sends out the relay-forward message. For MC-IPsec, no special configuration is required as long as the DHCPv6 server can route relay-reply messages back to the correct chassis.

## 4.11.4 IPv6 IPsec Support

The SR OS provides the following IPv6 support to IPsec functions:

- IPv6 packets as the ESP tunnel payload
- IPv6 as the ESP tunnel encapsulation

### 4.11.4.1 IPv6 as Payload

IPv6 as payload allows IPv6 packets to be forwarded within an IPsec tunnel. Current support includes the following:

- Tunnel type support:
  - Static LAN-to-LAN tunnel
  - Dynamic LAN-to-LAN tunnel
  - Remote-access tunnel (only IKEv2 is supported)
- The prefix length of the IPv6 address on a private interface must be /96 or longer

### 4.11.4.2 IPv6 as Payload: Static LAN-to-LAN Tunnel

There are three methods to forward IPv6 traffic into static tunnels on the private side:

1. The destination address is a configured destination IP (**dest-ip**) under the tunnel context
  - The **dest-ip** can be either an IPv6 address or an IPv4 address.
  - In the case of IPv6, it must be either an IPv6 global unicast address or an IPv6 link-local address.
  - In the case of IPv4, it can be used to forward IPv4 traffic into the tunnel.
  - In case of unicast address, dest-ip must be within the prefix configured on the private interface.
  - Up to 16 destination IPs can be configured per ipsec-tunnel.
2. A v6 route with a configured destination IP as the next-hop, this route can be learned from either a static or dynamic from a routing protocol such as BGP.
3. An IPv6 static route with an ipsec-tunnel used as the next-hop.

A security policy supports either an IPv4 entry or an IPv6 entry or both for dual-stack.

#### 4.11.4.3 IPv6 as Payload: Dynamic LAN-to-LAN Tunnel

With dynamic LAN-to-LAN tunnels, the system will automatically create a v6 reverse route in the private VPRN based on the received TSr payload with the tunnel as the nexthop.

#### 4.11.4.4 IPv6 as Payload: Remote-Access Tunnel

The system supports the following IKEv2 IPv6 configuration attributes:

- INTERNAL\_IP6\_ADDRESS
- INTERNAL\_IP6\_DNS

The system supports only one internal IPv6 address per tunnel. The following IPv6-related RADIUS attributes are also supported in access-accept:

- Framed-IPv6-Prefix will be translated into INTERNAL\_IP6\_ADDRESS in the configuration payload, which includes two parts. A 16-byte v6 prefix and a one-byte prefix length.
- Alc-Ipv6-Primary-Dns
- Alc-Ipv6-Secondary-Dns

If an internal v6 address has been assigned to the remote-access client, then the Framed-IPv6-Prefix will also be included in RADIUS accounting-request packet. The assigned internal v6 address must be within the prefix configured on the corresponding private interface.

If the client request both v4 and v6 address and address source (such as RADIUS or LAA) assign both v4 and v6 address, then both v4 and v6 addresses will be assigned to the client via the configuration payload.

#### 4.11.4.5 IPv6 as Encapsulation

IPv6 as encapsulation allows IPv4 or IPv6 packets to be forwarded within an IPv6 ESP tunnel, also the IKE protocol can run over IPv6. Current support includes:

- Tunnel type support:
  - Static LAN-to-LAN tunnel
  - Dynamic LAN-to-LAN tunnel
  - Remote-access tunnel (For IKEv1, only v4 over v6 is supported)

---

For a given **ipsec-gw** or **ipsec-tunnel**, only one local gateway address is supported, which could be either an IPv4 or IPv6 address. The SR OS also provides fragmentation and reassembly support for IPv6 ESP/IKE packets.



## 4.12 MLDv2 over IPsec

The system supports replicating IPv6 multicast traffic into IKEv2 IPsec tunnels based on the MLDv2 report received from the IPsec client.

If a client needs to receive IPv6 multicast traffic over an IPsec tunnel, it includes corresponding multicast address ranges in the traffic selector during CHILD\_SA negotiation. After the CHILD\_SA is created, the client sends an MLDv2 report to join certain multicast groups over the CHILD\_SA. The SeGW terminates the MLDv2 report message and begins replicating requested multicast traffic into the CHILD\_SA.

Internally, the system treats each multicast-enabled CHILD\_SA as an MLD interface called **ipsec-interface** in various multicast show commands.

This feature supports only IPv6 multicast with MLDv2 and Source Specific Multicast (SSM).

This feature supports only IKEv2 tunnels. For IKEv2 static tunnel, this feature only supports a single child SA per tunnel for multicast traffic.

### 4.12.1 MLDv2 over IPsec – Traffic Selector

The negotiated traffic selector of CHILD\_SA that transports IPv6 multicast traffic must include the following address ranges:

- an address range for MLDv2 traffic
- an address range for multicast source (IPv6 global unicast address)
- an address range for expected multicast group

The following is an example of a traffic selector of a CHILD\_SA that only carries multicast traffic:

- TSi
  - FF02::1/128 # destination address of the MLDv2 generic query packet
  - FE80::/64 # IPv6 link local address range, source address of the MLDv2 report packet
  - FF3E::/32 # IPv6 multicast address range, global scope. This is for multicast data traffic and MLDv2 (S,G) specific query
- TSr
  - Multicast source address range (global unicast)

- FF02::16/128 # destination address of the MLDv2 report packet
- FE80::/64 #source address of the MLDv2 query packet

## 4.12.2 MLDv2 over IPsec – Configuration

This feature is enabled by adding private IPsec interface in MLD configuration, for example

```
config>service>vprn>
 mld
 interface "priv"
 no shutdown
 exit
 no shutdown
 exit
 interface "priv" tunnel create
 ipv6
 address 2001:dead::1/96
 exit
 sap tunnel-1.private:200 create
 exit
 exit
```

The MLD configuration under the private interface level is ignored by the system.

## 4.13 Configuring IPsec with CLI

### 4.13.1 Provisioning a Tunnel ISA

A tunnel ISA can only be provisioned on an FP2- or FP3-based IOM. The following output displays a card and ISA configuration.

```
*A:ALA-49>config# info

...
 card 1
 card-type iom4-e
 mda 1
 mda-type me40-1gb-csfp
 no shutdown
 exit
 mda 2
 mda-type isa2-tunnel
 no shutdown
 exit
 no shutdown
 ...

*A:ALA-49>config#
```

### 4.13.2 Configuring a Tunnel Group

The following output displays a tunnel group configuration in the ISA context. The **multi-active** command specifies that there could be multiple active ISAs in the tunnel group, the **mda** command specifies the MDA ID of the ISA in the tunnel group. There could be multiple MDA commands in the tunnel group.

```
*A:ALA-49>config# info

...
 isa
 tunnel-group 1 create
 multi-active
 mda 1/2
 no shutdown
 exit
 exit
 ...

*A:ALA-49>config#
```

### 4.13.3 Configuring Router Interfaces for IPsec

The following output displays an interface “internet” configured using the network port (1/1/1), which provides network connection on the public side.

```
*A:ALA-49>config# info

...
router
 interface "internet"
 address 10.10.7.118/24
 port 1/1/1
 exit
 interface "system"
 address 10.20.1.118/32
 exit
 autonomous-system 123
exit
...

*A:ALA-49>config#
```

### 4.13.4 Configuring IPsec Parameters

The following output displays an IPsec configuration example.

```
config>ipsec
 ike-transform 100 create
 dh-group 14
 ike-auth-algorithm sha256
 ike-encryption-algorithm aes128
 isakmp-lifetime 90000
 exit
 ike-policy 100 create
 ike-version 2
auth-method psk
 ike-transform 100
exit
```

### 4.13.5 Configuring IPsec in Services

The following output displays an IES and VPRN service with IPsec parameters configured.

```
*A:ALA-49>config# info

```

```
...
service
 ies 100 customer 1 create
 interface "ipsec-public" create
 address 10.10.10.1/24
 sap tunnel-1.public:1 create
 exit
 exit
 no shutdown
exit
vpnn 200 customer 1 create
 ipsec
 security-policy 1 create
 entry 1 create
 local-ip 172.16.118.0/24
 remote-ip 172.16.91.0/24
 exit
 exit
 exit
 route-distinguisher 1:1
 interface "ipsec-private" tunnel create
 sap tunnel-1.private:1 create
 ipsec-tunnel "remote-office" create
 security-policy 1
 local-gateway-address 10.10.10.118 peer 10.10.7.91 delivery-
service 100
 dynamic-keying
 ike-policy 1
 pre-shared-key "humptydumpty"
 transform 1
 exit
 no shutdown
 exit
 exit
 exit
 interface "corporate-network" create
 address 172.16.118.118/24
 sap 1/1/2 create
 exit
 exit
 static-route-entry 172.16.91.0/24
 ipsec-tunnel "t1"
 no shutdown
 exit
 exit
 no shutdown
exit
exit
...

*A:ALA-49>config#
```

## 4.13.6 Configuring X.509v3 Certificate Parameters

The following displays steps to configure certificate enrollment.

**1. Generate a key.**

```
admin certificate gen-keypair cf3:/key_plain_rsa2048 size 2048 type rsa
```

**2. Generate a certificate request.**

```
admin certificate gen-local-cert-req keypair cf3:/key_plain_rsa2048 subject-
rdn "C=US,ST=CA,CN=7750" file 7750_req.cs
```

**3. Send the certificate request to CA-1 to sign and get the signed certificate.****4. Import the key.**

```
admin certificate import type key input cf3:/
key_plain_rsa2048 output key1_rsa2048 format der
```

**5. Import the signed certificate.**

```
admin certificate import type cert input cf3:/
7750_cert.pem output 7750cert format pem
```

The following displays steps to configure CA certificate/CRL import.

**1. Import the CA certificate.**

```
admin certificate import type cert input cf3:/
CA_1_cert.pem output ca_cert format pem
```

**2. Import the CA's CRL.**

```
admin certificate import type crl input cf3:/
CA_1_crl.pem output ca_crl format pem
```

The following displays a certificate authentication for IKEv2 static LAN-to-LAN tunnel configuration.

```
config>system>security>pki# info

ca-profile "alu-root" create
cert-file "alu_root.cert"
crl-file "alu_root.crl"
no shutdown
exit

config>ipsec# info

ike-policy 1 create
ike-version 2
auth-method cert-auth
ike-transform 1
exit
ipsec-transform 1 create
exit
ike-transform 1 create
exit
cert-profile "segw" create
entry 1 create
```

```

 cert segw.cert
 key segw.key
 exit
 no shutdown
exit
trust-anchor-profile "nokia" create
 trust-anchor "nokia-root"
exit

config>service>vprn>if>sap

 ipsec-tunnel "t50" create
 security-policy 1
 local-gateway-
address 192.168.55.30 peer 192.168.33.100 delivery-service 300
 dynamic-keying
 ike-policy 1
 transform 1
 cert
 trust-anchor-profile "nokia"
 cert-profile "segw"
 exit
 exit
 no shutdown
exit

```

The following displays an example of the syntax to import a certificate from the pem format.

```

*A:SR-7/Dut-A# admin certificate import type cert input cf3:/pre-import/R1-
0cert.pem output R1-0cert.der format pem

```

The following displays and example of the syntax to export a certificate to the pem format.

```

*A:SR-7/Dut-A# admin certificate export type cert input R1-0cert.der output cf3:/
R1-0cert.pem format pem

```

## 4.13.7 Configuring MC-IPsec

### 4.13.7.1 Configuring MIMP

The following is an MIMP configuration example.

```

config>redundancy>multi-chassis

 peer 10.2.2.2 create
 mc-ipsec
 bfd-enable

```

```

 tunnel-group 1 create
 peer-group 2
 priority 120
 no shutdown
 exit
 exit
 no shutdown
exit

```

The peer's tunnel-group id is not necessarily the same as the local tunnel-group id. With **bfd-enable**, the BFD parameters are specified under the interface that the MIMP source address resides on, which must be a loopback interface in the base routing instance. The default source address of MIMP is the system address.

The **keep-alive-interval** and **hold-on-neighbor-failure** define the MIMP alive parameter, however, BFD could be used for faster chassis failure detection.

The SR OS also provides a **tool** command to manually trigger the switchover such as:

```
tools perform redundancy multi-chassis mc-ipsec force-switchover tunnel-group 1
```

### 4.13.7.2 Configuring Multi-Chassis Synchronization

The following displays an MCS for MC-IPsec configuration.

```

config>redundancy>multi-chassis>

 peer 10.2.2.2 create
 sync
 ipsec
 tunnel-group 1 sync-tag "sync_tag_1" create
 no shutdown
 exit

```

The **sync-tag** must matched on both chassis for the corresponding tunnel-groups.

### 4.13.7.3 Configuring Routing for MC-IPsec

The following configuration is an example using a route policy to export /32 local tunnel address route:

```

config>router>policy-options>

 policy-statement "exportOSPF"
 entry 10
 from

```



```

 protocol ipsec
 state ipsec-master-with-peer
 exit
 action accept
 metric set 500
 exit
exit
entry 20
 from
 protocol ipsec
 state ipsec-non-master
 exit
 action accept
 metric set 1000
 exit
exit
entry 30
 from
 protocol ipsec
 state ipsec-master-without-peer
 exit
 action accept
 metric set 1000
 exit
exit
exit
exit

```

The following configuration shows shunting in public and private service.

Shunting in public service:

```

config>service>ies>
 interface "ipsec-pub" create
 address 172.16.100.254/24
 sap tunnel-1.public:100 create
 exit
 static-tunnel-redundant-next-hop 10.1.1.1
exit

```

Shunting in private service:

```

config>service>vprn>
 interface "ipsec-priv" tunnel create
 ...
 static-tunnel-redundant-next-hop 10.7.7.1
 exit

```

Shunting is enabled by configuring redundant next-hop on a public or private IPsec interface

**static-tunnel-redundant-next-hop** — Shunting nexthop for a static tunnel.

**dynamic-tunnel-redundant-next-hop** — Shunting next-hop for a dynamic tunnel.

## 4.13.8 Configuring and Using CMPv2

CMPv2 server information is configured under corresponding ca-profile by using following key commands:

```
config>system>security>pki>ca-profile
 cmpv2
 url <url-string> [service-id <service-id>]
 response-signing-cert <filename>
 key-list
 key <password> reference <reference-number>
```

The **url** command specifies the HTTP URL of the CMPv2 server, the service specifies the routing instance that the system used to access the CMPv2 server (if omitted, then system will use base routing instance).

The service ID is only needed for inband connections to the server via VPRN services. IES services are not to be referenced by the service ID as any of those are considered base routing instance.

The **response-signing-cert** command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA's certificate will be used.

The **keylist** specifies a list of pre-shared-key used for CMPv2 initial registration message protection.

For example:

```
config>system>security>pki>ca-profile>
 cmpv2
 url "http://cmp.example.com/request" service-id 100
 key-list
 key passwordToBeUsed reference "1"
```

All CMPv2 operations are invoked by using the **admin certificate cmpv2** command.

If there is no **key-list** defined under the **cmpv2** configuration, the system will default to the **cmpv2** transaction input for the command line in regards to authenticating a message without a senderID. Also, if there is no senderID in the response message, and there IS a key-list defined, it will choose the lexicographical first entry only, if that fails, it will have a fail result for the transaction.

Refer to the command reference section for details about syntax and usage. The system supports optional commands (such as, **always-set-sender-ir**) to support inter-op with CMPv2 servers. Refer to [CMPv2 Commands](#) for details.

## 4.13.9 Configuring OCSP

OCSP server information is configured under the corresponding ca-profile:

```
config>system>security>pki>ca-profile>
 ocs
 responder-url <url-string>
 service <service-id>
```

The **responder-url** command specifies the HTTP URL of the OCSP responder. The **service** command specifies the routing instance that system used to access the OCSP responder.

Example:

```
config>system>security>pki>ca-profile>
 ocs
 responder-url "http://ocsp.example.com/request"
 service 100
```

For a given ipsec-tunnel or ipsec-gw, the user can configure a primary method, a secondary method and a default result.

```
config>service>ies>if>sap>ipsec-gw>
config>service>vprn>if>sap>ipsec-gw>
config>service>vprn>if>sap>ipsec-tun>dynamic-keying
 cert
 status-verify
 primary {ocsp | crl} secondary {ocsp | crl}
 default-result {revoked | good}
```

Example:

```
config>service>ies>if>sap>ipsec-gw>dynamic-keying
 cert
 status-verify
 primary ocsp secondary crl
```

## 4.13.10 Configuring IKEv2 Remote — Access Tunnel

The following are configuration tasks for an IKEv2 remote-access tunnel:

- Create an ike-policy with one of the auth-methods that enabled the remote-access tunnel.
- Configure a tunnel-template/ipsec-transform. This is the same as configuring a dynamic LAN-to-LAN tunnel.

- Create a radius-authentication-policy and optionally, a radius-accounting-policy (a radius-server-policy and a radius-server must be preconfigured).
- Configure a private VPRN service and private tunnel interface with an address on the interface. The internal address assigned to the client must come from the subnet on the private interface.
- Configure a public IES/VPRN service and an ipsec-gw under the public tunnel SAP.
- Configure the radius-authentication-policy and radius-accounting-policy (optional) under the ipsec-gw.
- Certificate the related configuration if any certificate related authentication method is used.

The following shows an example using cert-radius:

```
config>system>security>pki# info

 ca-profile "NOKIA-ROOT" create
 cert-file "NOKIA-ROOT.cert"
 crl-file "NOKIA-ROOT.crl"
 no shutdown
 exit

A:SeGW>config>aaa# info

 radius-server-policy "femto-aaa" create
 servers
 router "management"
 server 1 name "svr-1"
 exit
 exit

A:SeGW>config>router# info

 radius-server
 server "svr-
1" address 10.10.10.1 secret "KR35xB3W4aUXtL8o3WzPD." hash2 create
 exit
 exit

config>ipsec# info

 ike-policy 1 create
 ike-version 2
 auth-method cert-radius
 ike-transform 1
 exit
 ipsec-transform 1 create
 exit
 ike-transform 1 create
 exit
 tunnel-template 1 create
 transform 1
 exit
```

```

cert-profile "c1" create
 entry 1 create
 cert SeGW2.cert
 key SeGW2.key
 exit
 no shutdown
exit
trust-anchor-profile "tap-1" create
 trust-anchor "NOKIA-ROOT"
exit
radius-authentication-policy "femto-auth" create
 include-radius-attribute
 calling-station-id
 called-station-id
 exit
 password "DJzlyYKCefyhomnFcFSBuLZovSemMKde" hash2
 radius-server-policy "femto-aaa"
exit
radius-accounting-policy "femto-acct" create
 include-radius-attribute
 calling-station-id
 framed-ip-addr
 exit
 radius-server-policy "femto-aaa"
exit

config>service>ies# info

 interface "pub" create
 address 172.16.100.0/31
 tos-marking-state untrusted
 sap tunnel-1.public:100 create
 ipsec-gw "rw"
 cert
 trust-anchor-profile "tap-1"
 cert-profile "c1"
 exit
 default-secure-service 400 interface "priv"
 default-tunnel-template 1
 ike-policy 1
 local-gateway-address 172.16.100.1
 radius-accounting-policy "femto-acct"
 radius-authentication-policy "femto-auth"
 no shutdown
 exit
 exit
exit
no shutdown

A:SeGW>config>service>vprn# info

 route-distinguisher 400:11
 interface "priv" tunnel create
 address 10.20.20.1/24
 sap tunnel-1.private:200 create
 exit
 exit
 interface "l1" create

```

```

 address 10.9.9.9/32
 loopback
 exit
 no shutdown

```

-----

### 4.13.11 Configuring IKEv2 Remote — Access Tunnel with Local Address Assignment

The following are configuration tasks of IKEv2 remote-access tunnel:

- Create an **ike-policy** with any **auth-method**.
- Configure the **tunnel-template** or **ipsec-transform**. (This is the same as configuring a dynamic LAN-to-LAN tunnel.)
- Configure a private VPRN service and a private tunnel interface with an address on the interface. The internal address assigned to the client must come from the subnet on the private interface.
- Configure a local DHCPv4 or DHCPv6 server with address pool that from which the internal address to be assigned from.
- Configure public IES/VPRN service and **ipsec-gw** under public tunnel SAP.
- Configure the local address assignment under **ipsec-gw**.

The following output shows an example using cert-auth:

```

config>system>security>pki# info

 ca-profile "smallcell-root" create
 cert-file "smallcell-root-ca.cert"
 revocation-check crl-optional
 no shutdown
 exit

config>ipsec# info

 ike-policy 3 create
 ike-version 2
 auth-method cert-auth
 nat-traversal
 ike-transform 1
 exit
 ipsec-transform 1 create
 exit
 ike-transform 1 create
 exit
 cert-profile "segw-mlab" create
 entry 1 create
 cert SeGW-MLAB.cert
 key SeGW-MLAB.key

```

```

 exit
 no shutdown
 exit
 trust-anchor-profile "sc-root" create
 trust-anchor "smallcell-root"
 exit
 tunnel-template 1 create
 transform 1
 exit

config>service>ies# info

 interface "pub" create
 address 172.16.100.253/24
 tos-marking-state untrusted
 sap tunnel-1.public:100 create
 ipsec-gw "rw"
 default-secure-service 400 interface "priv"
 default-tunnel-template 1
 ike-policy 3
 local-address-assignment
 ipv6
 address-source router 400 dhcp-server "d6" pool "1"
 exit
 no shutdown
 exit
 local-gateway-address 172.16.100.1
 cert
 trust-anchor-profile "sc-root"
 cert-profile "segw-mlab"
 status-verify
 default-result good
 exit
 exit
 local-id type fqdn value segwmobilelab.nokia.com
 no shutdown
 exit
 exit
 exit
 no shutdown

config>service>vprn# info

 dhcp6
 local-dhcp-server "d6" create
 use-pool-from-client
 pool "1" create
 options
 dns-server 2001:db8::808:808
 exit
 exclude-prefix 2001:db8:beef::101/128
 prefix 2001:db8::beef::/96 failover access-driven pd wan-
host create
 exit
 exit
 no shutdown
 exit
 exit
 route-distinguisher 400:1

```

---

```
interface "priv" tunnel create
 ipv6
 address 2001:db8::beef::101/96
 exit
 sap tunnel-1.private:200 create
 exit
exit
no shutdown
```

-----



---

## 4.14 IP Tunnel Command Reference

### 4.14.1 Command Hierarchies

- [Hardware Commands](#)
- [ISA Commands](#)
- [IPsec Commands](#)
  - [Certificate Profile Commands](#)
  - [Client Database Commands](#)
  - [Internet Key Exchange \(IKE\) Commands](#)
  - [IPsec Transform Commands](#)
  - [RADIUS Policy Commands](#)
  - [IPsec Static Security Association Commands](#)
  - [IPsec Static Security Association Commands](#)
  - [Trust Anchor Profile/TS List Commands](#)
- [Service Configuration Commands](#)
  - [IES Commands](#)
  - [VPRN Commands](#)
  - [IPsec Mastership Election Commands](#)
  - [Related Commands](#)
  - [CMPv2 Commands](#)
  - [Auto-Update Commands](#)
- [Show Commands](#)
- [Debug Commands](#)
- [Tools Commands](#)
- [Clear Commands](#)
- [Admin Commands](#)

## 4.14.1.1 Configuration Commands

### 4.14.1.1.1 Hardware Commands

```

config
 — card slot-number
 — mda mda-slot
 — mda-type isa-tunnel
 — no mda-type

```

### 4.14.1.1.2 ISA Commands

```

config
 — isa
 — tunnel-group tunnel-group-id [create]
 — tunnel-group tunnel-group-id isa-scale-mode isa-scale-mode [create]
 — no tunnel-group tunnel-group-id
 — active-mda-number number
 — no active-mda-number
 — backup mda-id
 — no backup
 — description description-string
 — no description
 — [no] ipsec-responder-only
 — [no] mda mda-id
 — [no] multi-active
 — primary mda-id
 — no primary
 — reassembly [wait-msecs]
 — no reassembly
 — [no] shutdown
 — stats-collection
 — [no] isa-dp-cpu-usage

```

### 4.14.1.1.3 IPsec Commands

#### Certificate Profile Commands

```

config
 — ipsec
 — cert-profile profile-name [create]
 — no cert-profile profile-name
 — entry entry-id [create]
 — no entry entry-id
 — cert cert-filename
 — no cert

```

- **key** *key-filename*
- **no key**
- **rsa-signature** {pkcs1 | pss}
- **[no] send-chain**
  - **[no] ca-profile** *name*
- **[no] shutdown**

## Client Database Commands

- ```
config
— ipsec
  — client-db db-name [create]
  — no client-db db-name
    — client client-index [create]
    — no client client-index
      — client-identification
        — idi any
        — idi ipv4-prefix {any | ipv4-prefix/ipv4-prefix-length}
        — idi ipv6-prefix {any | ipv6-prefix/ipv6-prefix-length}
        — idi string-type string-type string-value string-value
        — no idi
        — peer-ip-prefix ip-prefix/ip-prefix-length
        — peer-ip-prefix ipv4-any
        — peer-ip-prefix ipv6-any
        — no peer-ip-prefix
      — client-name name
      — no client-name
      — credential
        — pre-shared-key key [hash | hash2]
        — no pre-shared-key
      — private-interface ip-int-name
      — no private-interface
      — private-service service-id
      — private-service name service-name
      — no private-service
      — [no] shutdown
      — ts-negotiation ts-list list-name
      — no ts-negotiation
      — tunnel-template tunnel-template-id
      — no tunnel-template
    — description description-string
    — no description
    — match-list
      — [no] idi
      — [no] peer-ip-prefix
    — [no] shutdown
```

Internet Key Exchange (IKE) Commands

- ```
config
— ipsec
 — ike-policy ike-policy-id [create]
 — no ike-policy ike-policy-id
```

- **auth-method** {psk | plain-psk-xauth | cert-auth | psk-radius | cert-radius | eap | auto-eap-radius | auto-eap}
- **no auth-method**
- **auto-eap-method** {psk | cert | psk-or-cert}
- **auto-eap-own-method** {psk | cert}
- **description** *description-string*
- **no description**
- **dpd** [interval *interval*] [max-retries *max-retries*] [reply-only]
- **no dpd**
- **ike-mode** {main | aggressive}
- **no ike-mode**
- **ike-transform** *ike-transform-id* [*ike-transform-id*]
- **no ike-transform**
- **ike-version** {1 | 2}
- [no] **ikev1-ph1-responder-delete-notify**
- **ikev2-fragment** *mtu* *octets* *reassemble-timeout* *seconds*
- **no ikev2-fragment**
- **ipsec-lifetime** *ipsec-lifetime*
- **no ipsec-lifetime**
- **limit-init-exchange** [*reduced-max-exchange-timeout* *seconds*]
- **no limit-init-exchange**
- **lockout** *failed-attempts* *count* *duration* *duration-minutes* **block** *block-minutes* [*max-port-per-ip* *number-of-ports*]
- **no lockout**
- [no] **match-peer-id-to-cert**
- **nat-traversal** [force] [keep-alive-interval *keep-alive-interval*] [force-keep-alive]
- **no nat-traversal**
- **own-auth-method** {psk | cert | eap-only}
- **no own-auth-method**
- **pfs** [dh-group {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21}]
- **no pfs**
- **relay-unsolicited-cfg-attribute**
  - [no] **internal-ip4-address**
  - [no] **internal-ip4-dns**
  - [no] **internal-ip4-netmask**
  - [no] **internal-ip6-dns**
  - [no] **internal-ip6-address**
- [no] **send-idr-after-eap-success**
- **ike-transform** *ike-transform-id* [create]
- **ike-transform** *ike-transform-id*
  - **dh-group** {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21}
  - **ike-auth-algorithm** *auth-algorithm*
  - **ike-encryption-algorithm** *encryption-algorithm*
  - **isakmp-lifetime** *seconds*
- [no] **show-ipsec-keys**

## IPsec Transform Commands

### config

- **ipsec**
  - **ipsec-transform** *transform-id* [create]
  - **no ipsec-transform** *transform-id*

- **esp-auth-algorithm** {null | md5 | sha1 | sha256 | sha384 | sha512 | aes-xcbc | auth-encryption}
- **no esp-auth-algorithm**
- **esp-encryption-algorithm** {null | des | 3des | aes128 | aes192 | aes256 | aes128-gcm8 | aes128-gcm12 | aes128-gcm16 | aes192-gcm8 | aes192-gcm12 | aes192-gcm16 | aes256-gcm8 | aes256-gcm12 | aes256-gcm16 | null-aes128-gmac | null-aes192-gmac | null-aes256-gmac}
- **no esp-encryption-algorithm**
- **ipsec-lifetime** *seconds*
- **ipsec-lifetime** inherit
- **pfs-dh-group** {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21}
- **pfs-dh-group** inherit
- **no pfs-dh-group**

## RADIUS Policy Commands

- ```
config
  — ipsec
    — radius-accounting-policy name [create]
    — no radius-accounting-policy name
      — [no] include-radius-attribute
        — [no] acct-stats
        — [no] called-station-id
        — [no] calling-station-id
        — [no] client-cert-subject-key-id
        — [no] framed-ip-addr
        — [no] framed-ipv6-prefix
        — [no] nas-identifier
        — [no] nas-ip-addr
        — [no] nas-port-id
      — radius-server-policy radius-server-policy-name
      — no radius-server-policy
      — update-interval minutes [jitter seconds]
      — no update-interval
    — radius-authentication-policy name [create]
    — no radius-authentication-policy name
      — [no] include-radius-attribute
        — [no] called-station-id
        — [no] calling-station-id
        — [no] client-cert-subject-key-id
        — [no] nas-identifier
        — [no] nas-ip-addr
        — [no] nas-port-id
      — password password [hash | hash2]
      — no password
      — radius-server-policy radius-server-policy-name
      — no radius-server-policy
```

IPsec Static Security Association Commands

- ```
config
 — ipsec
 — static-sa sa-name [create]
```

- **no static-sa** *sa-name*
  - **authentication** *auth-algorithm ascii-key ascii-string*
  - **authentication** *auth-algorithm hex-key hex-string [hash|hash2]*
  - **no authentication**
  - **description** *description-string*
  - **no description**
  - **direction** *ipsec-direction*
  - **no direction**
  - **protocol** *ipsec-protocol*
  - **no protocol**
  - **spi** *spi*
  - **no spi**

### Trust Anchor Profile/TS List Commands

- ```
config
  — ipsec
    — trust-anchor-profile name [create]
    — no trust-anchor-profile name
      — [no] trust-anchor ca-profile-name
    — ts-list list-name [create]
    — no ts-list list-name
      — local
        — entry entry-id [create]
        — no entry entry-id
          — address prefix ip-prefix/ip-prefix-len
          — address from begin-ip-address to end-ip-address
          — no address
          — protocol any
          — protocol protocol-id port opaque
          — protocol protocol-id port any
          — protocol protocol-id port from begin-port-id to end-port-id
          — no protocol
        — remote
          — entry entry-id [create]
          — no entry entry-id
            — address prefix ip-prefix/ip-prefix-len
            — address from begin-ip-address to end-ip-address
            — no address
            — protocol any
            — protocol protocol-id port opaque
            — protocol protocol-id port any
            — protocol protocol-id port from begin-port-id to end-port-id
            — no protocol
```

Tunnel Template Commands

- ```
config
 — ipsec
 — tunnel-template ipsec-template-identifier [create]
 — no tunnel-template ipsec-template-identifier
 — [no] clear-df-bit
 — description description-string
```

- **no description**
- **encapsulated-ip-mtu** *octets*
- **no encapsulated-ip-mtu**
- **icmp6-generation**
  - **pkt-too-big** *interval seconds*
  - **pkt-too-big** *message-count count*
  - **[no] pkt-too-big**
- **ip-mtu** *octets*
- **no ip-mtu**
- **private-tcp-mss-adjust** *octets*
- **no private-tcp-mss-adjust**
- **public-tcp-mss-adjust** **auto**
- **public-tcp-mss-adjust** *octets*
- **no public-tcp-mss-adjust**
- **replay-window** {32 | 64 | 128 | 256 | 512}
- **no replay-window**
- **[no] sp-reverse-route**
- **transform** *transform-id [transform-id]*
- **no transform**

## 4.14.1.2 Service Configuration Commands

### 4.14.1.2.1 IES Commands

- ```

config
  — service
    — ies service-id [customer customer-id] [vpn vpn-id] [name name]
      — interface ip-int-name [tunnel]
        — dynamic-tunnel-redundant-next-hop ip-address
        — no dynamic-tunnel-redundant-next-hop
        — sap sap-id [create]
          — ip-tunnel ip-tunnel-name [create]
          — no ip-tunnel ip-tunnel-name
            — backup-remote-ip ip-address
            — no backup-remote-ip
            — [no] clear-df-bit
            — delivery-service {service-id | svc-name}
            — no delivery-service
            — description description-string
            — no description
            — [no] dest-ip ip-address
            — dscp dscp-name
            — no dscp
            — [no] gre-header
            — gre-header send-key send-key receive-key receive-key
            — ip-mtu octets
            — no ip-mtu
            — private-tcp-mss-adjust octets
            — no private-tcp-mss-adjust

```

-
- **public-tcp-mss-adjust** *octets*
 - **public-tcp-mss-adjust** **auto**
 - **no private-tcp-mss-adjust**
 - **reassemble** [*wait-msecs*]
 - **no reassemble**
 - **remote-ip** *ip-address*
 - **no remote-ip**
 - **[no] shutdown**
 - **source** *ip-address*
 - **no source**
 - **ipsec-gw** *name*
 - **no ipsec-gw**
 - **cert**
 - **cert-profile** *name*
 - **no cert-profile**
 - **status-verify**
 - **default-result** {*revoked* | *good*}
 - **no default-result**
 - **primary** *primary* **secondary** *secondary*
 - **trust-anchor-profile** *name*
 - **no trust-anchor-profile**
 - **client-db** *name*
 - **client-db** *name* **fallback**
 - **client-db** *name* **no-fallback**
 - **no client-db**
 - **default-secure-service** *service-id* **interface** *ip-int-name*
 - **no default-secure-service**
 - **default-tunnel-template** *ipsec-template-identifier*
 - **no default-tunnel-template**
 - **[no] dhcp**
 - **gi-address** *ip-address*
 - **no gi-address**
 - **[no] send-release**
 - **server** *ip-address* [*ip-address...*(up to 8 max)]
router *router-instance*
 - **server** *ip-address* [*ip-address...*(up to 8 max)]
service-name *service-name*
 - **no server**
 - **[no] shutdown**
 - **[no] dhcp6**
 - **link-address** *ipv6-address*
 - **no link-address**
 - **[no] send-release**
 - **server** *ip-address* [*ip-address*] **router** *router-instance*
 - **server** *ip-address* [*ip-address*] **service-name** *service-name*
 - **no server**
 - **[no] shutdown**
 - **ike-policy** *ike-policy-id*
 - **no ike-policy**
 - **[no] local-address-assignment**
 - **ipv4**

- **address-source** **router** *router-instance*
 - dhcp-server** *local-dhcp4-svr-name*
 - pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]
- **address-source** **service-name** *service-name*
 - dhcp-server** *local-dhcp4-svr-name*
 - pool** *dhcp4-server-pool*
 - [**secondary-pool** *secondary-pool-name*]
- **no address-source**
- **ipv6**
 - **address-source** **router** *router-instance*
 - dhcp-server** *local-dhcp6-svr-name*
 - pool** *dhcp6-server-pool*
 - **address-source** **service-name** *service-name*
 - dhcp-server** *local-dhcp6-svr-name*
 - pool** *dhcp6-server-pool*
 - **no address-source**
- **[no] shutdown**
- **local-gateway-address** *ip-address*
- **no local-gateway-address**
- **local-id** **type** {*ipv4* | *fqdn* | *ipv6*} [*value value*]
- **no local-id**
- **max-history-esp-key-records** *max-records*
- **no max-history-esp-key-records**
- **max-history-ike-key-records** *max-records*
- **no max-history-ike-key-records**
- **pre-shared-key** *key* [{*hash* | *hash2*}]
- **no pre-shared-key**
- **radius-accounting-policy** *policy-name*
- **no radius-accounting-policy**
- **radius-authentication-policy** *name*
- **no radius-authentication-policy**
- **[no] shutdown**
- **ts-negotiation** **ts-list** *list-name*
- **no ts-negotiation**
- **static-tunnel-redundant-next-hop** *ip-address*
- **no static-tunnel-redundant-next-hop**

4.14.1.2.2 VPRN Commands

- ```

config
— service
 — vpn service-id [name name] [customer customer-id] [create]
 — no vpn service-id
 — ipsec
 — [no] allow-reverse-route-override
 — security-policy security-policy-id [create]
 — no security-policy security-policy-id
 — entry entry-id [create]
 — no entry entry-id

```

```

— local-ip {ip-prefix/prefix-length | ip-prefix netmask | any}
— local-v6-ip ipv6-prefix/prefix-length
— local-v6-ip any
— no local-v6-ip
— remote-ip {ip-prefix/prefix-length | ip-prefix netmask |
any}
— remote-v6-ip any
— remote-v6-ip ipv6-prefix/prefix-length
— no remote-v6-ip

config
— service
— vpn service-id [name name] [customer customer-id] [create]
— no vpn service-id
— interface ip-int-name [create]
— interface ip-int-name [create] tunnel
— no interface ip-int-name
— dynamic-tunnel-redundant-next-hop ip-address
— no dynamic-tunnel-redundant-next-hop
— ipv6
— address ipv6-address/prefix-length [eui-64] [preferred] [track-
srrp srrp-instance] [modifier cga-modifier] [dad-disable]
[primary-preference primary-preference]
— no address ipv6-address/prefix-length
— link-local-address ipv6-address [dad-disable]
— no link-local-address
— sap sap-id [create]
— no sap sap-id
— ip-tunnel ip-tunnel-name [create]
— no ip-tunnel ip-tunnel-name
— backup-remote-ip ip-address
— no backup-remote-ip
— [no] clear-df-bit
— delivery-service {service-id | svc-name}
— no delivery-service
— description description-string
— no description
— [no] dest-ip ip-address
— dscp dscp-name
— no dscp
— [no] gre-header
— gre-header send-key send-key receive-key receive-key
— ip-mtu octets
— no ip-mtu
— private-tcp-mss-adjust octets
— no private-tcp-mss-adjust
— public-tcp-mss-adjust auto
— public-tcp-mss-adjust octets
— no public-tcp-mss-adjust
— reassemble [wait-msecs]
— no reassemble
— remote-ip ip-address
— no remote-ip
— [no] shutdown

```

- **source** *ip-address*
- **no source**
- [no] **ipsec-gw**
  - **cert**
    - **cert-profile** *profile*
    - **no cert-profile**
    - **status-verify**
      - **default-result** {revoked | good}
      - **no default-result**
      - **primary** *primary* **secondary** *secondary*
    - **trust-anchor-profile** *name*
    - **no trust-anchor-profile**
  - **client-db** *name*
  - **client-db** *name* **fallback**
  - **client-db** *name* **no-fallback**
  - **client-db** *name*
  - **no client-db**
  - **default-secure-service** *service-id* **interface** *ip-int-name*
  - **no default-secure-service**
  - **default-tunnel-template** *ipsec-template-identifier*
  - **no default-tunnel-template**
- [no] **dhcp**
  - **gi-address** *ip-address*
  - **no gi-address**
  - [no] **send-release**
  - **server** *ip-address* [*ip-address*] **router** *router-instance*
  - **server** *ip-address* [*ip-address*] **service-name** *service-name*
  - **no server**
  - [no] **shutdown**
- [no] **dhcp6**
  - **link-address** *ip-address*
  - **no link-address**
  - [no] **send-release**
  - **server** *ip-address* [*ip-address*] **router** *router-instance*
  - **server** *ip-address* [*ip-address*] **service-name** *service-name*
  - **no server**
  - [no] **shutdown**
- **ike-policy** *ike-policy-id*
- **no ike-policy**
- [no] **local-address-assignment**
  - **ipv4**
    - **address-source** **router** *router-instance* **dhcp-server** *local-dhcp4-svr-name* **pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]
    - **address-source** **service-name** *service-name* **dhcp-server** *local-dhcp4-svr-name* **pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]

---

```

— no address-source
— ipv6
— address-source router router-instance
 dhcp-server local-dhcp6-svr-name
 pool dhcp6-server-pool
— address-source service-name service-
 name dhcp-server local-dhcp6-svr-
 name pool dhcp6-server-pool
— no address-source
— [no] shutdown
— local-gateway-address ip-address
— no local-gateway-address
— local-id type {ipv4 | fqdn | ipv6} [value value]
— no local-id
— max-history-esp-key-records max-records
— no max-history-esp-key-records
— max-history-ike-key-records max-records
— no max-history-ike-key-records
— pre-shared-key key [{hash | hash2}]
— no pre-shared-key
— radius-accounting-policy policy-name
— no radius-accounting-policy
— radius-authentication-policy name
— no radius-authentication-policy
— [no] shutdown
— ts-negotiation ts-list list-name
— no ts-negotiation
— ipsec-tunnel ipsec-tunnel-name [create]
— no ipsec-tunnel ipsec-tunnel-name
— [no] bfd-designate
— [no] bfd-enable {service service-id | service-name
 service-name} interface interface-name dst-ip ip-
 address
— [no] clear-df-bit
— description description-string
— no description
— [no] dest-ip ip-address
— [no] dynamic-keying
— [no] auto-establish
— cert
— cert-profile profile
— no cert-profile
— status-verify
— default-result {revoked | good}
— no default-result
— primary primary secondary
 secondary
— trust-anchor-profile name
— no trust-anchor-profile
— ike-policy ike-policy-id
— no ike-policy
— local-id type {ipv4 | fqdn | ipv6} [value value]
— no local-id
— pre-shared-key key [{hash | hash2}]

```

- **no pre-shared-key**
- **transform** *transform-id* [*transform-id*...(up to 4 max)]
- **no transform**
- **encapsulated-ip-mtu** *octets*
- **no encapsulated-ip-mtu**
- **icmp6-generation**
  - **pkt-too-big**
  - **pkt-too-big** *interval seconds*
  - **pkt-too-big** *message-count count*
  - **no pkt-too-big**
- **ip-mtu** *octets*
- **no ip-mtu**
- **local-gateway-address** *ip-address* **peer** *ip-address* **delivery-service** *service-id*
- **no local-gateway-address**
- **[no] manual-keying**
  - **security-association** *security-entry-id* **authentication-key** *authentication-key* **encryption-key** *encryption-key spi spi* **transform** *transform-id* **direction** {*inbound* | *outbound*}
  - **no security-association** *security-entry-id* **direction** {*inbound* | *outbound*}
- **max-history-esp-key-records** *max-records*
- **no max-history-esp-key-records**
- **max-history-ike-key-records** *max-records*
- **no max-history-ike-key-records**
- **private-tcp-mss-adjust** *octets*
- **no private-tcp-mss-adjust**
- **public-tcp-mss-adjust** **auto**
- **public-tcp-mss-adjust** *octets*
- **no public-tcp-mss-adjust**
- **replay-window** {*32* | *64* | *128* | *256* | *512*}
- **no replay-window**
- **security-policy** *security-policy-id* [**strict-match**]
- **no security-policy**
- **static-tunnel-redundant-next-hop** *ip-address*
- **no static-tunnel-redundant-next-hop**

#### 4.14.1.2.3 IPsec Mastership Election Commands

- ```
configure
  — redundancy
    — multi-chassis
      — peer ip-address [create]
      — no peer ip-address
      — [no] mc-ipsec
        — [no] bfd-enable
        — discovery-interval interval-secs [boot interval-secs]
        — no discovery-interval
```

- **hold-on-neighbor-failure** *multiplier*
- **no hold-on-neighbor-failure**
- **keep-alive-interval** *interval*
- **no keep-alive-interval**
- **tunnel-group** *tunnel-group-id* [**create**]
- **no tunnel-group** *tunnel-group-id*
 - **peer-group** *tunnel-group-id*
 - **no peer-group**
 - **priority** *priority*
 - **no priority**
 - [**no**] **shutdown**

4.14.1.2.4 Related Commands

- ```

config
 — router
 — policy-options
 — policy-statement
 — entry
 — from
 — state state
 — no state

config
 — redundancy
 — multi-chassis
 — peer
 — sync
 — [no] ipsec
 — tunnel-group tunnel-group-id sync-tag tag-name [create]
 — no tunnel-group tunnel-group-id

```

#### 4.14.1.2.5 CMPv2 Commands

- ```

config
  — system
    — security
      — pki
        — ca-profile name [create]
        — no ca-profile name
          — cmpv2
            — [no] accept-unprotected-errormsg
            — [no] accept-unprotected-pkiconf
            — [no] always-set-sender-for-ir
            — http-response-timeout timeout
            — no http-response-timeout
            — http-version [1.0 | 1.1]
            — key-list

```

- **key** *password* [**hash** | **hash2**] *reference*
reference-number
- **no key** *reference* *reference-number*
- **response-signing-cert** *filename*
- **no response-signing-cert**
- **[no] same-recipnonce-for-pollreq**
- **url** *url-string* [**service-id** *service-id*]
- **url** *url-string* [**service-name** *service-name*]
- **no url**
- **revocation-check** {**crl** | **crl-optional**}
- **certificate-display-format** {**ascii** | **utf8**}

admin

- **certificate**
 - **cmpv2**
 - **cert-request** **ca** *ca-profile-name* **current-key** *key-filename* **current-cert** *cert-filename* [**hash-alg** *hash-algorithm*] **newkey** *key-filename* **subject-dn** *subject-dn* [**domain-name** *domain-names*] [**ip-addr** , *ip-address* | *ipv6-address* ,] **save-as** *save-path-of-result-cert*
 - **clear-request** **ca** *ca-profile-name*
 - **initial-registration** **ca** *ca-profile-name* **key-to-certify** *key-filename* **protection-alg** {**password** *password* *reference* *ref-number* | **signature** [**cert** *cert-file-name* [**send-chain** [**with-ca** *ca-profile-name*]]] [**protection-key** *key-file-name*] [**hash-alg** {**md5** | **sha1** | **sha224** | **sha256** | **sha384** | **sha512**}] } **subject-dn** *dn* [**domain-name** *domain-names*] [**ip-addr** , *ip-address*|*ipv6-address* ,] **save-as** *save-path-of-result-cert*
 - **key-update** **ca** *ca-profile-name* **newkey** *key-filename* **oldkey** *key-filename* **oldcert** *cert-filename* [**hash-alg** *hash-algorithm*] **save-as** *save-path-of-result-cert*
 - **poll** **ca** *ca-profile-name*
 - **show-request** [**ca** *ca-profile-name*]

4.14.1.2.6 Auto-Update Commands

config

- **system**
 - **file-transmission-profile** *name* [**create**]
 - **no file-transmission-profile** *name*
 - **ipv4-source-address** *ip-address*
 - **no ipv4-source-address**
 - **ipv6-source-address** *ipv6-address*
 - **no ipv6-source-address**
 - **redirection** *level*
 - **no redirection**
 - **retry** *count*
 - **no retry**
 - **router** *router-instance*
 - **router service** *vpn-service-name*
 - **timeout** *seconds*

config

```

— system
  — security
    — pki
      — ca-profile name [create]
      — no ca-profile name
        — auto-crl-update [create]
        — no auto-crl-update
          — crl-urls
            — url-entry entry-id [create]
            — no url-entry entry-id
              — file-transmission-profile profile-name
              — no file-transmission-profile
              — url url
              — no url
            — periodic-update-interval [days days] [hrs hours] [min
              minutes] [sec seconds]
            — pre-update-time [days days] [hrs hours] [min minutes]
              [sec seconds]
            — retry-interval seconds
            — no retry-interval
            — schedule-type schedule-type
            — [no] shutdown
  admin
    — certificate
      — crl-update ca ca-profile-name

```


4.14.1.2.7 Show Commands

```

show
  — ipsec
    — cert-profile name association
    — cert-profile [name]
    — cert-profile name entry [value]
    — certificate filename association
    — client-db
    — client-db db-name association
    — client-db db-name client client-index
    — client-db db-name
    — gateway name name
    — gateway [name name] tunnel [private-address-type private-address-type]
    — gateway [service service-id] [oper-state oper-state]
    — gateway tunnel [ip-address:port]
    — gateway name name tunnel ip-address:port
    — gateway name name tunnel
    — gateway [name name] tunnel state state
    — gateway [name name] tunnel idi-value idi-prefix
    — gateway tunnel count
    — gateway tunnel [private-address-type private-address-type]
    — ike-policy
    — ike-policy ike-policy-id
    — ike-policy ike-policy-id association [all]
    — ike-transform [ike-transform-id]
    — lockout router router-id local-gateway-address local-gateway-address mda mda
    — lockout router router-id local-gateway-address local-gateway-address remote ip-
      address[:port]
    — lockout router router-id mda mda
    — radius-accounting-policy [name]
    — radius-authentication-policy [name]
    — security-policy service service-id [security-policy-id security-policy-id]
    — security-policy
    — service service-id
    — static-sa
    — static-sa name sa-name
    — static-sa spi spi
    — transform [transform-id]
    — trust-anchor-profile trust-anchor-profile association
    — trust-anchor-profile [trust-anchor-profile ]
    — ts-list [list-name]
    — ts-list list-name association [all]
    — ts-list list-name local-entry [1..32]
    — ts-list list-name remote-entry [1..32]
    — ts-list list-name {local | remote}
    — tunnel ipsec-tunnel-name
    — tunnel
    — tunnel count
    — tunnel state state
    — tunnel-template [ipsec-template-identifier]
    — tunnel-template ipsec-template-identifier association [all]
  — redundancy
  
```

```

— multi-chassis
  — mc-ipsec peer ip-address tunnel-group tunnel-group-id
  — mc-ipsec peer ip-address

show
  — isa
    — statistics
      — ip-tunnel-stats
        — number-of-tunnels tunnel-type tunnel-type isa mda
        — number-of-tunnels tunnel-type tunnel-type system
        — number-of-tunnels tunnel-type tunnel-type tunnel-group tunnel-
          group-id
        — throughput tunnel-type tunnel-type system [history-stats-in-count
          count] [history-stats-in-min minutes] [current]
        — throughput tunnel-type tunnel-type type type system [history-stats-
          in-count count] [history-stats-in-min minutes] [current] [show-
          oid]
        — throughput tunnel-type tunnel-type isa mda [history-stats-in-count
          count] [history-stats-in-min minutes] [current]
        — throughput tunnel-type tunnel-type type type isa mda [history-stats-
          in-count count] [history-stats-in-min minutes] [current] [show-
          oid]
        — throughput tunnel-type tunnel-type tunnel-group tunnel-group-id
          [history-stats-in-count count] [history-stats-in-min minutes]
          [current]
        — throughput tunnel-type tunnel-type type type tunnel-group tunnel-
          group-id [history-stats-in-count count] [history-stats-in-min
          minutes] [current] [show-oid]
        — traffic-forward tunnel-type tunnel-type [type type] isa mda
      — ipsec-stats
        — ike-exchange-failure-rate gateway name
        — ike-exchange-failure-rate reason reason gateway name [show-oid]
        — ike-exchange-failure-rate isa mda
        — ike-exchange-failure-rate reason reason isa mda [show-oid]
        — ike-exchange-failure-rate system
        — ike-exchange-failure-rate reason reason system [show-oid]
        — ike-exchange-failure-rate tunnel-group tunnel-group-id [history-
          stats-in-count count] [history-stats-in-min minutes] [current]
        — ike-exchange-failure-rate reason reason tunnel-group tunnel-group-
          id [history-stats-in-count count] [history-stats-in-min minutes]
          [current] [show-oid]
        — ikev2-msg-drop message-type message-type isa mda [show-oid]
        — number-of-tunnels gateway name [history-stats-in-count count]
          [history-stats-in-min minutes] [current]
        — number-of-tunnels tunnel-type tunnel-type gateway name [history-
          stats-in-count count] [history-stats-in-min minutes] [current]
          [show-oid]
        — number-of-tunnels isa mda [history-stats-in-count count] [history-
          stats-in-min minutes] [current]
        — number-of-tunnels tunnel-type tunnel-type isa mda [history-stats-in-
          count count] [history-stats-in-min minutes] [current] [show-oid]
        — number-of-tunnels system [history-stats-in-count count] [history-
          stats-in-min minutes] [current]

```

-
- **number-of-tunnels** *tunnel-type tunnel-type system* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]
 - **number-of-tunnels** *tunnel-group tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current]
 - **number-of-tunnels** *tunnel-type tunnel-type tunnel-group tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]
 - **throughput** *gateway name* [history-stats-in-count *count*] [history-stats-in-min *min*] [current]
 - **throughput** *type type gateway name* [history-stats-in-count *count*] [history-stats-in-min *min*] [current] [show-oid]
 - **throughput** *isa mda* [history-stats-in-count *count*] [history-stats-in-min *min*] [current]
 - **throughput** *type type isa mda* [history-stats-in-count *count*] [history-stats-in-min *min*] [current] [show-oid]
 - **throughput** *system* [history-stats-in-count *count*] [history-stats-in-min *min*] [current]
 - **throughput** *type type system* [history-stats-in-count *count*] [history-stats-in-min *min*] [current] [show-oid]
 - **throughput** *tunnel-group tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *min*] [current]
 - **throughput** *type type tunnel-group tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *min*] [current] [show-oid]
 - **traffic-forward** [type *type*] *gateway name*
 - **traffic-forward** [type *type*] *isa mda*
 - **traffic-forward** [type *type*] *gateway name dynamic-tunnel ip-address:port*
 - **traffic-forward** [type *type*] *tunnel ipsec-tunnel-name*
 - **tunnel-setup-rate** *gateway name* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current]
 - **tunnel-setup-rate** *tunnel-type tunnel-type gateway name* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]
 - **tunnel-setup-rate** *isa mda* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current]
 - **tunnel-setup-rate** *tunnel-type tunnel-type isa mda* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]
 - **tunnel-setup-rate** *system* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current]
 - **tunnel-setup-rate** *tunnel-type tunnel-type system* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]
 - **tunnel-setup-rate** *tunnel-group tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current]
 - **tunnel-setup-rate** *tunnel-type tunnel-type tunnel-group tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]
 - **tunnel-isa**
 - **cpu-usage** *mda* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current]
 - **cpu-usage** *mda* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid] *type {control-plane | data-plane}*
 - **memory-allocation-failure-rate** *mda* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]

4.14.1.2.8 Debug Commands

```

debug
  — certificate
    — [no] auto-crl-updates
      — [no] ca-profile profile-name
    — [no] cmpv2
      — [no] ca-profile profile-name
    — [no] ocsp
      — [no] ca-profile profile-name
  — ipsec
    — [no] certificate filename
    — [no] no client-db db-name
    — gateway name name tunnel ip-address[:port] [nat-ip nat-ip[:port]] [detail] [no-dpd-debug] [display-keys]
    — no gateway name name tunnel ip-address[:port] [nat-ip nat-ip[:port]]
    — gateway name name tunnel-subnet ip-prefix/ip-prefix-length [port port] [detail] [no-dpd-debug] [display-keys]
    — no gateway name name tunnel-subnet ip-prefix/ip-prefix-length
    — tunnel ipsec-tunnel-name [detail] [no-dpd-debug] [display-keys]
    — no tunnel ipsec-tunnel-name

```

4.14.1.2.9 Tools Commands

```

tools
  — dump
    — ipsec
      — stats
        — ike-stats gateway name [dynamic-tunnel ip-address:port]
        — ike-stats isa mda
        — ike-stats ipsec-tunnel-name
  — perform
    — ipsec
      — client-db db-name lookup peer-ip peer-ip-address
      — client-db db-name lookup idi string-type {fqdn | rfc822} string-value string-value [peer-ip peer-ip-address]
      — client-db db-name lookup idi address idi-ip-address [peer-ip peer-ip-address]
      — ike-initiate tunnel-group-id ipsec-group-id
      — ike-initiate tunnel-name ipsec-tunnel-name
    — redundancy
      — multi-chassis
        — mc-ipsec
          — force-switchover tunnel-group local-group-id [now][to {master | standby}]

```

4.14.1.2.10 Clear Commands

```

clear

```

- **ipsec**
 - **gateway** *name name tunnel ip-address:port* [**statistics**] [**saved-key**]
 - **gateway** *name name tunnel ip-address:port*
 - **gateway** *name name* [**saved-key**]
 - **gateway** *name name tunnel ip-address:port* [**saved-key**]
 - **lockout** *router router-id*
 - **lockout** *router router-id local-gateway-address local-gateway-address*
 - **lockout** *router router-id local-gateway-address local-gateway-address remote ip-address[:port]*
 - **stats**
 - **ike-stats** *gateway name* [**dynamic-tunnel ip-address:port**]
 - **ike-stats** *isa mda*
 - **ike-stats** *ipsec-tunnel-name*
 - **tunnel** *ipsec-tunnel-name*
 - **tunnel** *ipsec-tunnel-name* [**saved-key**]
 - **tunnel** *ipsec-tunnel-name* [**stats**] [**saved-key**]
 - **tunnel** *isa mda* [**saved-key**]

4.14.1.2.11 Admin Commands

- admin**
 - **ipsec**
 - **display-key** *type {ike | esp} gateway name name dynamic-tunnel ip-address:port*
 - **display-key** *type {ike | esp} tunnel ipsec-tunnel-name*

4.14.2 Command Descriptions

4.14.2.1 Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>ipsec>client-db config>ipsec>client-db>client config>ipsec>ike-policy config>ipsec>tnl-temp config>isa>ipsec-group config>isa>tunnel-group config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-tunnel

Description	This command creates a text description which is stored in the configuration file to help identify the content of the entity. The no form of the command removes the string from the configuration.
Parameters	<i>string</i> — The description character string. Allowed values are any string up to 80 characters in length composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	<pre>config>ipsec>cert-profile config>ipsec>client-db config>ipsec>client-db>client config>isa config>isa>aa-group config>isa>tunnel-grp config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group config>service>ies>if>sap>ip-tunnel config>service>ies>if>sap>ipsec-gw config>service>ies>if>sap>ipsec-gw>dhcp config>service>ies>if>sap>ipsec-gw>dhcp6 config>service>ies>if>sap>ipsec-gw>lcl-addr-assign config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw>dhcp config>service>vprn>if>sap>ipsec-gw>dhcp6 config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign</pre>
Description	This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command. The shutdown command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

4.14.2.2 Hardware Commands

mda-type

Syntax	mda-type <i>isa-tunnel</i>

	no mda-type
Context	config>card>mda
Description	This command provisions or de-provisions an MDA to or from the device configuration for the slot.
Parameters	<i>isa-tunnel</i> — Specifies the ISA tunnel.

4.14.2.3 ISA Commands

isa

Syntax	isa
Context	config
Description	This command enables the context to configure Integrated Services Adapter (ISA) parameters.

tunnel-group

Syntax	tunnel-group <i>tunnel-group-id</i> [create] tunnel-group <i>tunnel-group-id</i> isa-scale-mode <i>isa-scale-mode</i> [create] no tunnel-group <i>tunnel-group-id</i>
Context	config>isa
Description	This command allows a tunnel group to be created or edited. A tunnel group is a set of one or more MS-ISAs that support the origination and termination of IPsec and IP/GRE tunnels. All of the MS-ISAs in a tunnel group must have <i>isa-tunnel</i> as their configured <i>mda-type</i>. On VSR, isa-scale-mode must be specified, which defines the number of tunnels on each ISA. The no form of the command deletes the specified tunnel group from the configuration
Parameters	<i>tunnel-group-id</i> — Identifies the tunnel-group. Values 1 to 16 <i>isa-scale-mode</i> — Defines the maximum number of all tunnels (all types combined) which can be established on each ISA of the tunnel group. create — Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled or disabled in the environment>create context.

active-mda-number

Syntax	active-mda-number <i>number</i> no active-mda-number
Context	config>isa>tunnel-grp
Description	This command specifies the number of active MS-ISA within all configured MS-ISA in the tunnel-group with multi-active enabled. IPsec traffic will be load balanced across all active MS-ISAs. If the number of configured MS-ISA is greater than the active-mda-number then the delta number of MS-ISA will be backup.
Default	active-mda-number 1
Parameters	<i>number</i> — Specifies the number of active MDAs. Values 1 to 16

backup

Syntax	backup <i>mda-id</i> no backup
Context	config>isa>tunnel-grp
Description	This command assigns an ISA IPsec module configured in the specified slot to this IPsec group. The backup module provides the IPsec group with warm redundancy when the primary module in the group is configured. An IPsec group must always have a primary configured. Primary and backup modules have equal operational status and when both modules are coming up, the one that becomes operational first becomes the active module. An IPsec module can serve as a backup for multiple IPsec groups but the backup can become active for only one ISA IPsec group at a time. All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPsec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported. The operator is notified through SNMP events when: • When the ISA IPsec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active). • When ISA IPsec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up). • When an ISA IPsec activity switch took place. The no form of the command removes the specified module from the IPsec group.

Default	no backup
Parameters	<i>mda-id</i> — Specifies the card/slot identifying a provisioned module to be used as a backup module.
Values	mda-id: <i>slot/mda</i> slot 1 to up to 10 depending on chassis model mda 1 to 2

mda

Syntax	[no] mda <i>mda-id</i>
Context	config>isa>tunnel-grp
Description	This command specifies the MDA ID of the MS-ISA as the member of tunnel-group with multi-active enabled. Up to 16 MDA could be configured under the same tunnel-group.
Parameters	<i>mda-id</i> — Specifies the id of MS-ISA.
Values	iom-slot-id/mda-slot-id

ipsec-responder-only

Syntax	[no] ipsec-responder-only
Context	config>isa>tunnel-group
Description	With this command configured, system will only act as IKE responder except for the automatic CHILD_SA re-key upon MC-IPsec switchover.
Default	no ipsec-responder-only

multi-active

Syntax	[no] multi-active
Context	config>isa>tunnel-grp
Description	This command enables configuring multiple active MS-ISA in the tunnel-group. IPsec traffic will be load balanced to configured active MS-ISAs. Operational notes: • A shutdown of group and removal of all existing configured tunnels of the tunnel-group are needed before provisioning command “multi-active”. • If the tunnel-group is admin-up with “multi-active” configured then the configuration of “primary” and “backup” are not allowed.

- The active-mda-number must be $\leq$ total number of ISA configured.
 - If active-mda-number is less than total number of ISA configured then the delta number of ISA will become backup ISA.

Default no multi-active

primary

Syntax **primary** *mda-id*
no primary

Context config>isa>tunnel-grp

Description This command assigns an ISA IPsec module configured in the specified slot to this IPsec group. The backup ISA IPsec provides the IPsec group with warm redundancy when the primary ISA IPsec in the group is configured. Primary and backup ISA IPsec have equal operational status and when both MDAs are coming up, the one that becomes operational first becomes the active ISA IPsec.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPsec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPsec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPsec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPsec activity switch took place.

The **no** form of the command removes the specified primary ID from the group's configuration.

Default no primary

Parameters *mda-id* — Specifies the card/slot identifying a provisioned IPsec ISA.

reassembly

Syntax **reassembly** [*wait-msecs*]
no reassembly

Context config>isa>tunnel-group
config>service>ies>if>sap>gre-tunnel
config>service>vprn>if>sap>gre-tunnel

Description	This command configures IP packet reassembly for IPsec and GRE tunnels supported by an MS-ISA. The reassemble command at the tunnel-group level configures IP packet reassembly for all IPsec and GRE tunnels associated with the tunnel-group. The reassemble command at the GRE tunnel level configures IP packet reassembly for that one specific GRE tunnel, overriding the tunnel-group configuration. The no form of the command disables IP packet reassembly.
Default	no reassembly (tunnel-group level) reassemble (gre-tunnel level)
Parameters	wait — Specifies the maximum number of milliseconds that the ISA tunnel application will wait to receive all fragments of a particular IPsec or GRE packet. If one or more fragments are still missing when this limit is reached the partially reassembled datagram is discarded and an ICMP time exceeded message is sent to the source host (if allowed by the ICMP configuration of the sending interface). Internally, the configured value is rounded up to the nearest multiple of 100 ms. Values 1 to 5000 Default 2000 (tunnel-group level)

stats-collection

Syntax	stats-collection
Context	config>isa>tunnel-grp
Description	This command enables the context to configure ISA statistics collection parameters.

isa-dp-cpu-usage

Syntax	[no] isa-dp-cpu-usage
Context	config>isa>tunnel-grp>stats-collection
Description	This command enables the system to collect statistics used to derive ISA CPU data plane usage. When enabled, this command impacts the ISA performance.

4.14.2.4 Certificate Profile Commands

cert-profile

Syntax	cert-profile <i>profile-name</i> [create]

no cert-profile *profile-name*

Context	config>ipsec
Description	This command creates a new cert-profile or enters the configuration context of an existing cert-profile. The no form of the command removes the profile name from the cert-profile configuration.
Parameters	<i>profile-name</i> — Specifies the name of the certification profile up to 32 characters.

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>ipsec>cert-profile
Description	This command configures the certificate profile entry information. The no form of the command removes the <i>entry-id</i> value from the cert-profile configuration.
Parameters	<i>entry-id</i> — Specifies the entry ID. Values 1 to 8

cert

Syntax	cert <i>cert-filename</i> no cert
Context	config>ipsec>cert-profile>entry
Description	This command specifies the file name of an imported certificate for the cert-profile entry. The no form of the command removes the cert-file-name from the entry configuration.
Default	no cert

key

Syntax	key <i>key-filename</i> no key
Context	config>ipsec>cert-profile>entry
Description	This command specifies the filename of an imported key for the cert-profile entry.

The **no** form of the command removes the key filename from the entry configuration.

Default	no key
Parameters	<i>key-filename</i> — Specifies the filename of an imported key.

rsa-signature

Syntax	rsa-signature { pkcs1 pss }
Context	config>ipsec>cert-profile>entry
Description	This command specifies the signature scheme for RSA key.
Default	pkcs1
Parameters	pkcs1 — Specifies the RSA pkcs#1 v1.5 signature scheme. pss — Specifies the RSA probabilistic signature scheme.

send-chain

Syntax	[no] send-chain
Context	config>ipsec>cert-profile>entry
Description	This command enters the configuration context of send-chain in the cert-profile entry . The configuration of this command is optional, by default system will only send the certificate specified by cert command in the selected entry to the peer. This command allows system to send additional CA certificates to the peer. These additional CA certificates must be in the certificate chain of the certificate specified by the cert command in the same entry.

ca-profile

Syntax	[no] ca-profile <i>name</i>
Context	config>ipsec>cert-profile>entry>send-chain
Description	This command specifies a CA certificate in the specified ca-profile to be sent to the peer. Multiple configurations (up to seven) of this command are allowed in the same entry.
Parameters	<i>name</i> — Specifies the profile name up to 32 characters.

4.14.2.5 Client Database Commands

client-db

Syntax	client-db <i>db-name</i> [create] no client-db <i>db-name</i>
Context	config>ipsec
Description	This command creates a new IPsec client-db or enters the configuration context of an existing client-db. An IPsec client-db can be used for IKEv2 dynamic LAN-to-LAN tunnel authentication and authorization. When a new tunnel request is received, the system will match the request to the client entries configured in client-db and use credentials returned by the matched client entry for authentication. If authentication succeeds, the system could also use the IPsec configuration parameters (such as private-service-id) returned by the matched entry to set up the tunnel. The configured client-db is referenced under the ipsec-gw configuration context using the client-db command. The no form of the command removes the <i>db-name</i> from the configuration.
Parameters	<i>db-name</i> — Specifies the name of this IPsec client up to 32 characters. create — Keyword used to create the security policy instance. The create keyword requirement can be enabled or disabled in the environment>create context.

client

Syntax	client <i>client-index</i> [create] no client <i>client-index</i>
Context	config>ipsec>client-db
Description	This command creates a new IPsec client entry in the client-db or enters the configuration context of an existing client entry. There may be multiple client entries defined in the same client-db. If there are multiple entries that match the new tunnel request, then the system will select the entry that has smallest client-index. The no form of the command reverts to the default.
Parameters	client-index — Specifies the ID of the client entry. Values 1 to 8000

create — Keyword used to create the security policy instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

client-identification

Syntax	client-identification
Context	config>ipsec>client-db>client
Description	This command enables the context to configure client ID information of this IPsec client. If there are multiple match input are configured in the match-list of the client-db, then all corresponding match criteria must be configured for the client-entry.

idi

Syntax	idi any idi ipv4-prefix { any <i>ipv4-prefix/ipv4-prefix-length</i> } idi ipv6-prefix { any <i>ipv6-prefix/ipv6-prefix-length</i> } idi string-type <i>string-type</i> string-value <i>string-value</i> no idi
Context	config>ipsec>client-db> client>client-id
Description	This command specifies a match criteria that uses the peer's identification initiator (IDi) as the input, only one IDi criteria can be configured for a given client entry. This command supports the following matching methods: • idi any: Matches any type of IDi with any value. • idi ipv4-prefix: Matches an IDi with the type ID_IPV4_ADDR. If the any parameter is specified, then it will match any IPv4 address. If an IPv4 prefix is specified, then it will match an IPv4 address that is within the specified prefix. • idi ipv6-prefix: Matches an IDi with the type ID_IPV6_ADDR. If the any parameter is specified, then it will match any IPv6 address. If an IPv6 prefix is specified, then it will match an IPv6 address that is within the specified prefix. • idi string-type: Supports following type of IDi: – FQDN: Either a full match or a suffix match – RFC822: Either a full match or a suffix match The no form of the command reverts to the default.
Default	no idi
Parameters	any — Matches any type of IDi with any value. <i>ipv4-prefix/ipv4-prefix-length</i> — Matches any IPv4 address and prefix.

ipv6-prefix/ipv6-prefix-length — Matches any IPv6 address and prefix.

string-type — Matches the type of IDi value for this IPsec client entry.

Values fqdn, fqdn-suffix, rfc822, rfc822-suffix

string-value — Matches the IDi value within the client ID for this IPsec client entry up to 256 characters.

peer-ip-prefix

Syntax	peer-ip-prefix <i>ip-prefix/ip-prefix-length</i> peer-ip-prefix ipv4-any peer-ip-prefix ipv6-any no peer-ip-prefix
Context	config>ipsec>client-db> client>client-id
Description	This command specifies match criteria that uses the peer's tunnel IP address as the input. Only one peer-ip-prefix criteria can be configured for a given client entry. The no form of the command reverts to the default.
Default	no peer-ip-prefix
Parameters	<i>ip-prefix/ip-prefix-length</i> — Specifies an IPv4 or IPv6 prefix. It is considered a match if the peer's tunnel IP address is within the specified prefix. ipv4-any — Matches any IPv4 address. ipv6-any — Matches any IPv6 address.

client-name

Syntax	client-name <i>name</i> no client-name
Context	config>ipsec>client-db>client
Description	This command specifies the name of the client entry. The client name can be used in CLI navigation or in show commands.
Default	no client-name
Parameters	<i>name</i> — Specifies the name of the client.

credential

Syntax	credential
Context	config>ipsec>client-db>client
Description	This command enables the context to configure the parameters used to authenticate peers.

pre-shared-key

Syntax	pre-shared-key <i>key</i> [hash hash2] no pre-shared-key
Context	config>ipsec>client-db>client>credential
Description	This command specifies a pre-shared key used to authenticate peers. The no form of the command reverts to the default.
Default	no pre-shared-key
Parameters	key — An ASCII string to use as the pre-shared key for dynamic keying. When the hash or hash2 parameters are not used, the key is a clear text key; otherwise, the key text is encrypted. hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the hash2 encrypted variable cannot be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

private-interface

Syntax	private-interface <i>ip-int-name</i> no private-interface
Context	config>ipsec>client-db>client
Description	This command specifies the private interface name that is used for tunnel setup. The no form of the command reverts to the default.
Default	no private-interface

Parameters *ip-int-name* — Specifies the name of the private interface.

private-service

Syntax **private-service** *service-id*
 private-service name *service-name*
 no private-service

Context config>ipsec>client-db>client

Description This command specifies the private service ID that is used for tunnel setup.

 The **no** form of the command reverts to the default.

Default no private-service

Parameters *service-id* — Specifies the service ID of the tunnel delivery service.
 This variant of the command is only supported in 'classic' configuration-mode
 (**configure system management-interface configuration-mode classic**). The
 private-service name *service-name* variant can be used in all configuration modes.

Values {*id* | *svc-name*}

id: 1 to 2147483647
 svc-name: up to 64 characters (*svc-name* is an alias for input only. The
 svc-name gets replaced with an id automatically by SR OS
 in the configuration).

name *service-name* — Identifies the service, up to 64 characters.

ts-negotiation

Syntax **ts-negotiation ts-list** *list-name*
 no ts-negotiation

Context config>ipsec>client-db>client

Description This command specifies the traffic selector (TS) to be used for tunnel setup.

 The no form of the command reverts to the default.

Default no ts-negotiation

Parameters *list-name* — Specifies the TS list used by this tunnel, up to 32 characters.

tunnel-template

Syntax	tunnel-template <i>tunnel-template-id</i> no tunnel-template
Context	config>ipsec>client-db>client
Description	This command specifies the tunnel template to be used for tunnel setup. The no form of the command reverts to the default.
Default	no tunnel-template
Parameters	<i>tunnel-template-id</i> — Specifies the identifier of the tunnel template. Values 1 to 2048

match-list

Syntax	match-list
Context	config>ipsec>client-db
Description	This command enables the context of the client-db's match list. The match list defines the match input used during IPsec's tunnel setup. If there are multiple inputs configured in the match list, then they all must have matches before the system considers a client entry is a match.

idi

Syntax	[no] idi
Context	config>ipsec>client-db>match-list
Description	This command enables the Identification Initiator (IDi) type in the IPsec client matching process. The no form of the command disables the IDi matching process.
Default	no idi

peer-ip-prefix

Syntax	[no] peer-ip-prefix
Context	config>ipsec>client-db>match-list
Description	This command enables the use of the peer's tunnel IP address as the match input.

The **no** form of the command disables the peer IP prefix matching process.

Default no peer-ip-prefix

4.14.2.6 Internet Key Exchange (IKE) Commands

ipsec

Syntax	ipsec
Context	config
Description	This command enables the context to configure Internet Protocol Security (IPsec) parameters. IPsec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

ike-policy

Syntax	ike-policy <i>ike-policy-id</i> [create] no ike-policy <i>ike-policy-id</i>
Context	config>ipsec
Description	This command enables the context to configured an IKE policy. The no form of the command
Parameters	<i>ike-policy-id</i> — Specifies a policy ID value to identify the IKE policy. Values 1 to 2048

trust-anchor-profile

Syntax	trust-anchor-profile <i>name</i> [create] no trust-anchor-profile <i>name</i>
Context	config>ipsec
Description	This command specifies the trust anchor profile name for the IPsec tunnel or IPsec GW.
Default	no trust-anchor-profile
Parameters	<i>name</i> — Specifies the name of trust anchor profile up to 32 characters.

trust-anchor-profile

Syntax	trust-anchor-profile <i>name</i> no trust-anchor-profile <i>name</i>
Context	config>service>ies>if>sap>ipsec-gw>cert config>service>vpn>if>sap>ipsec-gw>cert config>service>vpn>if>sap>ipsec-tunnel>cert
Description	This command specifies the trust anchor profile name for the IPsec tunnel or IPsec GW.
Default	no trust-anchor-profile
Parameters	<i>name</i> — Specifies the name of trust anchor profile, up to 32 characters.

trust-anchor

Syntax	[no] trust-anchor <i>ca-profile-name</i>
Context	config>ipsec>trust-anchor-profile
Description	This command specifies a CA profile as a trust anchor CA. Up to 8 multiple trust anchors can be specified in a single trust anchor profile.
Parameters	<i>ca-profile-name</i> — Specifies the name of the trust anchor profile, up to 32 characters.

auth-method

Syntax	auth-method { psk plain-psk-xauth cert-auth psk-radius cert-radius eap auto-eap-radius auto-eap } no auth-method
Context	config>ipsec>ike-policy
Description	This command specifies the authentication method used with this IKE policy. The no form of the command removes the parameter from the configuration.
Default	no auth-method
Parameters	psk — Both client and gateway authenticate each other by a hash derived from a pre-shared secret. Both client and gateway must have the PSK. This work with both IKEv1 and IKEv2 plain-psk-xauth — Both client and gateway authenticate each other by pre-shared key and RADIUS. This work with IKEv1 only. psk-radius — Use the pre-shared-key and RADIUS to authenticate. IKEv2 remote-access tunnel only.

- cert-radius** — Use the certificate, public/private key and RADIUS to authenticate. IKEv2 remote-access tunnel only.
- eap** — Use the EAP to authenticate peer. IKEv2 remote-access tunnel only
- auto-eap-radius** — Use EAP or potentially other method to authenticate the peer. IKEv2 remote-access tunnel only. Also see [auto-eap-method](#) and [auto-eap-own-method](#).
- auto-eap** — Use the EAP or potentially other RADIUS-related method to authenticate the peer. IKEv2 remote-access tunnel only. Also see [auto-eap-method](#) and [auto-eap-own-method](#).

auto-eap-method

Syntax	auto-eap-method {psk cert psk-or-cert}
Context	config>ipsec>ike-policy
Description	This command enables following behavior for IKEv2 remote-access tunnel when auth-method is configured as auto-eap-radius: • If there is no AUTH payload in IKE_AUTH request, then system use EAP to authenticate client and also will own-auth-method to generate AUTH payload. • If there is AUTH payload in IKE_AUTH request: – if auto-eap-method is psk, then system proceed as auth-method:psk-radius – if auto-eap-method is cert, then system proceed as auth-method:cert-radius – if auto-eap-method is psk-or-cert, then: • if the "Auth Method" field of AUTH payload is PSK, then system proceed as auth-method:psk-radius • if the "Auth Method" field of AUTH payload is RSA or DSS, then system proceed as auth-method:cert-radius – The system will use auto-eap-own-method to generate AUTH payload. This command only applies when auth-method is configured as auto-eap-radius.
Default	auto-eap-method cert
Parameters	psk — Uses the pre-shared-key as the authentication method. cert — Uses the certificate as the authentication method. psk-or-cert — Uses either the pre-shared-key or certificate based on the “Auth Method” field of the received AUTH payload.

auto-eap-own-method

Syntax auto-eap-own-method {psk | cert}

Context	config>ipsec>ike-policy
Description	This command enables following behavior for IKEv2 remote-access tunnel when auth-method is configured as auto-eap-radius: • If there is no AUTH payload in IKE_AUTH request, then system use EAP to authenticate client and also will own-auth-method to generate AUTH payload. • If there is AUTH payload in IKE_AUTH request: – if auto-eap-method is psk, then system proceed as auth-method:psk-radius. – if auto-eap-method is cert, then system proceed as auth-method:cert-radius. – if auto-eap-method is psk-or-cert, then: • if the "Auth Method" field of AUTH payload is PSK, then system proceed as auth-method:psk-radius. • if the "Auth Method" field of AUTH payload is RSA or DSS, then system proceed as auth-method:cert-radius. – The system will use auto-eap-own-method to generate AUTH payload. This command only applies when auth-method is configured as auto-eap-radius.
Default	auto-eap-method cert
Parameters	psk — Uses a pre-shared-key to generate AUTH payload. cert — Uses a public/private key to generate AUTH payload.

dpd

Syntax	dpd [interval <i>interval</i>] [max-retries <i>max-retries</i>] [reply-only] no dpd								
Context	config>ipsec>ike-policy								
Description	This command controls the dead peer detection mechanism. The no form of the command removes the parameters from the configuration.								
Default	no dpd								
Parameters	<i>interval</i> — Specifies the DPD interval, in seconds. Since more time is necessary to determine if there is incoming traffic, the actual time needed to bring down the tunnel is larger than the DPD interval multiplied by max-retries. <table><tr><td>Values</td><td>10 to 300</td></tr><tr><td>Default</td><td>30</td></tr></table> <i>max-retries</i> — Specifies the maximum number of retries before the tunnel is removed. <table><tr><td>Values</td><td>2 to 5</td></tr><tr><td>Default</td><td>3</td></tr></table>	Values	10 to 300	Default	30	Values	2 to 5	Default	3
Values	10 to 300								
Default	30								
Values	2 to 5								
Default	3								

reply-only — Specifies whether to initiate a DPD request if there is an incoming ESP or IKE packet. Issuing the command without the reply-only keyword does not initiate a DPD request if there is an incoming ESP packet.

ike-mode

Syntax	ike-mode { main aggressive } no ike-mode
Context	config>ipsec>ike-policy
Description	This command specifies one of either two modes of operation. IKE version 1 can support main mode and aggressive mode. The difference lies in the number of messages used to establish the session. The no form of the command reverts to the default.
Default	no ike-mode
Parameters	main — Specifies identity protection for the hosts initiating the IPsec session. This mode takes slightly longer to complete. aggressive — Specifies that the aggressive mode provides no identity protection but is faster.

ike-transform

Syntax	ike-transform <i>ike-transform-id</i> [<i>ike-transform-id</i> ...(up to 4 max)] no ike-transform
Context	config>ipsec>ike-policy
Description	This command specifies the IKE transform to be used in the IKE policy. Up to four IKE transforms can be specified. If multiple IDs are specified, the system selects an IKE transform based on the peer's proposal. If the system is a tunnel initiator, it uses the configured IKE transform to generate the SA payload.
Default	no ike-transform
Parameters	<i>ike-transform-id</i> — Specifies up to four existing IKE transform instances to be associated with this IKE policy. Values 1 to 4096

ike-version

Syntax	ike-version { 1 2 }

Context	config>ipsec>ike-policy
Description	This command sets the IKE version (1 or 2) that the ike-policy will use.
Default	ike-version 1
Parameters	1 2 — Specifies the version of IKE protocol.

ikev1-ph1-responder-delete-notify

Syntax	[no] ikev1-ph1-responder-delete-notify
Context	config>ipsec>ike-policy
Description	This command specifies the system, when deleting an IKEv1 phase 1 SA for which it was the responder, to send a delete notification to the peer. This command only applies when the configured ike-version 1. This command is ignored with IKE version 2. The no form of the command reverts to the default.
Default	ikev1-ph1-responder-delete-notify

ikev2-fragment

Syntax	ikev2-fragment mtu <i>octets</i> reassembly-timeout <i>seconds</i> no ikev2-fragment
Context	config>ipsec>ike-policy
Description	This command enables IKEv2 protocol level fragmentation (RFC 7383). The specified MTU is the maximum size of IKEv2 packet.
Default	no ikev2-fragment
Parameters	<i>octets</i> — Specifies the MTU for IKEv2 messages. Values 512 to 9000 <i>seconds</i> — Specifies the timeout for reassembly. Values 1 to 5

limit-init-exchange

Syntax	limit-init-exchange [<i>reduced-max-exchange-timeout seconds</i>] no limit-init-exchange
Context	config>ipsec>ike-policy

Description	This command limits the number of ongoing IKEv2 initial exchanges per tunnel to 1. When the system receives a new IKEv2 IKE_SA_INIT request when there is an ongoing IKEv2 initial exchange from same peer, then system reduces the timeout value of the existing exchange to the specified reduced-max-exchange-timeout. If the reduced-max-exchange-timeout is disabled, then the system does not reduce the timeout value. The no form of this command reverts to the default value.
Default	limit-init-exchange reduced-max-exchange-timeout 2
Parameters	<i>seconds</i> — Specifies the maximum timeout for the in-progress initial IKE exchange. Values 2 to 60, disabled

lockout

Syntax	lockout failed-attempts <i>count</i> duration <i>duration-minutes</i> block <i>block-minutes</i> [max-port-per-ip <i>number-of-ports</i>] no lockout
Context	config>ipsec>ike-policy
Description	This command enables the lockout mechanism for the IPsec tunnel. The system will lock out an IPsec client for the configured time interval if the number of failed authentications exceeds the configured value within the specified duration. This command only applies when the system acts as a tunnel responder. A client is defined as the tunnel IP address plus the port. Optionally, the max-port-per-ip parameter can be configured as the maximum number of ports allowed behind the same IP address. If this threshold is exceeded, then all ports behind the IP address are blocked. The no form of this command disables the lockout mechanism.
Default	no lockout
Parameters	<i>count</i> — Specifies the maximum number of failed authentications allowed during the <i>duration-minutes</i> interval Values 1 to 64 Default 3 <i>duration-minutes</i> — Specifies the interval of time, in minutes, during which the configured failed authentication count must be exceeded in order to trigger a lockout Values 1 to 60 Default 5

block-minutes — Specifies the number of minutes that the client is blocked if the configured failed authentication count is exceeded

Values 1 to 1440, infinite

Default 10

number-of-ports — Specifies the maximum number of ports allowed behind the same IP address

Values 1 to 32000

Default 16

match-peer-id-to-cert

Syntax	[no] match-peer-id-to-cert
Context	config>ipsec>ike-policy
Description	This command enables checking the IKE peer's ID matches the peer's certificate when performing certificate authentication.
Default	no match-peer-id-to-cert

nat-traversal

Syntax	nat-traversal [force] [keep-alive-interval <i>keep-alive-interval</i>] [force-keep-alive] no nat-traversal
Context	config>ipsec>ike-policy
Description	This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled or in forced mode. The no form of the command reverts the parameters to the default.
Default	no nat-traversal
Parameters	force — Forces to enable NAT-T keep-alive-interval <i>keep-alive-interval</i> — Specifies the keep-alive interval in seconds. Values 120 to 600 force-keep-alive — When specified, the keep-alive does not expire.

own-auth-method

Syntax	own-auth-method {psk cert eap-only}

no own-auth-method

Context	config>ipsec>ike-policy
Description	This command configures the authentication method used with this IKE policy on its own side.
Default	no own-auth-method

pfs

Syntax	pfs [dh-group {1 2 5 14 15 19 20 21}] no pfs
Context	config>ipsec>ike-policy
Description	This command enables perfect forward secrecy on the IPsec tunnel using this policy. PFS provides for a new Diffie-Hellman key exchange each time the SA key is renegotiated. After that SA expires, the key is forgotten and another key is generated (if the SA remains up). This means that an attacker who cracks part of the exchange can only read the part that used the key before the key changed. There is no advantage in cracking the other parts if they attacker has already cracked one. The no form of the command disables PFS. If this it turned off during an active SA, when the SA expires and it is time to re-key the session, the original Diffie-Hellman primes will be used to generate the new keys.
Default	no pfs
Parameters	dh-group {1 2 5 14 15 19 20 21} — Specifies which Diffie-Hellman group to use for calculating session keys. More bits provide a higher level of security, but require more processing. Three groups are supported with IKE-v1: Group 1: 768 bits Group 2: 1024 bits Group 5: 1536 bits Group 14: 2048 bits Group 15: 3072 bits Group 19: P-256 ECC Curve, 256 bits Group 20: P-384 ECC Curve, 384 bits Group 21: P-512 ECC Curve, 512 bits

relay-unsolicited-cfg-attribute

Syntax	relay-unsolicited-cfg-attribute
Context	config>ipsec>ike-policy

Description This command enters relay unsolicited configuration attributes context. With this configuration, the configured attributes returned from source (such as a RADIUS server) will be returned to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

internal-ip4-address

Syntax [no] internal-ip4-address

Context config>ipsec>ike-policy>relay-unsol-attr

Description This command will return IPv4 address from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip4-address

internal-ip4-dns

Syntax [no] internal-ip4-dns

Context config>ipsec>ike-policy>relay-unsol-attr

Description This command will return IPv4 DNS server address from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip4-dns

internal-ip4-netmask

Syntax [no] internal-ip4-netmask

Context config>ipsec>ike-policy>relay-unsol-attr

Description This command will return IPv4 netmask from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip4-netmask

internal-ip6-dns

Syntax [no] internal-ip6-dns

Context	config>ipsec>ike-policy>relay-unsol-attr
Description	This command will return IPv6 DNS server address from source (RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.
Default	no internal-ip6-dns

internal-ip6-address

Syntax	[no] internal-ip6-address
Context	config>ipsec>ike-policy>relay-unsol-attr
Description	This command will return IPv6 address from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.
Default	no internal-ip6-address

send-idr-after-eap-success

Syntax	[no] send-idr-after-eap-success
Context	config>ipsec>ike-policy
Description	This command enables the system to add the Identification Responder (IDr) payload in the last IKE authentication response after an Extensible Authentication Protocol (EAP) Success packet is received. When disabled, the system will not include IDr payload. The no form of the command disables sending the IDr payload in the last IKE.
Default	send-idr-after-eap-success

ike-transform

Syntax	ike-transform <i>ike-transform-id</i> [create] no ike-transform <i>ike-transform-id</i>
Context	config>ipsec
Description	This commands creates a new or enters an existing IKE transform instance. The IKE transform include following configuration for IKE SA: • DH Group • IKE authentication algorithm • IKE encryption algorithm

- IKE SA lifetime

The *ike-transform-id* is referenced in the **ike-policy** configuration.

Parameters *ike-transform* — Specifies a number used to uniquely identify an IKE transform instance

Values 1 to 4096

create — Keyword used to create the ike-transform instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

dh-group

Syntax **dh-group** {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21}

Context config>ipsec>ike-transform

Description This command specifies the Diffie-Hellman group to be used in this IKE transform instance.

Default dh-group 2 (1024-bit — More Modular Exponential (MODP))

Parameters **dh-group** {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21} — Specifies which Diffie-Hellman group to use for calculating session keys. More bits provide a higher level of security, but require more processing. Three groups are supported with IKE-v1:

Group 1: 768 bits
Group 2: 1024 bits
Group 5: 1536 bits
Group 14: 2048 bits
Group 15: 3072 bits
Group 19: P-256 ECC Curve, 256 bits
Group 20: P-384 ECC Curve, 384 bits
Group 21: P-512 ECC Curve, 512 bits

ike-auth-algorithm

Syntax **ike-auth-algorithm** *auth-algorithm*

Context config>ipsec>ike-transform

Description This command specifies the IKE authentication algorithm for the IKE transform

Default ike-auth-algorithm sha1

Parameters *auth-algorithm* — Specifies the values used to identify the hashing algorithm

Values **md5** — Configures the use of the hmac-md5 algorithm for authentication

- sha1** — Configures the use of the hmac-sha1 algorithm for authentication
- sha256** — Configures the use of the hmac-sha256 algorithm for authentication.
- sha384** — Configures the use of the hmac-sha384 algorithm for authentication
- sha512** — Configures the use of the hmac-sha512 algorithm for authentication.
- aes-xcbc** — Configures the use of aes-xcbc (RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*) algorithm for authentication.

ike-encryption-algorithm

Syntax	ike-encryption-algorithm encryption-algorithm
Context	config>ipsec>ike-transform
Description	This command specifies the IKE encryption algorithm to be used in the IKE transform instance.
Default	ike-encryption-algorithm aes128
Parameters	encryption-algorithm — Specifies the IKE encryption algorithm
Values	des — Configures the 56-bit des algorithm for encryption. This is an older algorithm with relatively weak security. While better than nothing, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level. 3des — Configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make information more secure. aes128 — Configures the aes algorithm with a block size of 128 bits. This is a mandatory implementation size for aes. This is a very strong algorithm choice. aes192 — Configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes. aes256 — Configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes. aes128-gcm8 - Configures ESP to use aes-gcm with a 128-bit key size and an 8-byte ICV for encryption and authentication. aes128-gcm16 - Configures ESP to use aes-gcm with a 128-bit key size and a 16-byte ICV for encryption and authentication. aes256-gcm8 - Configures ESP to use aes-gcm with a 256-bit key size and an 8-byte ICV for encryption and authentication.

aes256-gcm16 - This parameter configures ESP to use aes-gcm with a 256-bit key size and a 16-byte ICV for encryption and authentication.

isakmp-lifetime

Syntax	isakmp-lifetime <i>seconds</i>
Context	config>ipsec>ike-transform
Description	This command specifies the lifetime of the IKE SA.
Default	isakmp-lifetime 86400
Parameters	<i>seconds</i> — Specifies the Phase 1 life time for this IKE transform.
Values	1200 to 31536000

show-ipsec-keys

Syntax	[no] show-ipsec-keys
Context	config>ipsec
Description	This command enables user to optionally include IKE-SA or CHILD-SA keys in the output of debug ipsec or admin ipsec display-key . The no form of the command disallows the user from including keys in the output.
Default	no show-ipsec-keys

4.14.2.7 IPsec Transform Commands

ipsec-transform

Syntax	ipsec-transform <i>transform-id</i> [create] no ipsec-transform <i>transform-id</i>
Context	config>ipsec
Description	This command enables the context to create an ipsec-transform policy. IPsec transforms policies can be shared. A change to the ipsec-transform is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

IPsec transform policy assignments to a tunnel require the tunnel to be shutdown.

The **no** form of the command removes the ID from the configuration.

Parameters *transform-id* — Specifies a policy ID value to identify the IPsec transform policy.

Values 1 to 2048

create — This keyword is mandatory when creating an ipsec-transform policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

esp-auth-algorithm

Syntax **esp-auth-algorithm** {**null** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** | **aes-xcbc** | **auth-encryption**}

no esp-auth-algorithm

Context config>ipsec>transform

Description This command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a manually configured tunnel must share the same configuration parameters for the IPsec tunnel to enter the operational state.

The **no** form of the command disables the authentication.

Default esp-auth-algorithm sha1

Parameters **null** — This is a very fast algorithm specified in RFC 2410, which provides no authentication.

md5 — This parameter configures ESP to use the **hmac-md5** algorithm for authentication.

sha1 — This parameter configures ESP to use the **hmac-sha1** algorithm for authentication.

sha256 — This parameter configures ESP to use the **sha256** algorithm for authentication.

sha384 — This parameter configures ESP to use the **sha384** algorithm for authentication.

sha512 — This parameter configures ESP to use the **sha512** algorithm for authentication.

aes-xcbc — Specifies the **aes-xcbc** algorithm for authentication.

auth-encryption — This parameter must be configured when **esp-encryption-algorithm** is either **aes-gcm** or **aes-gmac**.

esp-encryption-algorithm

Syntax	esp-encryption-algorithm { null des 3des aes128 aes192 aes256 aes128-gcm8 aes128-gcm12 aes128-gcm16 aes192-gcm8 aes192-gcm12 aes192-gcm16 aes256-gcm8 aes256-gcm12 aes256-gcm16 null-aes128-gmac null-aes192-gmac null-aes256-gmac } no esp-encryption-algorithm
Context	config>ipsec>ipsec-transform
Description	This command specifies the encryption algorithm to use for the IPsec session. Encryption only applies to esp configurations. If encryption is not defined, esp will not be used. For IPsec tunnels to come up, both ends need to be configured with the same encryption algorithm. The no form of the command removes the specified encryption algorithm.
	 Note: When aes-gcm or aes-gmac is configured: • esp-auth-algorithm must be set to auth-encryption • the system will not include the authentication algorithm in the ESP proposal of the SA payload • ipsec-transform cannot be used for manual keying
Default	esp-encryption-algorithm aes128
Parameters	null — This parameter configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on. des — This parameter configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level. 3des — This parameter configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make things more secure. aes128 — This parameter configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes. As of today, this is a very strong algorithm choice. aes192 — This parameter configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes. aes256 — This parameter configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes. aes128-gcm8 — Configures ESP to use aes-gcm with a 128-bit key size and an 8-byte ICV for encryption and authentication.

- aes128-gcm12** — Configures ESP to use aes-gcm with a 128-bit key size and a 12-byte ICV for encryption and authentication.
- aes128-gcm16** — Configures ESP to use aes-gcm with a 128-bit key size and a 16-byte ICV for encryption and authentication.
- aes192-gcm8** — Configures ESP to use aes-gcm with a 192-bit key size and an 8-byte ICV for encryption and authentication.
- aes192-gcm12** — Configures ESP to use aes-gcm with a 192-bit key size and a 12-byte ICV for encryption and authentication.
- aes192-gcm16** — Configures ESP to use aes-gcm with a 192-bit key size and a 16-byte ICV for encryption and authentication.
- aes256-gcm8** — Configures ESP to use aes-gcm with a 256-bit key size and an 8-byte ICV for encryption and authentication.
- aes256-gcm12** — Configures ESP to use aes-gcm with a 256-bit key size and a 12-byte ICV for encryption and authentication.
- aes128-gcm16** — Configures ESP to use aes-gcm with a 256-bit key size and a 16-byte ICV for encryption and authentication.
- null-aes128gmac** — Configures ESP to use aes-gmac with a 128-bit key size for authentication only.
- null-aes192gmac** — Configures ESP to use aes-gmac with a 192-bit key size for authentication only.
- null-aes256gmac** — Configures ESP to use aes-gmac with a 256-bit key size for authentication only.

ipsec-lifetime

Syntax	ipsec-lifetime <i>ipsec-lifetime</i> no ipsec-lifetime
Context	config>ipsec>ike-policy
Description	This command specifies the lifetime of the Phase 2 IKE key. The no form of the command reverts to the default.
Default	3600
Parameters	<i>ipsec-lifetime</i> — Specifies the Phase 2 lifetime for this IKE policy in seconds. Values 1200 to 31536000

ipsec-lifetime

Syntax	ipsec-lifetime <i>seconds</i> ipsec-lifetime inherit
Context	config>ipsec>ipsec-transform
Description	This command specifies the CHILD_SA. If the inherit parameter is specified, then the system uses the IPsec lifetime configuration in the corresponding IKE policy configured in the same IPsec gateway or IPsec tunnel.
Default	ipsec-lifetime inherit
Parameters	<i>seconds</i> — Specifies the lifetime of the Phase 2 IKE key in seconds. Values 1200 to 31536000 inherit — Specifies that the system uses the ipsec-lifetime configuration in the corresponding IKE policy that is configured for the same IPsec gateway or IPsec tunnel.

pfs-dh-group

Syntax	pfs-dh-group { 1 2 5 14 15 19 20 21 } pfs-dh-group inherit no pfs-dh-group
Context	config>ipsec>ipsec-transform
Description	This command specifies the Diffie-Hellman group to be used for Perfect Forward Secrecy (PFS) computation during CHILD_SA rekeying. The no form of the command reverts to the default.
Default	pfs-dh-group inherit
Parameters	{ 1 2 5 14 15 19 20 21 } — Specifies the Diffie-Hellman group to achieve PFS. inherit — Specifies that the value of the DH group used by the system is inherited from the IPsec gateway or IPsec tunnel.

4.14.2.8 IPsec Static Security Association Commands

static-sa

Syntax	static-sa <i>sa-name</i> [create]

no static-sa *sa-name*

Context config>ipsec

Description This command configures an IPsec static SA.

authentication

Syntax **authentication** *auth-algorithm* **ascii-key** *ascii-string*
authentication *auth-algorithm* **hex-key** *hex-string* [**hash**|**hash2**]
no authentication

Context config>ipsec>static-sa

Description This command configures the authentication algorithm to use for an IPsec manual SA.

Default no authentication

Parameters *auth-algorithm* — Specifies the used authentication algorithm.

Values mda5, sha1

ascii-string — Specifies an ASCII key; 16 characters for **md5** and 20 characters for **sha1**.

hex-string — Specifies a HEX key; 32 hex nibbles for **md5** and 40 hex nibbles for **sha1**.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

description

Syntax **description** *description-string*
no description

Context config>ipsec>static-sa

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Parameters *string* — The description character string. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.

direction

Syntax **direction** *ipsec-direction*
no direction

Context config>ipsec>static-sa

Description This command configures the direction for an IPsec manual SA.

The **no** form of the command reverts to the default value.

Default direction bidirectional

Parameters *ipsec-direction* — Identifies the direction to which this static SA entry can be applied.
Values inbound, outbound, bidirectional

protocol

Syntax **protocol** *ipsec-protocol*
no protocol

Context config>ipsec>static-sa

Description This command configures the security protocol to use for an IPsec manual SA. The **no** statement resets to the default value.

Default protocol esp

Parameters *ipsec-protocol* — Identifies the IPsec protocol used with this static SA.
Values **ah** — Specifies the Authentication Header protocol.
esp — Specifies the Encapsulation Security Payload protocol.

spi

Syntax **spi** *spi*
no spi

Context config>ipsec>static-sa

Description This command configures the SPI key value for an IPsec manual SA.

This command specifies the SPI (Security Parameter Index) used to lookup the instruction to verify and decrypt the incoming IPsec packets when the value of the **direction** command is **inbound**.

The SPI value specifies the SPI that will be used in the encoding of the outgoing packets when the value of the **direction** command is **outbound**. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.

If **no spi** is selected, then this static SA cannot be used.

The **no** form of the command reverts to the default value.

Default	no spi
Parameters	<i>spi</i> — Specifies the security parameter index for this SA.
Values	256 to 16383

4.14.2.9 Trust Anchor Profile/TS Commands

auto-establish

Syntax	[no] auto-establish
Context	config>service>vpn>if>sap>ipsec-tun>dynamic-keying
Description	The system will automatically establish phase 1 SA as soon as the tunnel is provisioned and enabled (no shutdown). This option should only be configured on one side of the tunnel. Any associated static routes will remain up as long as the tunnel could be up, even though it may actually be operationally down according to the CLI.

ts-list

Syntax	ts-list <i>list-name</i> [create] no ts-list <i>list-name</i>
Context	config>ipsec
Description	This command creates a new traffic selector (TS). The no form of the command removes the list name from the configuration.
Parameters	<i>list-name</i> — Specifies the name of the TS-list.

local

Syntax	local
Context	config>ipsec>ts-list
Description	This command enables the context to configure local TS-list parameters. The TS-list is the traffic selector of the local system, such as TSr, when the system acts as an IKEv2 responder.

remote

Syntax	remote
Context	config>ipsec>ts-list
Description	This command enables the context to configure remote TS-list parameters. The TS-list is the traffic selector of the local system, such as TSi, when the system acts as an IKEv2 responder.

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>ipsec>ts-list>local config>ipsec>ts-list>remote
Description	This command creates a new TS-list entry or enables the context to configure an existing TS-list entry. The no form of the command removes the entry from the local or remote configuration.
Parameters	<i>entry-id</i> — Specifies the entry ID Values 1 to 32

address

Syntax	address prefix <i>ip-prefix/ip-prefix-len</i> address from <i>begin-ip-address to end-ip-address</i> no address
Context	config>ipsec>ts-list>local>entry config>ipsec>ts-list>remote>entry
Description	This command specifies the address range in the IKEv2 traffic selector.
Default	no address

- Parameters** *ip-prefix/ip-prefix-len* — Specifies the IP prefix and subnet mask.
- begin-ip-address* — Specifies the beginning address of the range for this entry.
- end-ip-address* — Specifies the ending address of the range for this entry.

protocol

- Syntax** **protocol any**
 protocol protocol-id port opaque
 protocol protocol-id port any
 protocol protocol-id port from begin-port-id to end-port-id
 no protocol
- Context** config>ipsec>ts-list>local>entry
 config>ipsec>ts-list>remote>entry
- Description** This command specifies the protocol and port range in the IKEv2 traffic selector.
- The SR OS supports OPAQUE ports and port ranges for the following protocols:
- TCP
 - UDP
 - SCTP
 - ICMP
 - ICMPv6
 - MIPv6
- For ICMP and ICMPv6, the *port* value takes the form *icmp-type/icmp-code*. For MIPv6, the *port* value is the mobility header type. For other protocols, only the **port any** configuration can be used.
- Default** no protocol
- Parameters** *protocol-id* — Specifies the protocol ID. The value can be a number, a protocol name, or **any**.
- begin-port-id* — Specifies the beginning of the port range.
- Values** For TCP, UDP, and SCTP, the value is the port number.
- For ICMP and ICMPv6, the value takes the form *icmp-type/icmp-code*; for example, 0/0.
- For MIPv6, the value is the mobility header type.
- end-port-id* — Specifies the end of the port range
- Values** For TCP, UDP, and SCTP, the value is the port number.
- For ICMP and ICMPv6, the value takes the form *icmp-type/icmp-code*; for example, 0/0.

For MIPv6, the value is the mobility header type.

opaque — Specifies OPAQUE ports.

any — Specifies any port.

ts-negotiation

Syntax	ts-negotiation ts-list <i>list-name</i> no ts-negotiation
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw
Description	This command enables the IKEv2 traffic selector negotiation with the specified ts-list.
Parameters	<i>list-name</i> — Specifies the ts-list name

4.14.2.10 Tunnel Template Commands

tunnel-template

Syntax	tunnel-template <i>ipsec-template-identifier</i> [create] no tunnel-template <i>ipsec-template-identifier</i>
Context	config>ipsec
Description	This command creates a tunnel template. Up to 2000 templates are allowed.
Parameters	<i>ipsec-template-identifier</i> — Specifies the template identifier. Values 1 to 2048 create — Mandatory keyword used when creating a tunnel-template in the IPsec context. The create keyword requirement can be enabled or disabled in the environment>create context.

clear-df-bit

Syntax	[no] clear-df-bit
Context	config>ipsec>tnl-temp
Description	This command enables clearing of the Do-not-Fragment bit.
Default	no clear-df-bit

encapsulated-ip-mtu

Syntax	encapsulated-ip-mtu <i>octets</i> no encapsulated-ip-mtu
Context	config>ipsec>tnl-temp config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-tun
Description	This command specifies the max size of encapsulated tunnel packet for the ipsec-tunnel/ip-tunnel or the dynamic tunnels terminated on the ipsec-gw. If the encapsulated v4 or v6 tunnel packet exceeds the encapsulated-ip-mtu , then system fragments the packet against the encapsulated-ip-mtu.
Default	no encapsulated-ip-mtu
Parameters	<i>octets</i> — Specifies the max size in octets. Values 512 to 9000

icmp6-generation

Syntax	icmp6-generation
Context	config>ipsec>tnl-temp config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-tun
Description	This command enables the ICMPv6 packet generation configuration context.

pkt-too-big

Syntax	pkt-too-big interval <i>seconds</i> pkt-too-big message-count <i>count</i> [no] pkt-too-big
Context	config>ipsec>tnl-temp>icmp6-gen config>service>vprn>if>sap>ipsec-tun>icmp6-gen
Description	This command enables system to send ICMPv6 PTB (Packet Too Big) message on private side and optionally specifies the rate. With this command configured, system will send PTB back if received v6 packet on private side is bigger than 1280 bytes and also exceeds the private MTU of the tunnel.

The **ip-mtu** command (under **ipsec-tunnel** or **tunnel-template**) specifies the private MTU for the ipsec-tunnel or dynamic tunnel.

Parameters	<i>seconds</i> — the maximum interval during which messages can be sent, in seconds. Values 1 to 60 Default 10 <i>count</i> — the maximum number of ICMPv6 messages that can be sent during the configured interval Values 10 to 1000 Default 100

ip-mtu

Syntax	ip-mtu <i>octets</i> no ip-mtu
Context	config>ipsec>tnl-temp
Description	This command configures the template IP MTU.
Default	no ip-mtu
Parameters	<i>octets</i> — Specifies the maximum size in octets. Values 512 to 9000

private-tcp-mss-adjust

Syntax	private-tcp-mss-adjust <i>octets</i> no private-tcp-mss-adjust
Context	config>ipsec>tnl-temp config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-tun config>service>ies>if>sap>ip-tunnel
Description	This command enables TCP MSS adjust for IPsec or IP tunnels on the private side. When the command is configured, the system updates the TCP MSS option to the value of the received TCP SYN packet on the private side. The no form of the command disables TCP MSS adjust on the private side.
Default	no private-tcp-mcc-adjust

Parameters *octets* — Specifies the new TCP MSS value in octets.

Values 512 to 9000

public-tcp-mss-adjust

Syntax **public-tcp-mss-adjust** *octets*

public-tcp-mss-adjust **auto**

no public-tcp-mss-adjust

Context config>ipsec>tnl-temp
config>service>vpn>if>sap>ipsec-tun
config>service>vpn>if>ip-tunnel
config>service>ies>if>sap>ip-tunnel

Description This command enables TCP MSS adjust for IPsec or IP tunnels on the public side. When the command is configured, the system updates the TCP MSS option value to received.TCP SYN packet encapsulation in the ESP packet.

If **auto** is specified, the system derives the new MSS value based on the public MTU and IPsec overhead.

The **no** form of this command disables TCP MSS adjust on the public side.

Default no public-tcp-mss-adjust

Parameters **auto** — Derive the new MSS value based on the public MTU and IPsec overhead.

octets — Specifies the new TCP MSS value in octets.

Values 512 to 9000

replay-window

Syntax **replay-window** {32 | 64 | 128 | 256 | 512}

no replay-window

Context config>ipsec>tnl-temp

Description This command sets the anti-replay window.

The **no** form of the command removes the parameter from the configuration.

Default no replay-window

Parameters {32 | 64 | 128 | 256 | 512} — Specifies the size of the anti-replay window.

sp-reverse-route

Syntax	[no] sp-reverse-route
Context	config>ipsec>tnl-temp
Description	This command specifies whether the node using this template will accept framed-routes sent by the RADIUS server and install them for the lifetime of the tunnel as managed routes. The no form of the command disables sp-reverse-route.
Default	no sp-reverse-route

transform

Syntax	transform transform-id [transform-id] no transform
Context	config>ipsec>tnl-temp config>service>ies>if>sap>ipsec-gw config>service>vpn>if>sap>ipsec-gw config>service>vpn>if>sap>ipsec-tunnel
Description	This command configures IPsec transform.
Default	no transform
Parameters	<i>transform-id</i> — Specifies up to four transform IDs.

4.14.2.11 Service Configuration Commands

ipsec

Syntax	ipsec
Context	config>service>vpn>ipsec
Description	This command enables the context to configure IPsec policies.

cert-profile

Syntax	cert-profile name no cert-profile

Context	config>service>ies>if>sap>ipsec-gw>cert config>service>vprn>if>sap>ipsec-gw>cert config>service>vprn>if>sap>ipsec-tun>dyn>cert
Description	This command specifies a cert-profile for the IPsec tunnel or IPsec gw.
Parameters	<i>name</i> — Specifies the name of profile up to 32 characters.

allow-reverse-route-override

Syntax	allow-reverse-route-override
Context	config>service>vprn>ipsec
Description	With this command configured, the system will allow a new dynamic LAN-to-LAN tunnel that terminates in the private VPRN service to be created with an overlapping reverse route. If the ID is the same as an existing one, the existing CHILD_SA and route will be removed.
Default	no allow-reverse-route-override

security-policy

Syntax	security-policy <i>security-policy-id</i> [create] no security-policy <i>security-policy-id</i>
Context	config>service>vprn>ipsec
Description	This command configures a security policy to use for an IPsec tunnel.
Parameters	<i>security-policy-id</i> — specifies a value to be assigned to a security policy. Values 1 to 32768 create — Keyword used to create the security policy instance. The create keyword requirement can be enabled or disabled in the environment>create context.

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>service>vprn>ipsec>sec-plcy
Description	This command configures an IPsec security policy entry.
Parameters	<i>entry-id</i> — Specifies the IPsec security policy entry. Values 1 to 16

create — Keyword used to create the security policy entry instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

local-ip

Syntax	local-ip { <i>ip-prefix/prefix-length</i> <i>ip-prefix netmask</i> any }
Context	config>service>vpn>ipsec>sec-plcy>entry
Description	This command configures the local (from the VPN) IP prefix/mask for the policy parameter entry. Only one entry is necessary to describe a potential flow. The local-ip and remote-ip commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.
Parameters	<i>ip-prefix</i> — The destination address of the aggregate route in dotted decimal notation Values a.b.c.d (host bits must be 0) prefix-length 1 to 32 <i>netmask</i> — The subnet mask in dotted decimal notation any — keyword to specify that it can be any address

local-v6-ip

Syntax	local-v6-ip <i>ipv6-prefix/prefix-length</i> local-v6-ip any no local-v6-ip
Context	config>service>vpn>ipsec>sec-plcy>entry
Description	This command specifies the local v6 prefix for the security-policy entry.
Parameters	<i>ipv6-prefix/prefix-length</i> — Specifies the local v6 prefix and length Values ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D host bits must be 0 :: not allowed prefix-length [1 to 128]

any — keyword to specify that it can be any address.

remote-ip

Syntax	remote-ip { <i>ip-prefix/prefix-length</i> <i>ip-prefix netmask</i> any }
Context	config>service>vpn>ipsec>sec-plcy>entry
Description	This command configures the remote (from the tunnel) IP prefix/mask for the policy parameter entry. Only one entry is necessary to describe a potential flow. The local-ip and remote-ip commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.
Parameters	<i>ip-prefix</i> — The destination address of the aggregate route in dotted decimal notation. Values a.b.c.d (host bits must be 0) prefix-length 1 to 32 <i>netmask</i> — The subnet mask in dotted decimal notation. any — keyword to specify that it can be any address.

remote-v6-ip

Syntax	remote-v6-ip any remote-v6-ip <i>ipv6-prefix/prefix-length</i> no remote-v6-ip
Context	config>service>vpn>ipsec>sec-plcy>entry
Description	This command specifies the remote v6 prefix for the security-policy entry.
Parameters	<i>ipv6-prefix/prefix-length</i> — Specifies the local v6 prefix and length. Values ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D host bits must be 0 :: not allowed prefix-length [1 to 28]

any — A keyword to specify that any address can be used.

address

Syntax	address <i>ipv6-address/prefix-length</i> [eui-64] [track-srrp <i>srrp-instance</i>] [modifier <i>cga-modifier</i>] [dad-disable] [primary-preference <i>primary-preference</i>] no address <i>ipv6-address/prefix-length</i>
Context	config>service>vprn>if>ipv6
Description	This command add an IPv6 address to the tunnel interface. The prefix length must be 96 or higher.
Parameters	<i>ipv6-address/prefix-length</i> — Specifies the IPv6 address on the interface.

Values

```

ipv6-address/prefix: ipv6-address  x:x:x:x:x:x:x (eight 16-bit pieces)
                                x:x:x:x:x:d.d.d.d
                                x [0 to FFFF]H
                                d [0 to 255]D
prefix-length                    1 to 128

```

eui-64 — When the **eui-64** keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM interfaces, the Base MAC address of the chassis is used.

link-local-address

Syntax	link-local-address <i>ipv6-address</i> [dad-disable]
Context	config>service>vprn>if>ipv6
Description	This command specifies the link-local-address for the tunnel interface. Only one link-local-address is allowed per interface.
Parameters	<i>ipv6-address</i> — Specifies the IPv6 address on the interface.

Values

```

ipv6-address/prefix: ipv6-address  x:x:x:x:x:x:x (eight 16-bit pieces)
                                   x:x:x:x:x:d.d.d.d
                                   x [0 to FFFF]H
                                   d [0 to 255]D

```

dad-disable — Disables Duplicate Address Detection.

dynamic-tunnel-redundant-next-hop

Syntax	dynamic-tunnel-redundant-next-hop <i>ip-address</i> no dynamic-tunnel-redundant-next-hop
Context	config>service>ies>if config>service>vprn>if
Description	This command configures the dynamic ISA tunnel redundant next-hop address.
Default	no dynamic-tunnel-redundant-next-hop
Parameters	<i>ip-address</i> — Specifies the IP address of the next hop.

static-tunnel-redundant-next-hop

Syntax	static-tunnel-redundant-next-hop <i>ip-address</i> no static-tunnel-redundant-next-hop
Context	config>service>ies>if config>service>vprn>if
Description	This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for static IPsec tunnel. The specified next-hop address will be used by standby node to shunt IPsec traffic to master in case of it receives them. The next-hop address will be resolved in routing table of corresponding service.
Default	no static-tunnel-redundant-next-hop
Parameters	<i>ip-address</i> — Specifies the IP address of the next hop.

interface

Syntax	interface <i>ip-int-name</i> [create] [tunnel] no interface <i>ip-int-name</i>
Context	config>service>vprn
Description	This command creates a logical IP routing interface for a Virtual Private Routed Network (VPRN). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The **interface** command, under the context of services, is used to create and maintain IP routing interfaces within VPRN service IDs. The **interface** command can be executed in the context of an VPRN service ID. The IP interface created is associated with the service core network routing instance and default routing table. The typical use for IP interfaces created in this manner is for subscriber Internet access.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for **config router interface** and **config service vprn interface**. Interface names must not be in the dotted decimal notation of an IP address. For example, the name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

The available IP address space for local subnets and routes is controlled with the **config router service-prefix** command. The **service-prefix** command administers the allowed subnets that can be defined on service IP interfaces. It also controls the prefixes that may be learned or statically defined with the service IP interface as the egress interface. This allows segmenting the IP address space into **config router** and **config service** domains.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All VPRN IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The **no** form of this command removes IP the interface and all the associated configuration. The interface must be administratively shutdown before issuing the **no interface** command.

For VPRN services, the IP interface must be shutdown before the SAP on that interface may be removed. VPRN services do not have the **shutdown** command in the SAP CLI context. VPRN service SAPs rely on the interface status to enable and disable them.

- Parameters**
- ip-int-name* — Specifies the name of the IP interface. Interface names, up to 32 alphanumeric characters. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.
 - tunnel** — Specifies that the interface is configured as tunnel interface, which could be used to terminate IPsec or GRE tunnels in the private service.
 - create** — Keyword used to create the IPsec interface instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

sap

Syntax

```
sap sap-id [create]
no sap sap-id
```

Context	config>service>ies>if config>service>vprn>if
Description	This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique. All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object. Enter an existing SAP without the create keyword to edit SAP parameters. The SAP is owned by the service in which it was created. A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the config interface port-type port-id mode access command. Channelized TDM ports are always access ports. If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined. The no form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted.
Default	No SAPs are defined.
Special Cases	SAP Tunnels — sap tunnel-id.private public:tag — This parameter associates a tunnel group SAP with this interface. This context will provide a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The “tag” will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 to 4094.
Parameters	<i>sap-id</i> — Specifies the physical port identifier portion of the SAP definition. <i>port-id</i> — Specifies the physical port ID in the <i>slot/mda/port</i> format. If the card in the slot has Media Dependent Adapters (MDAs) installed, the <i>port-id</i> must be in the <i>slot_number/MDA_number/port_number</i> format. For example 61/2/3 specifies port 3 on MDA 2 in slot 61.

Table 27 Port ID Syntax

null	<i>port-id</i> <i>lag-id</i>
dot1q	{ <i>port-id</i> <i>lag-id</i> }:{ <i>qtag1</i> <i>cp-conn-prof-id</i> }

Table 27 Port ID Syntax (Continued)

qinq	{ <i>port-id</i> <i>lag-id</i> }:{ <i>qtag1</i> <i>cp-conn-prof-id</i> }.{ <i>qtag2</i> <i>cp-conn-prof-id</i> }	
	cp: keyword conn-prof-id: 1 to 8000	
port-id	slot/mda/port [.channel]	
	eth-sat-id	esat-id/slot/port
		esat: keyword
		id: 1 to 20
	pxc-id	psc-id.sub-port
		pxc psc-id.sub-port
		pxc: keyword
		id: 1 to 64
lag-id	lag-id	sub-port: a, b
		lag: keyword
		id: 1 to 800
qtag1	0 to 4094	
qtag2	* null 0 to 4094	

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels the port ID must include the channel ID. A period “.” separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

create — Keyword used to create a SAP instance.

ipsec-tunnel

Syntax **ipsec-tunnel** *ipsec-tunnel-name* [create]
no ipsec-tunnel *ipsec-tunnel-name*

Context config>service>vprn>if>sap

Description	This command specifies an IPsec tunnel name. An IPsec client sets up the encrypted tunnel across public network. The 7750 SR IPsec MDA acts as a concentrator gathering, and terminating these IPsec tunnels into an IES or VPRN service. This mechanism allows as service provider to offer a global VPRN service even if node of the VPRN are on an uncontrolled or insecure portion of the network.
Parameters	<i>ipsec-tunnel-name</i> — Specifies an IPsec tunnel name, up to 32 characters. create — Keyword used to create the IPsec tunnel instance. The create keyword requirement can be enabled or disabled in the environment>create context.

bfd-designate

Syntax	[no] bfd-designate
Context	config>service>vprn>if>sap>ipsec-tunnel
Description	This command specifies whether this IPsec tunnel is the BFD designated tunnel.
Default	no bfd-designate

bfd-enable

Syntax	[no] bfd-enable {service service-id service-name service-name} interface interface-name dst-ip ip-address
Context	config>service>vprn>if>sap>ipsec-tunnel
Description	This command assigns a BFD session to provide a heart-beat mechanism for a given IPsec tunnel. There can be only one BFD session assigned to any given IPsec tunnel, but there can be multiple IPsec tunnels using same BFD session. BFD controls the state of the associated tunnel. If the BFD session goes down, the system will also bring down the associated non-designated IPsec tunnel.
Parameters	<i>service-id</i> — Specifies the service ID on which the BFD session resides. <i>service-name</i> — Specifies the service name on which the BFD session resides. <i>interface-name</i> — Specifies the name of the interface used by the BFD session. <i>ip-address</i> — Specifies the destination address to be used for the BFD session.

dynamic-keying

Syntax	[no] dynamic-keying
Context	config>service>vprn>if>sap>ipsec-tunnel
Description	This command enables dynamic keying for the IPsec tunnel.

The **no** form of the command disables dynamic keying.

auto-establish

Syntax	[no] auto-establish
Context	config>service>vpn>if>sap>ipsec-tun>dynamic-keying
Description	This command specifies whether to attempt to establish a phase 1 exchange automatically. The no form of the command disables the automatic attempts to establish a phase 1 exchange.
Default	no auto-establish

transform

Syntax	transform <i>transform-id</i> [<i>transform-id</i>] no transform
Context	config>service>vpn>if>sap>ipsec-tun>dynamic-keying config>ipsec>tnl-temp
Description	This command associates the IPsec transform sets allowed for this tunnel. A maximum of four transforms can be specified. The transforms are listed in decreasing order of preference (the first one specified is the most preferred).
Default	no transform
Parameters	<i>transform-id</i> — Specifies the value used for transforms for dynamic keying. Values 1 to 2048

manual-keying

Syntax	[no] manual-keying
Context	config>service>vpn>if>sap>ipsec-tunnel
Description	This command configures Security Association (SA) for manual keying. When enabled, the command specifies whether this SA entry is created manually by the user or dynamically by the IPsec sub-system.

security-association

Syntax	security-association <i>security-entry-id</i> authentication-key <i>authentication-key</i> encryption-

	key <i>encryption-key</i> spi <i>spi</i> transform <i>transform-id</i> direction {inbound outbound} no security-association <i>security-entry-id</i> direction {inbound outbound}
Context	config>service>vprn>if>sap>ipsec-tunnel>manual-keying
Description	This command configures the information required for manual keying SA creation.
Parameters	<i>security-entry-id</i> — Specifies the ID of an SA entry. Values 1 to 16 encryption-key <i>encryption-key</i> — specifies the key used for the encryption algorithm. Values none or 0x0 to 0xFFFFFFFF...(max 64 hex nibbles) authentication-key <i>authentication-key</i> — The authentication key. Values none or 0x0 to 0xFFFFFFFF...(max 40 hex nibbles) spi <i>spi</i> — Specifies the Security Parameter Index (SPI) used to look up the instruction to verify and decrypt the incoming IPsec packets when the direction is inbound. When the direction is outbound, the SPI that will be used in the encoding of the outgoing packets. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet. Values 256 to 16383 transform <i>transform-id</i> — Specifies the transform entry that will be used by this SA entry. This object should be specified for all the entries created which are manual SAs. If the value is dynamic, then this value is irrelevant and will be zero. Values 1 to 2048 direction {inbound outbound} — Specifies the direction of an IPsec tunnel.

replay-window

Syntax	replay-window {32 64 128 256 512} no replay-window
Context	config>ipsec>tnl-temp config>service>vprn>if>sap>ipsec-tunnel
Description	This command specifies the size of the anti-replay window. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet.
Default	no replay-window
Parameters	{32 64 128 256 512} — Specifies the size of the SA anti-replay window.

security-policy

Syntax	security-policy <i>security-policy-id</i> [strict-match] no security-policy
Context	config>service>vpn>if>sap>ipsec-tunnel
Description	This command configures an IPsec security policy. The policy may then be associated with static IPsec tunnels defined in the same routing instance. With strict-match parameter enabled, when a CREATE_CHILD exchange request is received for a static IPsec tunnel, and this request is not a re-key request, then ISA matches the received TS<i>i</i> and TS<i>r</i> with the configured security policy. This can be a match only when a received TS (in TS<i>i</i> or TS<i>r</i>) address range matches exactly with the subnet in a security policy entry. If there is no match, then the setup fails, and TS_UNACCEPTABLE is sent. If there is a match, but there is an existing CHILD_SA for the matched security policy, then the setup fails, and NO_PROPOSAL_CHOSEN. If there is a match, and there is not CHILD_SA for the matched entry, then the subnet is sent in the matched security-policy entry as TS<i>i</i> and TS<i>r</i>, and the CHILD_SA is created.
Default	no security-policy
Parameters	<i>security-policy-id</i> — Specifies the IPsec security policy entry that the tunnel will use. Values 1 to 32768 strict-match — Enables strict match of security-policy entry.

4.14.2.12 Interface SAP Tunnel Commands

ip-tunnel

Syntax	ip-tunnel <i>ip-tunnel-name</i> [create] no ip-tunnel <i>ip-tunnel-name</i>
Context	config>service>ies>if>sap config>service>vpn>if>sap
Description	This command is used to configure an IP-GRE or IP-IP tunnel and associate it with a private tunnel SAP within an IES or VPRN service. The no form of the command deletes the specified IP/GRE or IP-IP tunnel from the configuration. The tunnel must be administratively shutdown before issuing the no ip-tunnel command.

Parameters *ip-tunnel-name* — Specifies the name of the IP tunnel. Tunnel names can be from 1 to 32 alphanumeric characters. If the string contains special characters (for example, #, \$, spaces), the entire string must be enclosed within double quotes.

source

Syntax **source** *ip-address*
 no source

Context config>service>ies>if>sap>ip-tunnel
 config>service>vprn>if>sap>ip-tunnel

Description This command sets the source IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. It must be an address in the subnet of the associated public tunnel SAP interface. The GRE tunnel does not come up until a valid source address is configured.

 The **no** form of the command deletes the source address from the GRE tunnel configuration. The tunnel must be administratively shutdown before issuing the **no source** command.

Default no source

Parameters *ip-address* — Specifies the source IPv4 address of the GRE tunnel.

Values 1.0.0.0 to 223.255.255.255

remote-ip

Syntax **remote-ip** *ip-address*
 no remote-ip

Context config>service>interface>ies>sap>ip-tunnel
 config>service>interface>vprn>sap>ip-tunnel

Description This command sets the primary destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

 The **no** form of the command deletes the destination address from the GRE tunnel configuration.

Default no remote-ip

Parameters *ip-address* — Specifies the destination IPv4 address of the GRE tunnel.

Values 1.0.0.0 to 223.255.255.255

backup-remote-ip

Syntax	backup-remote-ip <i>ip-address</i> no backup-remote-ip
Context	config>service>>ies>interface>sap>ip-tunnel config>service>vprn>interface>sap>ip-tunnel
Description	This command sets the backup destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If the primary destination address is not reachable in the delivery service (there is no route) or not defined then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service. The no form of the command deletes the backup-destination address from the GRE tunnel configuration.
Default	no backup-remote-ip
Parameters	<i>ip-address</i> — Specifies the destination IPv4 address of the GRE tunnel.
Values	1.0.0.0 to 223.255.255.255

clear-df-bit

Syntax	[no] clear-df-bit
Context	config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-tunnel
Description	This command instructs the MS-ISA to reset the DF bit to 0 in all payload IP packets associated with the GRE or IPsec tunnel, before any potential fragmentation resulting from the ip-mtu command. (This will require a modification of the header checksum.) The no clear-df-bit command, corresponding to the default behavior, leaves the DF bit unchanged. The no form of the command disables the DF bit reset.
Default	no clear-df-bit

delivery-service

Syntax	delivery-service { <i>service-id</i> <i>svc-name</i> } no delivery-service
Context	config>service>interface>ies>sap>delivery-service config>service>interface>vprn>sap>gre-tunnel

Description	This command sets the delivery service for GRE encapsulated packets associated with a particular GRE tunnel. This is the IES or VPRN service where the GRE encapsulated packets are injected and terminated. The delivery service may be the same service that owns the private tunnel SAP associated with the GRE tunnel. The GRE tunnel does not come up until a valid delivery service is configured. The no form of the command deletes the delivery-service from the GRE tunnel configuration.
Default	no delivery-service
Parameters	<i>service-id</i> — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel. Values 1 to 2147483647 <i>svc-name</i> — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel, up to 64 characters.

dscp

Syntax	dscp <i>dscp-name</i> no dscp
Context	config>service>interface>ies>sap config>service>interface>vprn>sap>gre-tunnel
Description	This command sets the DSCP code-point in the outer IP header of GRE encapsulated packets associated with a particular GRE tunnel. The default, set using the no form of the command, is to copy the DSCP value from the inner IP header (after remarking by the private tunnel SAP egress qos policy) to the outer IP header.
Default	no dscp
Parameters	<i>dscp</i> — Specifies the DSCP code-point to be used. Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dest-ip

Syntax	[no] dest-ip <i>ip-address</i>
Context	config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel config>service>vprn>sap>ipsec-tunnel

Description	This command configures a private IPv4 or IPv6 address of the remote tunnel endpoint. A tunnel can have up to 16 dest-ip commands. At least one dest-ip address is required in the configuration of a tunnel. A tunnel does not come up operationally unless all dest-ip addresses are reachable (part of a local subnet).		
	Unnumbered interfaces are not supported.		
Parameters	<i>ip-address</i> — Specifies the private IPv4 or IPv6 address of the remote IP tunnel endpoint. If this remote IP address is not within the subnet of the IP interface associated with the tunnel then the tunnel will not come up.		
	Values		
	<ip-address>	ipv4-address	a.b.c.d
		ipv6-address	x:x:x:x:x:x:x (eight 16-bit pieces)
			x:x:x:x:x:d.d.d.d
			x - [0 to FFFF]H
			d - [0 to 255]D

gre-header

Syntax	[no] gre-header gre-header send-key <i>send-key</i> receive-key <i>receive-key</i>
Context	config>service>ies>sap>ip-tunnel config>service>vprn>sap>ip-tunnel
Description	This command configures the type of the IP tunnel. If the gre-header command is configured then the tunnel is a GRE tunnel with a GRE header inserted between the outer and inner IP headers. If the no form of the command is configured then the tunnel is a simple IP-IP tunnel.
Default	no gre-header
Parameters	send-key <i>send-key</i> — Specifies a 32-bit unsigned integer. Values 0 to 4294967295 receive-key <i>receive-key</i> — Specifies a 32-bit unsigned integer. Values 0 to 4294967295

ip-mtu

Syntax	ip-mtu octets no ip-mtu
Context	config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel config>service>vprn>if>sap>ipsec-tunnel

Description	This command configures the IP maximum transmit unit (packet) for this interface. Because this connects a Layer 2 to a Layer 3 service, this parameter can be adjusted under the IES interface. The MTU that is advertised from the IES size is: MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu)) By default (for the Ethernet network interface), if no ip-mtu is configured it is (1568 - 14) equals 1554. The ip-mtu command instructs the MS-ISA to perform IP packet fragmentation, prior to IPsec encryption and encapsulation, based on the configured MTU value. In particular: If the length of a payload IP packet (including its header) exceeds the configured MTU value and the DF flag is clear (due to the presence of the clear-df-bit command or because the original DF value was 0) then the MS-ISA fragments the payload packet as efficiently as possible (i.e. it creates the minimum number of fragments each less than or equal to the configured MTU size); in each created fragment the DF bit shall be 0. If the length of a payload IP packet (including its header) exceeds the configured MTU value and the DF flag is set (because the original DF value was 1 and the tunnel has no clear-df-bit in its configuration) then the MS-ISA discards the payload packet without sending an ICMP type 3/code 4 message back to the packet's source address. The no ip-mtu command, corresponding to the default behavior, disables fragmentation of IP packets by the MS-ISA; all IP packets, regardless of size or DF bit setting, are allowed into the tunnel. The effective MTU for packets entering a tunnel is the minimum of the private tunnel SAP interface IP MTU value (used by the IOM) and the tunnel IP MTU value (configured using the above command and used by the MS-ISA). So if it desired to fragment IP packets larger than X bytes with DF set, rather than discarding them, the tunnel IP MTU should be set to X and the private tunnel SAP interface IP MTU should be set to a value larger than X.
Default	no ip-mtu

reassembly

Syntax	reassembly [<i>wait-msecs</i>] no reassembly
Context	config>service>ies>if>sap>ip-tunnel config>service>vprn>if>sap>ip-tunnel
Description	This command configures the reassembly wait time.

4.14.2.12.1 IPsec Gateway Commands

ipsec-gw

Syntax	ipsec-gw <i>name</i> no ipsec-gw
Context	config>service>ies>if>sap config>service>vpn>if>sap
Description	This command configures an IPsec gateway.

default-secure-service

Syntax	default-secure-service <i>service-id</i> interface <i>ip-int-name</i> no default-secure-service
Context	config>service>ies>if>sap>ipsec-gateway config>service>vpn>if>sap>ipsec-gateway
Description	This command specifies a service ID or service name of the default security service used by this SAP IPsec gateway.
Parameters	<i>service-id</i> — Specifies a default secure service. Values <i>service-id</i> : 1 to 2147483647 <i>svc-name</i> : An existing service name up to 64 characters.

default-tunnel-template

Syntax	default-tunnel-template <i>ipsec-template-identifier</i> no default-tunnel-template
Context	config>service>ies>if>sap>ipsec-gateway config>service>vpn>if>sap>ipsec-gateway
Description	This command configures a default tunnel policy template for the gateway.

dhcp

Syntax	[no] dhcp
Context	config>service>ies>if>sap>ipsec-gateway config>service>vpn>if>sap>ipsec-gateway

Description	This command enters the context of DHCPv4-based address assignment for IKEv2 remote-access tunnels. The system will act as a DHCPv4 client on behalf of the IPsec client, and also a relay agent to relay DHCPv4 packets to the DHCPv4 server. DHCPv4 DORA(Discovery/Offer/Request/Ack) exchange happens during IKEv2 remote-access tunnel setup. And system also supports standard renew In order to use this feature, the relay-proxy must be enabled on the corresponding interface (either the private interface or the interface that has the gi-address as the interface address.
Default	no dhcp

dhcp6

Syntax	[no] dhcp6
Context	config>service>ies>if>sap>ipsec-gateway config>service>vpn>if>sap>ipsec-gateway
Description	This command enters the context of DHCPv6-based address assignment for IKEv2 remote-access tunnels. The system will act as a DHCPv6 client on behalf of the IPsec client, and will also act as a relay agent to relay DHCPv6 packets to the DHCPv6 server. DHCPv6 exchange happens during IKEv2 remote-access tunnel setup. The system also supports standard renew.
Default	no dhcp6

gi-address

Syntax	gi-address <i>ip-address</i> no gi-address
Context	config>service>ies>if>sap>ipsec-gw>dhcp config>service>vpn>if>sap>ipsec-gw>dhcp
Description	This command specifies the gateway IP address of the DHCPv4 packets sent by the system. IPsec DHCP Relay uses only the gi-address configuration found under the IPsec gateway and does not take into account gi-address with src-ip-addr configuration below other interfaces
Default	no gi-address
Parameters	<i>ip-address</i> — Specifies the host IP address to be used for DHCP relay packets.

link-address

Syntax	link-address <i>ipv6-address</i> no link-address
Context	config>service>ies>if>sap>ipsec-gw>dhcp6 config>service>vprn>if>sap>ipsec-gw>dhcp6
Description	This command specifies the link address of the relayed DHCPv6 packets sent by the system.
Default	no link-address
Parameters	<i>ipv6-address</i> — Specifies a global unicast IPv6 address.

send-release

Syntax	[no] send-release
Context	config>service>ies>if>sap>ipsec-gw>dhcp config>service>ies>if>sap>ipsec-gw>dhcp6 config>service>vprn>if>sap>ipsec-gw>dhcp config>service>vprn>if>sap>ipsec-gw>dhcp6
Description	This command enables the system to send a DHCPv4/v6 release message when the IPsec tunnel is removed.
Default	no send-release

server

Syntax	server <i>ip-address</i> [<i>ip-address...</i> (up to 8 max)] router <i>router-instance</i> server <i>ip-address</i> [<i>ip-address...</i> (up to 8 max)] service-name <i>service-name</i> no server
Context	config>service>ies>if>sap>ipsec-gw>dhcp config>service>ies>if>sap>ipsec-gw>dhcp6 config>service>vprn>if>sap>ipsec-gw>dhcp config>service>vprn>if>sap>ipsec-gw>dhcp6
Description	This command specifies up to eight DHCPv4/v6 server addresses for DHCPv4/v6-based address assignment. If multiple server addresses are specified, the first advertised DHCPv4/v6 address received will be chosen.
Default	no server

Parameters	<i>ip-address</i> — Specifies a unicast IPv4 address (for DHCPv4) or global unicast IPv6 address (for DHCPv6).				
Values	<table><tr><td>ipv4-address</td><td>a.b.c.d</td></tr><tr><td>ipv6-address</td><td>x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D</td></tr></table>	ipv4-address	a.b.c.d	ipv6-address	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D
ipv4-address	a.b.c.d				
ipv6-address	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D				
	<i>router-instance</i> — Specifies the router instance ID used to reach the configured server address. This variant of the command is only supported in 'classic' configuration-mode (configure system management-interface configuration-mode classic). The server ip-address service-name service-name variant can be used in all configuration modes.				
Values	{router-name vprn-svc-id} <i>vprn-svc-id:</i> 1 to 2147483647 <i>router-name:</i> <i>router-name</i> is an alias for input only. The <i>router-name</i> gets replaced with an id automatically by SR OS in the configuration).				
Default	Base				
	<i>service-name</i> — Specifies the name of the IES or VPRN service used to reach the configured server address, up to 64 characters.				

ike-policy

Syntax	ike-policy <i>ike-policy-id</i> no ike-policy
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw
Description	This command configures IKE policy for the gateway.
Parameters	<i>ike-policy-id</i> — Specifies the IKE policy ID.
Values	1 to 2048

local-address-assignment

Syntax	[no] local-address-assignment

Context config>service>ies>if>sap>ipsec-gw
config>service>vprn>if>sap>ipsec-gw

Description This command enables the context to configure local address assignments for the IPsec gateway.

ipv4

Syntax **ipv4**

Context config>service>ies>if>sap>ipsec-gw>lcl-addr-assign
config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign

Description This command enables the context to configure IPv4 local address assignment parameters for the IPsec gateway.

address-source

Syntax **address-source router** *router-instance* **dhcp-server** *local-dhcp4-svr-name* **pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]
address-source service-name *service-name* **dhcp-server** *local-dhcp4-svr-name* **pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]
address-source router *router-instance* **dhcp-server** *local-dhcp6-svr-name* **pool** *dhcp6-server-pool*
address-source service-name *service-name* **dhcp-server** *local-dhcp6-svr-name* **pool** *dhcp6-server-pool*
no address-source

Context config>service>ies>if>sap>ipsec-gw>lcl-addr-assign>ipv4
config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign>ipv4
config>service>ies>if>sap>ipsec-gw>lcl-addr-assign>ipv6
config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign>ipv6

Description This command specifies the IPv4 or IPv6 source of the local address assignment for the IPsec gateway, which is a pool of a local DHCPv4 or DHCPv6 server. The system will assign an internal address to an IKEv2 remote-access client from the specified pool.

Beside the IP address, netmask and DNS server can also be returned. For IPv4, the netmask and DNS server address can be returned from the specified pool, as well as the IP address. The netmask returned to the IPsec client is derived from the subnet length from the **subnet** *x.x.x.x/m* **create** configuration, not the **subnet-mask** configuration in the subnet context. For IPv6, the DNS server address can be returned from the specified pool, as well as the IP address.

For IPv4, a secondary pool can be optionally specified. The secondary pool is used if the system is unable to assign addresses from the primary pool.

Default	no address-source
Parameters	<i>router-instance</i> — Specifies the router instance ID where the local DHCPv4 or DHCPv6 server is defined, up to 32 characters. This variant of the command is only supported in 'classic' configuration-mode (configure system management-interface configuration-mode classic). The address-source service-name service-name variant can be used in all configuration modes. <i>service-name</i> — Specifies the name of the service where the local DHCPv4 or DHCPv6 server is defined, up to 64 characters. <i>local-dhcp4-svr-name</i> — Specifies the name of the local DHCPv4 server, up to 32 characters. <i>local-dhcp6-svr-name</i> — Specifies the name of the local DHCPv6 server, up to 32 characters. <i>dhcp4-server-pool</i> — The name of the pool defined in the specified DHCPv4 server, up to 32 characters. <i>dhcp6-server-pool</i> — The name of the pool defined in the specified DHCPv6 server, up to 32 characters. <i>secondary-pool-name</i> — The name of the secondary pool defined in the specified server, up to 32 characters.

ipv6

Syntax	ipv6
Context	config>service>ies>if>sap>ipsec-gw>lcl-addr-assign config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign
Description	This command enables the context to configure IPv6 local address assignment parameters for the IPsec gateway.

local-gateway-address

Syntax	local-gateway-address ip-address no local-gateway-address
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw
Description	This command configures local gateway address of the IPsec gateway.
Parameters	<i>ip-address</i> — Specifies a unicast IPv4 address or a global unicast IPv6 address. This address must be within the subnet of the public interface.

local-gateway-address

Syntax	local-gateway-address <i>ip-address</i> peer <i>ip-address</i> delivery-service <i>service-id</i> no local-gateway-address
Context	config>service>vprn>if>sap>ipsec-tunnel
Description	This command specifies the local gateway address used for the tunnel and the address of the remote security gateway at the other end of the tunnel remote peer IP address to use.
Default	The base routing context is used if the delivery-router option is not specified.
Parameters	<i>ip-address</i> — IP address of the local end of the tunnel. delivery-service <i>service-id</i> — The ID of the IES or VPRN (front-door) delivery service of this tunnel. Use this service-id to find the VPRN used for delivery. Values <i>service-id</i> : 1 to 2147483648 <i>svc-name</i> : Specifies an existing service name up to 64 characters in length.

local-id

Syntax	local-id type { ipv4 fqdn ipv6 } [value <i>value</i>] no local-id
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw service>vprn>if>sap>ipsec-tun>dyn
Description	This command specifies the local ID for 7750 SRs used for IDi or IDr for IKEv2 tunnels. The no form of the command removes the parameters from the configuration.
Default	Depends on local-auth-method like following: • Psk:local tunnel ip address • Cert-auth: subject of the local certificate
Parameters	type — Specifies the type of local ID payload, it could be IPv4 or IPv6 address/FQDN domain name, distinguish name of subject in X.509 certificate. ipv4 — Specifies to use IPv4 as the local ID type, the default value is the local tunnel end-point address. ipv6 — Specifies to use IPv6 as the local ID type, the default value is the local tunnel end-point address. fqdn — Specifies to use FQDN as the local ID type. The value must be configured. <i>value</i> — Specifies the data type as an enumerated integer that describes the local identifier type used for IDi or IDr for IKEv2 up to 255 characters.

max-history-esp-key-records

Syntax	max-history-esp-key-records <i>max-records</i> no max-history-esp-key-records
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-tunnel
Description	This command enables the system to keep records of CHILD-SA keys for the corresponding ipsec-gw or ipsec-tunnel. There is a system wide limit of maximum number of IPsec tunnels that save keys. If the number of tunnel exceeds that limit, the system will not save keys for the new tunnels. Check with Nokia support for details of the limitation. This command is ignored if config>ipsec>no show-ipsec-keys is configured. The no form of the command prevents the system from keeping records.
Default	no max-history-esp-key-records
Parameters	<i>max-records</i> — Specifies the maximum number of recent records. Values 1 to 48

max-history-ike-key-records

Syntax	max-history-ike-key-records <i>max-records</i> no max-history-ike-key-records
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-tunnel
Description	This command enables system to keep records of IKE-SA keys for the corresponding ipsec-gw or ipsec-tunnel. This command is ignored if config>ipsec>no show-ipsec-keys is configured. There is a system wide limit of maximum number of IPsec tunnels that save keys. If the number of tunnel exceeds that limit, the system will not save keys for the new tunnels. Check with Nokia support for details of the limitation. The no form of the command prevents the system from keeping records.
Default	no max-history-ike-key-records
Parameters	<i>max-records</i> — Specifies the maximum number of recent records. Values 1 to 3

pre-shared-key

Syntax	pre-shared-key <i>key</i> [{ hash hash2 }] no pre-shared-key
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-tunnel>dynamic-keying
Description	This command configures the pre-shared key for the IPsec gateway or IPsec tunnel.
Default	no pre-shared-key
Parameters	key — An ASCII string to use as the pre-shared key for dynamic keying. When the hash or hash2 parameters are not used, the key is a clear text key; otherwise, the key text is encrypted. hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the hash2 encrypted variable cannot be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

radius-accounting-policy

Syntax	radius-accounting-policy <i>policy-name</i> no radius-accounting-policy
Context	config>service>ies>if>sap>ipsec-gw config>service>vprn>if>sap>ipsec-gw
Description	This command specifies the radius-accounting-policy to be used for the IKEv2 remote-access tunnels terminated on the ipsec-gw. The radius-accounting-policy is defined under config>ipsec context.
Parameters	<i>policy-name</i> — Specifies the name of an existing radius-accounting-policy.

radius-authentication-policy

Syntax	radius-authentication-policy <i>name</i> no radius-authentication-policy
Context	config>service>ies>if>sap>ipsec-gw

```
config>service>vprn>if>sap>ipsec-gw
```

Description This command specifies the policy to be used for the IKEv2 remote-access tunnels terminated on the IPsec GW. The **radius-authentication-policy** is defined under **config>ipsec** context.

Parameters *name* — Specifies the name of an existing RADIUS authentication policy.

cert

Syntax **cert**

Context config>service>ies>if>sap>ipsec-gw
config>service>vprn>if>sap>ipsec-gw

Description This command configures cert parameters used by this SAP IPsec gateway.

status-verify

Syntax **status-verify**

Context config>service>ies>if>sap>ipsec-gw>cert
config>service>vprn>if>sap>ipsec-gw>cert
config>service>vprn>if>sap>ipsec-tun>dyn>cert

Description This command enables the context to configure certificate revocation status verification parameters.

default-result

Syntax **default-result {revoked | good}**
no default-result

Context config>service>ies>if>sap>ipsec-gw>cert>status-verify
config>service>vprn>if>sap>ipsec-gw>cert>status-verify
config>service>vprn>if>sap>ipsec-tun>dyn>cert>status-verify

Description This command specifies the default result when both the primary and secondary method failed to provide an answer.

Default default-result revoked

Parameters **good** — Specifies that the certificate is considered as acceptable.
revoked — Specifies that the certificate is considered as revoked.

primary

Syntax	primary <i>primary</i> secondary <i>secondary</i>
Context	config>service>ies>if>sap>ipsec-gw>cert>status-verify config>service>vpn>if>sap>ipsec-gw>cert>status-verify config>service>vpn>if>sap>ipsec-tun>dyn>cert>status-verify
Description	This command specifies the primary and secondary methods that are used to verify the revocation status of the peer's certificate; either CRL or OCSP. OCSP or CRL uses the corresponding configuration in the CA profile of the issuer of the certificate in question.
Default	primary crl
Parameters	<i>primary</i> — Specifies the primary method of Certificate Status Verification (CSV) that is used to verify the revocation status of the certificate of the peer. Values ocsp — Specifies that the OCSP protocol should be used. The OCSP server is configured in the corresponding CA profile. crl — Specifies that the local CRL file should be used. The CRL file is configured in the corresponding CA profile. Default crl <i>secondary</i> — Specifies the secondary method of CSV that is used to verify revocation status of the certificate of the peer. Values ocsp — Specifies that the OCSP protocol should be used. The OCSP server is configured in the corresponding CA profile. crl — Specifies that the local CRL file should be used. The CRL file is configured in the corresponding CA profile. none — Specifies that no secondary methods of CSV are used. Default none

client-db

Syntax	client-db <i>name</i> client-db <i>name</i> fallback client-db <i>name</i> no-fallback no client-db
Context	config>service>ies>if>sap>ipsec-gw config>service>vpn>if>sap>ipsec-gw
Description	This command enables the use of an IPsec client database. The system uses the specified client database to authenticate IKEv2 dynamic LAN-to-LAN tunnel.

Default	no client-db
Parameters	<i>name</i> — Specifies the name of the client database fallback — Specifies whether or not this IPsec gateway falls back to the default authentication policy when the IPsec tunnel authentication request fails to match any clients in the IPsec database. no-fallback — Specifies that if the client database lookup fails to return a matched result, the system will fail the tunnel setup.

4.14.2.13 RADIUS Policy Commands

radius-accounting-policy

Syntax	radius-accounting-policy <i>name</i> [create] no radius-accounting-policy <i>name</i>
Context	config>ipsec
Description	This command specifies an existing RADIUS accounting policy to use to collect accounting statistics on this subscriber profile by RADIUS. This command is used independently of the collect-stats command.
Parameters	<i>name</i> — Specifies an existing RADIUS based accounting policy.

radius-authentication-policy

Syntax	radius-authentication-policy <i>name</i> [create] no radius-authentication-policy <i>name</i>
Context	config>ipsec
Description	This command specifies the radius authentication policy associated with this IPsec gateway.

include-radius-attribute

Syntax	[no] include-radius-attribute
Context	config>ipsec>rad-acct-plcy config>ipsec>rad-auth-plcy
Description	This command enables the context to specify the RADIUS parameters that the system should include into RADIUS authentication-request messages.

acct-stats

Syntax	[no] acct-stats
Context	config>ipsec>rad-acct-plcy>include
Description	This command enables the system to include accounting attributes in RADIUS acct-stop and interim-update packets. The no form of the command disables the system from including accounting attributes in RADIUS acct-stop and interim-update packets.

called-station-id

Syntax	[no] called-station-id
Context	config>ipsec>rad-acct-plcy>include config>ipsec>rad-auth-plcy>include
Description	This command includes called station ID attributes. The no form of the command excludes called station ID attributes.
Default	no called-station-id

calling-station-id

Syntax	[no] calling-station-id
Context	config>ipsec>rad-acct-plcy>include config>ipsec>rad-auth-plcy>include
Description	This command enables the inclusion of the calling-station-id attribute in RADIUS authentication requests and RADIUS accounting messages.
Default	no calling-station-id

client-cert-subject-key-id

Syntax	[no] client-cert-subject-key-id
Context	config>ipsec>rad-auth-plcy>include
Description	This command enables the inclusion of the Subject Key Identifier of the peer's certificate in the RADIUS Access-Request packet as VSA: Alc-Subject-Key-Identifier. Refer to the <i>7750 SR and VSR RADIUS Attributes Reference Guide</i> for more information.

Default no client-cert-subject-key-id

framed-ip-addr

Syntax [no] **framed-ip-addr**

Context config>ipsec>rad-acct-plcy>include

Description This command enables the inclusion of the **framed-ip-addr** attribute.

Default no framed-ip-addr

framed-ipv6-prefix

Syntax [no] **framed-ipv6-prefix**

Context config>ipsec>rad-acct-plcy>include

Description This command enables the inclusion of the **framed-ipv6-prefix** attribute.

Default no framed-ip-addr

nas-identifier

Syntax [no] **nas-identifier**

Context config>ipsec>rad-acct-plcy>include
config>ipsec>rad-auth-plcy>include

Description This command enables the generation of the **nas-identifier** RADIUS attribute.

Default no nas-identifier

nas-ip-addr

Syntax [no] **nas-ip-addr**

Context config>ipsec>rad-acct-plcy>include
config>ipsec>rad-auth-plcy>include

Description This command enables the generation of the NAS IP address attribute.

Default no nas-ip-addr

nas-port-id

Syntax	[no] nas-port-id
Context	config>ipsec>rad-acct-plcy>include config>ipsec>rad-auth-plcy>include
Description	This command enables the generation of the nas-port-id RADIUS attribute. Optionally, the value of this attribute (the SAP-id) can be prefixed by a fixed string and suffixed by the circuit-id or the remote-id of the client connection. If a suffix is configured, but no corresponding data is available, the suffix used will be 0/0/0/0/0/0.
Default	no nas-port-id

radius-server-policy

Syntax	radius-server-policy <i>radius-server-policy-name</i> no radius-server-policy
Context	config>ipsec>rad-acct-plcy config>ipsec>rad-auth-plcy
Description	This command references an existing radius-server-policy (available under the config>aaa context) for use in subscriber management authentication and accounting. When configured in an authentication-policy, following CLI commands are ignored in the policy to avoid conflicts: • all commands in the radius-authentication-server context • accept-authorization-change • coa-script-policy • accept-script-policy • request-script-policy When configured in a radius-accounting-policy, following CLI commands are ignored in the policy to avoid conflicts: • all commands in the radius-accounting-server context • acct-request-script-policy The no form of the command removes the radius-server-policy reference from the configuration
Default	no radius-server-policy
Parameters	<i>radius-server-policy-name</i> — Specifies the RADIUS server policy.

update-interval

Syntax	update-interval <i>minutes</i> [<i>jitter seconds</i>] no update-interval
Context	config>ipsec>rad-acct-plcy
Description	This command enables the system to send RADIUS interim-update packets for IKEv2 remote-access tunnels. The RADIUS attributes in the interim-update packet are the same as acct-start. The value of the Acct-status-type in the interim-update message is 3.
Default	update-interval 10
Parameters	<i>minutes</i> — Specifies the interval in minutes. Values 5 to 259200 <i>seconds</i> — Specifies the jitter as the number of seconds when the system sends each interim-update packet. Values 0 to 3600

password

Syntax	password <i>password</i> [hash hash2] no password
Context	config>ipsec>rad-auth-plcy
Description	This command specifies the password that is used in the RADIUS access requests. The no form of the command resets the password to its default of ALU and will be stored using hash/hash2 encryption.
Default	no password
Parameters	<i>password</i> — Specifies a password string up to 64characters. hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the hash2 encrypted variable cannot be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

4.14.2.14 CMPv2 Commands

pki

Syntax	pki
Context	config>system>security
Description	This command enables the context to configure PKI related parameters.

ca-profile

Syntax	ca-profile <i>name</i> [create] no ca-profile <i>name</i>
Context	config>system>security>pki
Description	This command creates a new ca-profile or enters the configuration context of an existing ca-profile. Up to 128 ca-profiles can be created in the system. A shutdown of the ca-profile will not affect the current up and running ipsec-tunnel or ipsec-gw that is associated with the ca-profile. However, authentication afterwards will fail with a shutdown ca-profile. Executing a no shutdown command in this context will cause the system to reload the configured cert-file and crl-file. A ca-profile can be applied under the ipsec-tunnel or ipsec-gw configuration. The no form of this command removes the name parameter from the configuration. A ca-profile cannot be removed until all the associated entities (ipsec-tunnel/gw) have been removed.
Parameters	<i>name</i> — Specifies the name of the ca-profile up to 32 characters. create — Keyword used to create a new ca-profile. The create keyword requirement can be enabled or disabled in the environment>create context.

certificate

Syntax	certificate
Context	admin
Description	This command enables the context to configure X.509 certificate related operational parameters.

certificate-display-format

Syntax	certificate-display-format {ascii utf8}
Context	config>system>security>pki
Description	This command specifies the certificate subject display format.
Default	certificate-display-format ascii
Parameters	ascii — Use ASCII encoding. utf8 — Use utf8 encoding.

cmpv2

Syntax	cmpv2
Context	admin>certificate config>system>security>pki>ca-profile
Description	This command enables the context to configure CMPv2 parameters. Changes are not allowed when the CA profile is enabled (no shutdown).

accept-unprotected-errormsg

Syntax	[no] accept-unprotected-errormsg
Context	config>system>security>pki>ca-profile>cmpv2
Description	This command enables the system to accept both protected and unprotected CMPv2 error message. Without this command, system will only accept protected error messages. The no form of the command causes the system to only accept protected PKI confirmation message.
Default	no accept-unprotected-errormsg

accept-unprotected-pkiconf

Syntax	[no] accept-unprotected-pkiconf
Context	config>system>security>pki>ca-profile>cmpv2
Description	This command enables the system to accept both protected and unprotected CMPv2 PKI confirmation messages. Without this command, system will only accept protected PKI confirmation message.

The **no** form of the command causes the system to only accept protected PKI confirmation message.

Default no accept-unprotected-pkiconf

always-set-sender-for-ir

Syntax [no] **always-set-sender-for-ir**

Context config>system>security>pki>ca-profile>cmpv2

Description This command specifies to always set the sender field in CMPv2 header of all Initial Registration (IR) messages with the subject name. By default, the sender field is only set if an optional certificate is specified in the CMPv2 request.

Default no always-set-sender-for-ir

key-list

Syntax **key-list**

Context config>system>security>pki>ca-profile>cmpv2

Description This command enables the context to configure pre-shared key list parameters.

key

Syntax **key** *password* [**hash** | **hash2**] **reference** *reference-number*
no key **reference** *reference-number*

Context config>system>security>pki>ca-profile>cmpv2>key-list

Description This command specifies a pre-shared key used for CMPv2 initial registration. Multiples of key commands are allowed to be configured under this context.

The password and reference-number is distributed by the CA via out-of-band means.

The configured password is stored in configuration file in an encrypted form by using SR OS hash2 algorithm.

The **no** form of the command removes the parameters from the configuration.

Parameters *password* — Specifies a printable ASCII string, up to 64 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

reference *reference-number* — Specifies a printable ASCII string, up to 64 characters in length.

url

Syntax	url <i>url-string</i> [service-id <i>service-id</i>] url <i>url-string</i> [service-name <i>service-name</i>] no url
Context	config>system>security>pki>ca-profile>cmpv2
Description	This command specifies HTTP URL of the CMPv2 server. The URL must be unique across all configured ca-profiles. The URL will be resolved by the DNS server configured (if configured) in the corresponding router context. If the <i>service-id</i> is 0 or omitted, then system will try to resolve the FQDN via DNS server configured in bof.cfg. After resolution, the system will connect to the address in management routing instance first, then base routing instance. If the service is VPRN, then the system only allows HTTP ports 80 and 8080.
Default	no url
Parameters	<i>url-string</i> — Specifies the HTTP URL of the CMPv2 server up to 180 characters. service-id <i>service-id</i> — Specifies the service instance that used to reach CMPv2 server. Values Service ID: 1 to 2147483647 base-router: 0

revocation-check

Syntax	revocation-check { crl crl-optional }
Context	config>system>security>pki>ca-profile

Description This command specifies the revocation method system used to check the revocation status of certificate issued by the CA, the default value is **crl**, which will use CRL. But if it is **crl-optional**, then it means when the user disables the ca-profile, then the system will try to load the configured CRL (specified by the **crl-file** command). However, if the system fails to load it for following reasons, then the system still brings the ca-profile oper-up, but leaves the CRL as **non-exist**.

- CRL file does not exist
- CRL is not properly encoded - maybe due to interrupted file transfer
- CRL does not match cert
- Wrong CRL version
- CRL expired

If the system needs to use the CRL of a specific ca-profile to check the revocation status of an end-entity cert, and the CRL is non-existent due to the above reasons, then the system will treat it as being unable to get an answer from CRL and fall back to the next status-verify method or default-result.

If the system needs to check the revocation of a CA cert in cert chain, and if the CRL is non-existent due to the above reasons, then the system will skip checking the revocation status of the CA cert. For example, if CA1 is issued by CA2, if CA2's revocation-check is **crl-optional** and the CA2's CRL is non-existent, then the system will not check CA1 cert's revocation status and consider it as "good".



Note: Users must shutdown the ca-profile to change the revocation-check configuration.

Default revocation-check crl

Parameters **crl** — Specifies to use the configured CRL.
crl-optional — Specifies that the CRL is optional.

http-response-timeout

Syntax **http-response-timeout** *timeout*
no http-response-timeout

Context config>system>security>pki>ca-profile>cmpv2

Description This command specifies the timeout value for HTTP response that is used by CMPv2.
The **no** form of the command reverts to the default.

Default http-response-timeout 30

Parameters *timeout* — Specifies the HTTP response timeout, in seconds.
Values 1 to 3600

http-version

Syntax **http-version** [1.0 | 1.1]
Context config>system>security>pki>ca-profile>cmpv2
Description This command configures the HTTP version for CMPv2 messages.
Default http-version 1.1

response-signing-cert

Syntax **response-signing-cert** *filename*
no response-signing-cert
Context config>system>security>pki>ca-profile>cmpv2
Description This command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA's certificate will be used.
Default no response-signing-cert
Parameters *filename* — Specifies the filename of the imported certificate.

same-recipnonce-for-pollreq

Syntax [**no**] **same-recipnonce-for-pollreq**
Context config>system>security>pki>ca-profile>cmpv2
Description This command enables the system to use same recipNonce as the last CMPv2 response for poll request.
Default no same-recipnonce-for-pollreq

cert-request

Syntax **cert-request** **ca** *ca-profile-name* **current-key** *key-filename* **current-cert** *cert-filename*
[**hash-alg** *hash-algorithm*] **newkey** *key-filename* **subject-dn** *subject-dn* [**domain-name**
domain-names] [**ip-addr** *ip-address* | *ipv6-address*] **save-as** *save-path-of-result-cert*

Context	admin>certificate>cmpv2
Description	This command requests an additional certificate after the system has obtained the initial certificate from the CA. The request is authenticated by a signature signed by the current-key, along with the current-cert. The hash algorithm used for signature is depends on the key type: • DSA key: SHA1 • RSA key: MD5/SHA1/SHA224 SHA256 SHA384 SHA512, by default is SHA1 In some cases, the CA may not return a certificate immediately, due to reasons such as request processing need manual intervention. In such cases, the admin certificate cmpv2 poll command can be used to poll the status of the request.
Parameters	ca <i>ca-profile-name</i> — Specifies a ca-profile name which includes CMP server information up to 32 characters. current-key <i>key-filename</i> — Specifies corresponding certificate issued by the CA up to 95 characters. current-cert <i>cert-filename</i> — Specifies the file name of an imported certificate that is attached to the certificate request up to 95 characters. newkey <i>key-filename</i> — Specifies the file name of the imported key up to 95 characters. hash-alg <i>hash-algorithm</i> — Specifies the hash algorithm for RSA key. Values md5,sha1,sha224,sha256,sha384,sha512 subject-dn <i>dn</i> — Specifies the subject of the requesting certificate up to 256 characters. Values attr1=val1,attr2=val2where: attrN={C ST O OU CN} save-as <i>save-path-of-result-cert</i> — Specifies the save full path name of saving the result certificate, up to 200 characters. domain-name <i>domain-names</i> — Specifies FQDNs for SubjectAltName of the requesting certificate, separated by commas, up to 512 characters. ip-addr <i>ip-address</i> <i>ipv6-address</i> — Specifies an IPv4 or IPv6 address for SubjectAtName of the requesting certificate.

clear-request

Syntax	clear-request <i>ca ca-profile-name</i>
Context	admin>certificate>cmpv2
Description	This command clears current pending CMPv2 requests toward the specified CA. If there are no pending requests, it will clear the saved result of prior request.
Parameters	ca <i>ca-profile-name</i> — Specifies a ca-profile name up to 32 characters.

initial-registration

Syntax **initial-registration** *ca ca-profile-name* **key-to-certify** *key-filename* **protection-alg** **{password password reference ref-number | signature [cert cert-file-name [send-chain [with-ca ca-profile-name]]] [protection-key key-file-name] [hash-alg {md5 | sha1 | sha224 | sha256 | sha384 | sha512}} subject-dn dn [domain-name domain-names] [ip-addr ip-address | ipv6-address] save-as save-path-of-result-cert**

Context admin>certificate>cmpv2

Description This command request initial certificate from CA by using CMPv2 initial registration procedure.

The **ca** parameter specifies a CA-profile which includes CMP server information.

The **key-to-certify** is an imported key file to be certified by the CA.

The protection-key is an imported key file used to for message protection if protection-alg is signature.

The request is authenticated either of following methods:

- A password and a reference number that pre-distributed by CA via out-of-band means.
- The specified password and reference number are not necessarily in the cmp-keylist configured in the corresponding CA-Profile
- A signature signed by the protection-key or key-to-certify, optionally along with the corresponding certificate. If the protection-key is not specified, system will use the key-to-certify for message protection. The hash algorithm used for signature is depends on key type:
 - DSA key: SHA1
 - RSA key: MD5/SHA1/SHA224 | SHA256 | SHA384 | SHA512, by default is SHA1

Optionally, the system could also send a certificate or a chain of certificates in extraCerts field. Certificate is specified by the “cert” parameter, it must include the public key of the key used for message protection.

Sending a chain is enabled by specify the **send-chain** parameter.

subject-dn specifies the subject of the requesting certificate.

save-as specifies full path name of saving the result certificate.

In some cases, CA may not return certificate immediately, due to reason like request processing need manual intervention. In such cases, the **admin certificate cmpv2** poll command could be used to poll the status of the request. If key-list is not configured in the corresponding **ca-profile**, then the system will use the existing password to authenticate the CMPv2 packets from server if it is in password protection.

If key-list is configured in the corresponding **ca-profile** and server doesn't send SenderKID, then the system will use lexicographical first key in the key-list to authenticate the CMPv2 packets from server in case it is in password protection.

Parameters	<i>ca-profile-name</i> — Specifies a ca-profile name which includes CMP server information up to 32 characters.
	<i>key-filename</i> — Specifies the file name of the key to certify up to 95 characters.
	<i>password</i> — Specifies an ASCII string up to 64 characters.
	<i>ref-number</i> — Specifies the reference number for this CA initial authentication key up to 64 characters.
	<i>cert-file-name</i> — specifies the certificate file up to 95 characters.
	<i>ca-profile-name</i> — Specifies to send the chain.
	<i>key-file-name</i> — Specifies the protection key associated with the action on the CA profile.
	<i>hash-algorithm</i> — Specifies the hash algorithm for RSA key.
	Values md5,sha1,sha224,sha256,sha384,sha512
	<i>dn</i> — Specifies the subject of the requesting certificate up to 256 characters.
	Values attr1 equals val1 attr2 equals val2 where: attrN equals {C ST O OU CN}
	<i>save-path-of-result-cert</i> — Specifies the save full path name of saving the result certificate up to 200 characters.
	domain-name <i>domain-names</i> — Specifies FQDNs for SubjectAltName of the requesting certificate, separated by commas, up to 512 characters.
	<i>ip-address</i> <i>ipv6-address</i> — Specifies an IPv4 or IPv6 address for SubjectAtName of the requesting certificate.

key-update

Syntax	key-update ca <i>ca-profile-name</i> newkey <i>key-filename</i> oldkey <i>key-filename</i> oldcert <i>cert-filename</i> [hash-alg <i>hash-algorithm</i>] save-as <i>save-path-of-result-cert</i>
Context	admin>certificate>cmpv2
Description	This command requests a new certificate from the CA to update an existing certificate due to reasons such as key refresh or replacing compromised key. In some cases, the CA may not return certificate immediately, due to reasons such as request processing need manual intervention. In such cases, the admin certificate cmpv2 poll command can be used to poll the status of the request.
Parameters	<i>ca-profile-name</i> — Specifies a ca-profile name which includes CMP server information up to 32 characters.

- key-filename* — Specifies the key file of the requesting certificate up to 95 characters.
- key-filename* — Specifies the key to be replaced up to 95 characters.
- cert-filename* — Specifies the file name of an imported certificate to be replaced up to 95 characters.
- hash-algorithm* — Specifies the hash algorithm for RSA key.
 - Values** md5,sha1,sha224,sha256,sha384,sha512
- save-path-of-result-cert* — Specifies the save full path name of saving the result certificate up to 200 characters.

poll

Syntax	poll ca <i>ca-profile-name</i>
Context	admin>certificate>cmpv2
Description	This command polls the status of the pending CMPv2 request toward the specified CA. If the response is ready, this command will resume the CMPv2 protocol exchange with server as the original command would do. The requests could be also still be pending as a result, then this command could be used again to poll the status. SR OS allows only one pending CMP request per CA, which means no new request is allowed when a pending request is present.
Parameters	<i>ca-profile-name</i> — Specifies a ca-profile name up to 32 characters.

show-request

Syntax	show-request [ca <i>ca-profile-name</i>]
Context	admin>certificate>cmpv2
Description	This command displays current the CMPv2 pending request toward the specified CA. If there is no pending request, the last pending request is displayed including the status (success/fail/rejected) and the receive time of last CMPv2 message from server. The following information is included in the output: • Request type, original input parameter (password is not displayed), checkAfter and reason in of last PollRepContent, time of original command input.
Parameters	<i>ca-profile-name</i> — Specifies a ca-profile name up to 32 characters. If not specified, the system will display pending requests of all ca-profiles.

4.14.2.15 Auto-Update Command Descriptions

file-transmission-profile

Syntax	file-transmission-profile <i>name</i> [create] no file-transmission-profile <i>name</i>
Context	config>system
Description	This command creates a new file transmission profile or enters the configuration context of an existing file-transmission-profile. The file-transmission-profile context defines transport parameters for protocol such as HTTP, include routing instance, source address, timeout value, and so on.
Parameters	<i>name</i> — Specifies the file-transmission-profile name, up to 32 characters.

ipv4-source-address

Syntax	ipv4-source-address <i>ip-address</i> no ipv4-source-address
Context	config>system>file-trans-prof
Description	This command specifies the IPv4 source address used for transport protocol. The no form of this command uses the default source address which typically is the address of the egress interface.
Default	no ipv4-source-address
Parameters	<i>ip-address</i> — Specifies a unicast v4 address. This should be a local interface address.

ipv6-source-address

Syntax	ipv6-source-address <i>ipv6-address</i> no ipv6-source-address
Context	config>system>file-trans-prof
Description	This command specifies the IPv6 source address used for transport protocol. The no form of this command uses the default source address which typically is the address of egress interface.
Default	no ipv6-source-address

Parameters *ipv6-address* — Specifies a unicast v6 address. This should be a local interface address.

redirection

Syntax **redirection** *level*
 no redirection

Context config>system>file-trans-prof

Description This command enables system to accept HTTP redirection response, along with the max level of redirection. The virtual router may send a new request to another server if the requested resources are not available (temporarily available to another server).

Default no redirection

Parameters *level* — Specifies the maximum level of redirection of the file transmission profile max level of HTTP redirection.

Values 1 to 8

retry

Syntax **retry** *count*
 no retry

Context config>system>file-trans-prof

Description This command specifies the number of retries on transport protocol level.

 When the virtual router does not receive any data from a server (e.g., FTP or HTTP server) after the configured **timeout seconds**, the router may repeat the request to the server. The number of retries specifies the maximum number of repeated requests.

 The **no** form of this command disables the retry.

Default no retry

Parameters *count* — Specifies the number of retries.

Values 1 to 256

router

Syntax **router** *router-instance*
 router service *vprn-service-name*

Context config>system>file-trans-prof

Description	This command specifies the routing instance that the transport protocol uses.
Default	router Base
Parameters	<i>router-instance</i> — Specifies the router instance on which the file transmission connection will be established. This variant of the command is only supported in 'classic' configuration-mode (configure system management-interface configuration-mode classic). The router service <i>vprn-service-name</i> variant can be used in all configuration modes.
Values	{router-name <i>vprn-svc-id</i> } <i>router-name</i> : Base, management <i>router-name</i> is an alias for input only. The <i>router-name</i> gets replaced with an id automatically by SR OS in the configuration). <i>vprn-svc-id</i> : 1 to 2147483647
Default	Base
	service <i>vprn-service-name</i> — Identifies the service, up to 64 characters.

timeout

Syntax	timeout <i>seconds</i>
Context	config>system>file-trans-prof
Description	This command specifies timeout value in seconds for transport protocol. The timeout is the maximum waiting time to receive any data from the server (e.g., FTP or HTTP server).
Default	timeout 60
Parameters	<i>seconds</i> — Specifies the connection timeout (in seconds) for the file transmission.
Values	1 to 3600

auto-crl-update

Syntax	auto-crl-update [create] no auto-crl-update
Context	config>system>security>pki>ca-prof
Description	This command creates an auto CRL update configuration context with the create parameter, or enters the auto-crl-update configuration context without the create parameter.

This mechanism auto downloads a CRL file from a list of configured HTTP URLs either periodically or before existing CRL expires. If the downloaded CRL is more recent than the existing one, then the existing one will be replaced.



Note: The configured URL must point to a DER encoded CRL file.

Parameters **create** — Creates an auto CRL update for the ca-profile.

crl-urls

Syntax **crl-urls**

Context config>system>security>pki>ca-prof>auto-crl-update

Description This command enables the context to configure **crl-urls** parameters. The system allows up to eight URL entries to be configured and will try each URL in order and stop when a qualified CRL is successfully downloaded. A qualified CRL is a valid CRL signed by the CA and is more recent than the existing CRL.

 If none of the configured URLs returns a qualified CRL, then:

- If the schedule-type is next-update-based, system will wait for configure retry-interval before it start from beginning of the list again.
- If the schedule-type is periodic, then system will wait till next periodic update time.

 If the user wants to manually stop the download, shutting down of auto-crl-retrieval could be used to achieve this.

url-entry

Syntax **url-entry** *entry-id* [**create**]
 no url-entry *entry-id*

Context config>system>security>pki>ca-prof>auto-crl-update>crl-urls

Description This command creates a new **crl-url** entry with the **create** parameter, or enters an existing url-entry configuration context without **create** parameter.

 The **no** form of this command removes the specified entry.

Parameters *entry-id* — Specifies a URL configured on this system.

Values 1 to 8

create — Creates an auto URL entry.

file-transmission-profile

Syntax	file-transmission-profile <i>profile-name</i> no file-transmission-profile
Context	config>system>security>pki>ca-prof>auto-crl-update>crl-urls>url-entry
Description	This command specifies the file-transmission-profile for the url-entry . When the system downloads a CRL from the configured URL in the url-entry it will use the transportation parameter configured in the file-transmission-profile . auto-crl-update supports Base/Management/VPNN routing instance. vpls-management is not supported. In case of VPNN, the HTTP server port can only be 80 or 8080. The no form of the command removes the specified profile name.
Default	no file-transmission-profile
Parameters	<i>profile-name</i> — Specifies the name of the file transmission profile to be matched up to 32 characters. The profile name is configured in the config>system>file-transmission-profile context.

url

Syntax	url <i>url</i> no url
Context	config>system>security>pki>ca-prof>auto-crl-update>crl-urls> url-entry
Description	This command specifies the HTTP URL of the CRL file for the url-entry . The system supports both IPv4 and IPv6 HTTP connections. Note: The URL must point to a DER encoded CRL.
Default	no url
Parameters	<i>url</i> — Specifies the URL, which specifies the location, where an updated CRL can be downloaded from.

periodic-update-interval

Syntax	periodic-update-interval [days <i>days</i>] [hrs <i>hours</i>] [min <i>minutes</i>] [sec <i>seconds</i>]
Context	config>system>security>pki>ca-prof>auto-crl-update

Description	This command specifies the interval for periodic updates. The minimal interval is 1 hour. The maximum interval is 366 days.
Default	periodic-update-interval days 1
Parameters	days <i>days</i> — Specifies the number of days for periodic updates. Values 0 to 366 <i>hours</i> — Specifies the number of hours for periodic updates. Values 0 to 23 <i>minutes</i> — Specifies the number of minutes for periodic updates. Values 0 to 59 <i>seconds</i> — Specifies the number of seconds for periodic updates. Values 0 to 59

retry-interval

Syntax	retry-interval <i>seconds</i> no retry-interval
Context	config>system>security>pki>ca-prof>auto-crl-update
Description	This command specifies the interval, in seconds, that the system waits before retrying the configured url-entry list when schedule-type is next-update-based and none of the URLs return a qualified CRL. The no form of the command causes the system to retry immediately without waiting.
Default	retry-interval 3600
Parameters	<i>seconds</i> — Specifies an interval, in seconds, before retrying to update the CRL. Values 1 to 31622400

pre-update-time

Syntax	pre-update-time [days <i>days</i>] [hrs <i>hours</i>] [min <i>minutes</i>] [sec <i>seconds</i>]
Context	config>system>security>pki>ca-prof>auto-crl-update
Description	This command specifies the pre-download time for next-update-based update.
Default	pre-update-time hrs 1

Parameters	<i>days</i> — Specifies the time period, in days, prior to the next update time of the current CRL. Values 0 to 366 <i>hours</i> — Specifies the time period, in hours, prior to the next update time of the current CRL. Values 0 to 23 <i>minutes</i> — Specifies the time period, in minutes, prior to the next update time of the current CRL. Values 0 to 59 <i>seconds</i> — Specifies the time period, in seconds, prior to the next update time of the current CRL. Values 0 to 59

schedule-type

Syntax	schedule-type <i>schedule-type</i>
Context	config>system>security>pki>ca-prof>auto-crl-update
Description	This command specifies the schedule type for auto CRL update. The system supports two types: • periodic: — The system will download a CRL periodically at the interval configured via the periodic-update-interval command. For example, if the periodic-update-interval is 1 day, then the system will download a CRL every 1 day. The minimal periodic-update-interval is 1 hour. • next-update-based — The system will download a CRL at the time = Next_Update_of_existing_CRL <i>minus</i> pre-update-time. For example, if the Next-Update of the existing CRL is 2015-06-30 06:00 and pre-update-time is 1 hour, then the system will start downloading at 2015-06-30, 05:00.
Default	schedule-type next-update-based
Parameters	<i>schedule-type</i> — Specifies the type of time scheduler to update the CRL. Values periodic, next-update-based

shutdown

Syntax	[no] shutdown
Context	config>system>security>pki>ca-prof>auto-crl-update
Description	This command disables the auto CRL update.

The **no** form of this command enables an auto CRL update. Upon **no shutdown**, if the configured CRL file does not exist, is invalid or is expired or if the schedule-type is next-update-based and current time passed (Next-Update_of_existing_CRL - pre-update-time), then system will start downloading CRL right away.

Default shutdown

crl-update

Syntax **crl-update ca** *ca-profile-name*

Context admin>certificate

Description This command manually triggers the CRL update for the specified **ca-profile**.
Using this command requires shutting down the auto-crl-update.

Parameters *ca-profile-name* — Specifies the name of the Certificate Authority profile.

4.14.2.16 IPsec Mastership Election Commands

The commands described in this section are supported on the 7750 SR only.

multi-chassis

Syntax **multi-chassis**

Context config>redundancy

Description This command enables the context to configure multi-chassis parameters.

peer

Syntax **peer** *ip-address* [**create**]
no peer *ip-address*

Context config>redundancy>multi-chassis

Description This command configures a multi-chassis redundancy peer.

Parameters *ip-address* — Specifies the peer address.
create — Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled or disabled in the **environment>create** context.

mc-ipsec

Syntax	[no] mc-ipsec
Context	config>redundancy>multi-chassis>peer
Description	This command enables the context to configure multi-chassis peer parameters.

bfd-enable

Syntax	[no] bfd-enable
Context	config>redundancy>multi-chassis>peer>mc-ipsec
Description	This command enables tracking a central BFD session, if the BFD session goes down, then system consider the peer is down and change the mc-ipsec status of configured tunnel-group accordingly. The BFD session uses specified the loopback interface (in the specified service) address as the source address and uses specified dst-ip as the destination address. Other BFD parameters are configured with the bfd command on the specified interface.
Default	no bfd-enable

discovery-interval

Syntax	discovery-interval <i>interval-secs</i> [boot <i>interval-secs</i>] no discovery-interval
Context	config>redundancy>multi-chassis>peer>mc-ipsec
Description	This command specifies the time interval of tunnel-group stays in the Discovery state. Interval-1 is used as discovery-interval when a new tunnel-group is added to multi-chassis redundancy (mp-ipsec); interval-2 is used as discovery-interval when system boot-up, it is optional, when it is not specified, the interval-1 will be used.
Default	discovery-interval 300 boot 300
Parameters	<i>interval-secs</i> — Specifies the maximum duration, in seconds, of the discovery interval during which a newly activated multi- chassis IPsec tunnel-group will remain dormant while trying to contact its redundant peer. Groups held dormant in this manner will neither pass traffic nor negotiate security keys. This interval ends when either the redundant peer is contacted and a master election occurs, or when the maximum duration expires. Values 1 to 1800

interval-secs — Specifies the maximum duration of an interval immediately following system start up. When the normal discovery interval for a group would expire while the post-boot discovery interval is still active, then the group's discovery interval is extended until the post-boot discovery interval expires. This allows an extension to the normal discovery stage of groups following a chassis reboot, to account for the larger variance in routing

Values 1 to 1800

hold-on-neighbor-failure

Syntax `hold-on-neighbor-failure multiplier`
`no hold-on-neighbor-failure`

Context config>redundancy>multi-chassis>peer>mc-ipsec

Description	This command specifies the number of keep-alive failures before the peer is considered to be down.

The **no** form of the command reverts to the default.

Default hold-on-neighbor-failure 3

Parameters *multiplier* — Specifies the hold time applied on the neighbor failure

Values 2 to 25

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context config>redundancy>multi-chassis>peer>mc-ipsec

Description	This command specifies the time interval of the mastership election protocol sending keep-alive packet.

The **no** form of the command reverts to the default.

Default keep-alive-interval 10

Parameters *interval* — Specifies the keep alive interval in tenths of seconds.

Values 5 to 500

tunnel-group

Syntax `tunnel-group tunnel-group-id [create]`

no tunnel-group *tunnel-group-id*

Context	config>redundancy>multi-chassis>peer>mc-ipsec
Description	This command enables multi-chassis redundancy for specified tunnel-group; or enters an already configured tunnel-group context. The configured tunnel-group could failover independently. The no form of the command removes the tunnel group ID from the configuration.
Parameters	<i>tunnel-group-id</i> — Specifies the tunnel-group identifier.
Values	1 to 16

peer-group

Syntax	peer-group <i>tunnel-group-id</i> no peer-group
Context	config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group
Description	This command specifies the corresponding tunnel-group id on peer node. The peer tunnel-group id does not necessary equals to local tunnel-group id. The no form of the command removes the tunnel group ID from the configuration.
Parameters	<i>tunnel-group-id</i> — Specifies the tunnel-group identifier.
Values	1 to 16

priority

Syntax	priority <i>priority</i> no priority
Context	config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group
Description	This command specifies the local priority of the tunnel-group, this is used to elect master, higher number win. If priority are same, then the peer has more active ISA win; and priority and the number of active ISA are same, then the peer with higher IP address win. The no form of the command removes the priority value from the configuration.
Default	priority 100
Parameters	<i>priority</i> — Specifies the priority of this tunnel-group.
Values	0 to 255

state

Syntax	state <i>state</i> no <i>state</i>												
Context	config>router>policy-options>policy-statement>entry>from												
Description	This command will configure a match criteria on the state attribute. The state attribute carries the state of an SRRP instance and it can be applied to: • subscriber-interface routes • subscriber-management routes (/32 IPv4 and IPv6 PD wan-host) • managed-routes (applicable only to IPv4). Based on the state attribute of the route we can manipulate the route advertisement into the network. We can enable or disable (in case there is no SRRP running) tracking of SRRP state by routes. This is done on a per subscriber-interface route basis, where a subscriber-interface route is tracking a single SRRP instance state (SRRP instance might be in a Fate Sharing Group). For subscriber-management and managed-routes, tracking is enabled per group interface under which SRRP is enabled.												
Parameters	<i>state</i> — The state attribute. <table><tr><th>Values</th><th></th></tr><tr><td>srrp-master</td><td>Track routes with the state attribute carrying srrp-master state</td></tr><tr><td>srrp-non-master</td><td>Track routes with the state attribute carrying srrp-non-master state.</td></tr><tr><td>ipsec-master-with-peer</td><td>Track routes with the state attribute carrying ipsec-master-with-peer state.</td></tr><tr><td>ipsec-non-master</td><td>Track routes with the state attribute carrying ipsec-non-master state.</td></tr><tr><td>ipsec-master-without-peer</td><td>Track routes with the state attribute carrying ipsec-master-without-peer state.</td></tr></table>	Values		srrp-master	Track routes with the state attribute carrying srrp-master state	srrp-non-master	Track routes with the state attribute carrying srrp-non-master state.	ipsec-master-with-peer	Track routes with the state attribute carrying ipsec-master-with-peer state.	ipsec-non-master	Track routes with the state attribute carrying ipsec-non-master state.	ipsec-master-without-peer	Track routes with the state attribute carrying ipsec-master-without-peer state.
Values													
srrp-master	Track routes with the state attribute carrying srrp-master state												
srrp-non-master	Track routes with the state attribute carrying srrp-non-master state.												
ipsec-master-with-peer	Track routes with the state attribute carrying ipsec-master-with-peer state.												
ipsec-non-master	Track routes with the state attribute carrying ipsec-non-master state.												
ipsec-master-without-peer	Track routes with the state attribute carrying ipsec-master-without-peer state.												

tunnel-group

Syntax	tunnel-group <i>tunnel-group-id</i> sync-tag <i>tag-name</i> [create] no tunnel-group <i>tunnel-group-id</i>
Context	config>redundancy>multi-chassis>peer>sync

Description	This command enables multi-chassis synchronization of IPsec states of specified tunnel-groups with a peer. The sync-tag parameter is used to match corresponding tunnel-group on both peers. IPsec states will be synchronized between tunnel-groups with same sync-tag.
Parameters	<i>tunnel-group-id</i> — Specifies the ID of the tunnel group. <i>tag-name</i> — Specifies the name of the sync-tag.

ipsec

Syntax	[no] ipsec
Context	config>redundancy>multi-chassis>peer>sync
Description	This command enables multi-chassis synchronization of IPsec states on system level.
Default	no ipsec

4.14.2.17 Show Commands

cert-profile

Syntax	cert-profile <i>name</i> association cert-profile [<i>name</i>] cert-profile <i>name</i> entry [<i>value</i>]
Context	show>ipsec
Description	This command displays IPsec certificate profile information.
Parameters	<i>name</i> — Specifies an existing certificate profile name association — Displays information for which this IPsec certificate profile is associated <i>value</i> — Displays information for the specified entry Values 1 to 8
Output	The following is an example output of the show ipsec cert-profile command.

Sample Output

```
*A:Dut-A# show ipsec cert-profile cert "cert-1.der"
=====
Certificate Profile Entry
=====
Id Cert                               Key                               Status Flags
-----
```

```

1 cert-1.der          key-1.der
=====
*A:Dut-A#

*A:Dut-A# show ipsec cert-profile "cert-1.der" entry 1
=====
IPsec Certificate Profile: cert-1.der Entry: 1 Detail
=====
Cert File       : cert-1.der
Key File        : key-1.der
Status Flags    : (Not Specified)
Comp Chain      : complete

Compute Chain CA Profiles
-----
CA10
CA9
CA8
CA7
CA6
=====
*A:Dut-A#

```

certificate

Syntax	certificate <i>filename</i> association
Context	show show>ipsec
Description	This command displays certificate-related information.
Parameters	<i>filename</i> — Specifies the certificate file name. association — Displays information for which this IPsec certificate is associated.
Output	The following is an example output of the show certificate command.

Sample Output

```

*A:Dut-B# show certificate ca-profile
-----
Max Cert Chain Depth: 7 (default)
-----
Certificate Display Format: 1 ASCII
=====
CA Profile
=====
CA Profile      Admin Oper  Cert File      CRL File
                  State State
-----
CA0              up    up    CA1-00cert.der  CA1-00crl.der
CA1              up    up    CA1-01cert.der  CA1-01crl.der
CA2              up    up    CA1-02cert.der  CA1-02crl.der

```



```
CA3          up    up    CA1-03cert.der      CA1-03crl.der
CA4          up    up    CA1-04cert.der      CA1-04crl.der
CA5          up    up    rsa_sha512_1024_0cert.d* rsa_sha512_1024_0crl.der
CA6          up    up    rsa_sha512_1024_1cert.d* rsa_sha512_1024_1crl.der
CA7          up    up    rsa_sha512_1024_2cert.d* rsa_sha512_1024_2crl.der
CA8          up    up    rsa_sha512_1024_3cert.d* rsa_sha512_1024_3crl.der
CA9          up    up    rsa_sha512_1024_4cert.d* rsa_sha512_1024_4crl.der
CA10         up    up    rsa_sha512_1024_5cert.d* rsa_sha512_1024_5crl.der
CA11         up    up    rsa_sha384_1024_0cert.d* rsa_sha384_1024_0crl.der
CA12         up    up    rsa_sha384_1024_1cert.d* rsa_sha384_1024_1crl.der
CA13         up    up    rsa_sha384_1024_2cert.d* rsa_sha384_1024_2crl.der
CA14         up    up    rsa_sha384_1024_3cert.d* rsa_sha384_1024_3crl.der
CA15         up    up    rsa_sha384_1024_4cert.d* rsa_sha384_1024_4crl.der
CA16         up    up    rsa_sha384_1024_5cert.d* rsa_sha384_1024_5crl.der
CMPv2        up    up    rsaCMPv2cert.der    rsaCMPv2CRL.der
```

Entries found: 18

=====

* indicates that the corresponding row element may have been truncated.

*A:Dut-B#

*A:Dut-B# show ipsec certificate cert-1.der association

=====

Associated Tunnels

```
=====
```

Tunnel	SvcId	Sap	Admin
tun-1-s-cert-v2	3	tunnel-1.private:3	Up
tun-1-s-cert-MTA-v2	8	tunnel-1.private:7	Up
tun-1-s-cert-i_op-ss-v2	42	tunnel-1.private:10	Up
tun-1-s-cert-MTA-i_op-ss-v2	48	tunnel-1.private:11	Up

IPsec Tunnels: 4

=====

*A:Dut-B#

In the following example, the "cert-1.der" is the certificate-profile name, whereas above the cert-1.der is the actual file in use.

*A:Dut-B# show ipsec cert-profile association "cert-1.der"

=====

IPsec tunnels using certificate profile

```
=====
```

SvcId	Type	SAP	Tunnel
3	vprn	tunnel-1.private:3	tun-1-s-cert-v2
8	vprn	tunnel-1.private:7	tun-1-s-cert-MTA-v2
42	vprn	tunnel-1.private:10	tun-1-s-cert-i_op-ss-v2
48	vprn	tunnel-1.private:11	tun-1-s-cert-MTA-i_op-ss-v2

=====

Number of tunnel entries: 4

=====

IPsec gateways using certificate profile

```
=====
```

SvcId	Type	SAP	Gateway

```

-----
1057      vprn    tunnel-1.public:18      d-cert-MTA-g1-1-v2
1092      vprn    tunnel-1.public:21      d-cert-i_op-ss-g1-1-v2
=====
Number of gateway entries: 2
=====
*A:Dut-B#

show ipsec gateway tunnel 10.2.2.100:500
=====
IPsec Remote Users Tunnel Detail
=====
IP Addr: 10.2.2.100:500, port: 500
-----
Service Id      : 300                Sap Id          : tunnel-1.public:100
Address         : 10.2.2.100:500
Private If      : priv
Private Address : 10.20.20.50
Private Service : 400                Template Id     : 1
Replay Window   : None              Bi Direction SA : true
Host MDA        : 1/2
Match TrustAnchor: labroot
Last Oper Changed: 05/04/2016 17:36:20
IKE IDI Type    : derAsn1Dn
IKE IDI Value   : CN=Client-1
-----
Dynamic Keying Parameters
-----
Transform Id1    : 1                Transform Id2    : None
Transform Id3    : None             Transform Id4    : None
IPsec GW Name    : rw
Local GW Address : 172.16.100.1
Ike Policy Id    : 1                Ike Pol Auth     : cert
Pre Shared Key   : None
Cert Profile     : segw
Trust Anchor Prof: labroot
Selected Cert    : segw-1.cert
Selected Key     : segw-1.key
Send Chain Prof  : None
Local Id Type    : none
Client Database
    Name         : (Not Specified)
    Client ID    : None
Radius Acct Plcy : None
Radius Auth Plcy : None
TS-List         : <none>
Certificate Status Verify
-----
Primary          : crl                Secondary       : none
Default Result   : good
DHCP
-----
Admin State      : Up                Send Release    : true
Service          : 400
Gi-Address       : 10.20.20.1
Server1-Address  : 10.9.9.9
DHCPv4 Lease
-----

```

```

Private Address      : 10.20.20.50
Acquired             : 2016/05/04 17:36:19 UTC
Renew                : 2016/05/04 18:06:19 UTC
Rebind               : 2016/05/04 18:28:49 UTC
Valid Lifetime
    End              : 2016/05/04 18:36:19 UTC
    Total             : 3600 seconds
    Remaining        : 3585 seconds
Server               : 10.9.9.9
-----
ISAKMP-SA
-----
State                : Up
Established           : 05/04/2016 17:36:20   Lifetime           : 86400
Expires              : 05/05/2016 17:36:20
ISAKMP Statistics
-----
Tx Packets           : 2                      Rx Packets           : 2
Tx Errors             : 0                      Rx Errors             : 0
Tx DPD               : 0                      Rx DPD               : 0
Tx DPD ACK           : 0                      Rx DPD ACK           : 0
DPD Timeouts         : 0                      Rx DPD Errors        : 0
-----
IPsec-SA : 1, Inbound (index 2)
-----
SPI                  : 207232
Auth Algorithm        : Sha1                   Encr Algorithm        : Aes128
Installed             : 05/04/2016 17:36:20   Lifetime             : 3600
Local Traffic Selectors:
10.9.9.9-10.9.9.9
    any protocol
Remote Traffic Selectors:
10.20.20.50-10.20.20.50
    any protocol
Aggregate Statistics
-----
Bytes Processed       : 0                      Packets Processed: 0
Crypto Errors         : 0                      Replay Errors       : 0
SA Errors              : 0                      Policy Errors       : 0
-----
IPsec-SA : 1, Outbound (index 1)
-----
SPI                  : 3433111520
Auth Algorithm        : Sha1                   Encr Algorithm        : Aes128
Installed             : 05/04/2016 17:36:20   Lifetime             : 3600
Local Traffic Selectors:
10.9.9.9-10.9.9.9
    any protocol
Remote Traffic Selectors:
10.20.20.50-10.20.20.50
    any protocol
Aggregate Statistics
-----
Bytes Processed       : 0                      Packets Processed: 0
Crypto Errors         : 0                      Replay Errors       : 0
SA Errors              : 0                      Policy Errors       : 0
=====
Fragmentation Statistics
=====

```

```
Encapsulation Overhead          : 73
Pre-Encapsulation
  Fragmentation Count           : 0
  Last Fragmented Packet Size   : 0
Post-Encapsulation
  Fragmentation Count           : 0
  Last Fragmented Packet Size   : 0
=====
=====
```

client-db

Syntax **client-db**
 client-db db-name association
 client-db db-name client client-index
 client-db db-name

Context show>ipsec

Description This commands displays information for client databases. Using this command without any parameters will list all configured client database.

Parameters *db-name* — Species to list all IPsec gateways that use the specified client database.
 association — Displays information for which this client database is associated.
 client client-index — Specifies the client index or client name of client entry in the client database.

Output The following is an example output of the **show client-db** command.

Sample Output

```
show ipsec client-db
=====
IPsec Client Database
=====
Name                               Admin State   Match List
-----
test                               Up            idi peer-ip-prefix
-----
No. of entries: 1
=====
show ipsec client-db "test"
=====
IPsec Client Database "test"
=====
Description: (Not Specified)
Match List : idi peer-ip-prefix
Admin State: Up
-----
Database Client List
-----
Index      Name                               Admin State
```

```
-----
1      client-1      Up
2      client-2      Up
-----
No. of entries: 2
-----
=====
```

gateway

Syntax **gateway name** *name*
 gateway [**name** *name*] **tunnel** [**private-address-type** *private-address-type*]
 gateway [**service** *service-id*]
 gateway tunnel [*ip-address:port*]
 gateway name *name* **tunnel** *ip-address:port*
 gateway name *name* **tunnel**
 gateway [**name** *name*] **tunnel state** *state*
 gateway [**name** *name*] **tunnel idi-value** *idi-prefix*
 gateway tunnel count
 gateway tunnel [**private-address-type** *private-address-type*]

Context show>ipsec

Description This command displays IPsec gateway information.

Parameters *name* — Specifies an IPsec gateway name.

service-id — Specifies the service ID of the default security service used by the IPsec gateway.

Values 1 to 214748364
 svc-name: Up to 64 characters maximum

ip-address:port — Displays the IP address and UDP port of the SAP IPsec gateway to the tunnel.

Values 0 to 65535

state — Specifies the state of the tunnel.

Values up, down

idi-prefix — Displays a string as an IDi prefix. With this parameter, the system lists all the peers with IDi that has specified prefixes.

count — Displays the number of IPsec gateway tunnels with the **ike-policy>authmethod** command set to **psk**.

Output The following is an example output of the **show ipsec gateway** command.

Sample Output

```

show ipsec gateway tunnel 10.2.2.100:500
=====
IPsec Remote Users Tunnel Detail
=====
IP Addr: 10.2.2.100:500, port: 500
-----
Service Id      : 300                Sap Id      : tunnel-1.public:100
Address         : 10.2.2.100:500
Private If      : priv
Private Address : 10.20.20.50
Private Service : 400                Template Id   : 1
Replay Window   : None              Bi Direction SA : true
Host MDA        : 1/2
Match TrustAnchor: labroot
Last Oper Changed: 05/04/2016 17:36:20
IKE IDI Type    : derAsn1Dn
IKE IDI Value   : CN=Client-1
-----
Dynamic Keying Parameters
-----
Transform Id1   : 1                Transform Id2   : None
Transform Id3   : None            Transform Id4   : None
IPsec GW Name   : rw
Local GW Address : 172.16.100.1
Ike Policy Id   : 1                Ike Pol Auth    : cert
Pre Shared Key  : None
Cert Profile    : segw
Trust Anchor Prof: labroot
Selected Cert   : segw-1.cert
Selected Key    : segw-1.key
Send Chain Prof : None
Local Id Type   : none
Client Database
    Name        : (Not Specified)
    Client ID    : None
Radius Acct Plcy : None
Radius Auth Plcy : None
TS-List         : <none>
Certificate Status Verify
-----
Primary         : crl                Secondary      : none
Default Result  : good
DHCP
-----
Admin State     : Up                Send Release    : true
Service         : 400
Gi-Address      : 10.20.20.1
Server1-Address : 10.9.9.9
DHCPv4 Lease
-----
Private Address : 10.20.20.50
Acquired        : 2016/05/04 17:36:19 UTC
Renew           : 2016/05/04 18:06:19 UTC
Rebind          : 2016/05/04 18:28:49 UTC
Valid Lifetime
    End          : 2016/05/04 18:36:19 UTC
    Total        : 3600 seconds
    Remaining    : 3585 seconds
Server          : 10.9.9.9

```

```

-----
ISAKMP-SA
-----
State           : Up
Established      : 05/04/2016 17:36:20   Lifetime       : 86400
Expires         : 05/05/2016 17:36:20
ISAKMP Statistics
-----
Tx Packets      : 2                      Rx Packets      : 2
Tx Errors       : 0                      Rx Errors       : 0
Tx DPD          : 0                      Rx DPD          : 0
Tx DPD ACK      : 0                      Rx DPD ACK      : 0
DPD Timeouts    : 0                      Rx DPD Errors    : 0
-----
IPsec-SA : 1, Inbound (index 2)
-----
SPI             : 207232
Auth Algorithm   : Sha1                  Encr Algorithm   : Aes128
Installed        : 05/04/2016 17:36:20   Lifetime        : 3600
Local Traffic Selectors:
10.9.9.9-10.9.9.9
    any protocol
Remote Traffic Selectors:
10.20.20.50-10.20.20.50
    any protocol
Aggregate Statistics
-----
Bytes Processed : 0                      Packets Processed: 0
Crypto Errors    : 0                      Replay Errors     : 0
SA Errors        : 0                      Policy Errors     : 0
-----
IPsec-SA : 1, Outbound (index 1)
-----
SPI             : 3433111520
Auth Algorithm   : Sha1                  Encr Algorithm   : Aes128
Installed        : 05/04/2016 17:36:20   Lifetime        : 3600
Local Traffic Selectors:
10.9.9.9-10.9.9.9
    any protocol
Remote Traffic Selectors:
10.20.20.50-10.20.20.50
    any protocol
Aggregate Statistics
-----
Bytes Processed : 0                      Packets Processed: 0
Crypto Errors    : 0                      Replay Errors     : 0
SA Errors        : 0                      Policy Errors     : 0
=====
Fragmentation Statistics
=====
Encapsulation Overhead           : 73
Pre-Encapsulation
    Fragmentation Count           : 0
    Last Fragmented Packet Size    : 0
Post-Encapsulation
    Fragmentation Count           : 0
    Last Fragmented Packet Size    : 0
=====

```

```

A:vsim-2# show ipsec gateway name "rw" tunnel 10.1.1.100
=====
IPsec Remote Users Tunnel Detail
=====
-----
IP Addr: 10.1.1.100, port: 500
-----
Service Id      : 300                Sap Id          : tunnel-1.public:100
Address         : 10.1.1.100
Private If      : priv
Private Address : 10.20.20.50
Private Service : 400                Template Id     : 1
Replay Window   : None              Bi Direction SA : true
Host MDA        : 1/2
Match TrustAnchor: labroot
Last Oper Changed: 12/14/2016 22:17:05
IKE IDI Type    : derAsn1Dn
IKE IDI Value   : CN=Client-1
TS List         : <none>
Pre-Shared Key  : <none>
IKE Policy      : (Not Specified)
TCP MSS
  Public        : N/A
  Private       : 1200 octets
-----
Dynamic Keying Parameters
-----
Transform Id1   : 1                Transform Id2    : None
Transform Id3   : None            Transform Id4    : None
IPsec GW Name   : rw
Local GW Address : 172.16.100.1
Ike Policy Id   : 1                Ike Pol Auth     : cert
Cert Profile    : segw
Trust Anchor Prof: labroot
Selected Cert   : segw-1.cert
Selected Key    : segw-1.key
Send Chain Prof : None
Local Id Type   : none
Client Database
  Client Index  : None
Radius Acct Plcy : None
Radius Auth Plcy : None
Certificate Status Verify
-----
Primary         : crl                Secondary        : none
Default Result  : good
-----
DHCP
-----
Admin State     : Up                Send Release     : true
Service         : 400
Gi-Address      : 10.20.20.1
Server1-Address : 10.9.9.9
DHCPv4 Lease
-----
Private Address : 10.20.20.50
Acquired        : 2016/12/14 22:17:04 UTC
Renew           : 2016/12/14 22:47:04 UTC
Rebind          : 2016/12/14 23:09:34 UTC

```



```

Valid Lifetime
  End      : 2016/12/14 23:17:04 UTC
  Total    : 3600 seconds
  Remaining : 3580 seconds
Server     : 10.9.9.9
-----
ISAKMP-SA
-----
State      : Up
Established : 12/14/2016 22:17:04   Lifetime      : 86400
Expires    : 12/15/2016 22:17:04
ISAKMP Statistics
-----
Tx Packets      : 2                Rx Packets      : 2
Tx Errors       : 0                Rx Errors       : 0
Tx DPD          : 0                Rx DPD          : 0
Tx DPD ACK      : 0                Rx DPD ACK      : 0
DPD Timeouts    : 0                Rx DPD Errors    : 0
-----
IPsec-SA : 1, Inbound (index 2)
-----
SPI          : 322790
Auth Algorithm : Sha1              Encr Algorithm   : Aes128
Installed    : 12/14/2016 22:17:05 Lifetime         : 3600
Local Traffic Selectors:
172.16.100.1-172.16.100.1
    any protocol
Remote Traffic Selectors:
10.20.20.50-10.20.20.50
    any protocol
Aggregate Statistics
-----
Bytes Processed : 0                Packets Processed: 0
Crypto Errors   : 0                Replay Errors     : 0
SA Errors       : 0                Policy Errors     : 0
-----
IPsec-SA : 1, Outbound (index 1)
-----
SPI          : 3462984686
Auth Algorithm : Sha1              Encr Algorithm   : Aes128
Installed    : 12/14/2016 22:17:05 Lifetime         : 3600
Local Traffic Selectors:
172.16.100.1-172.16.100.1
    any protocol
Remote Traffic Selectors:
10.20.20.50-10.20.20.50
    any protocol
Aggregate Statistics
-----
Bytes Processed : 0                Packets Processed: 0
Crypto Errors   : 0                Replay Errors     : 0
SA Errors       : 0                Policy Errors     : 0
=====
Fragmentation Statistics
=====
Encapsulation Overhead      : 73
Pre-Encapsulation
  Fragmentation Count       : 0
  Last Fragmented Packet Size : 0

```

```

Post-Encapsulation
  Fragmentation Count          : 0
  Last Fragmented Packet Size : 0
=====
=====

```

tunnel

- Syntax** `tunnel [gre-tunnel-name]`
- Context** `show>gre`
- Description** This command displays information about a particular GRE tunnel or all GRE tunnels.
- Parameters** *gre-tunnel-name* — Specifies the name of a GRE tunnel.
- Output** [Table 28](#) lists the information displayed for each GRE tunnel.

Table 28 Show GRE Tunnel Output Fields

Label	Description
TunnelName (Tunnel Name)	The name of the GRE tunnel.
SvcID (Service ID)	The service ID of the IES or VPRN service that owns the GRE tunnel.
SapId (Sap ID)	The ID of the private tunnel SAP that owns the GRE tunnel.
Description	The description for the GRE tunnel.
LocalAddress (Source Address)	The source address of the GRE tunnel (public/outer IP)
RemoteAddress (Remote Address)	The destination address of the GRE tunnel (public/outer IP)
Bkup RemAddr (Backup Address)	The backup destination address of the GRE tunnel (public/outer IP)
To (Target Address)	The remote address of the GRE tunnel (private/inner IP). This is the peer's IP address to the GRE tunnel. This comes from the tunnel configuration.
DlvrySvcId (Delivery Service)	The service ID of the IES or VPRN service that handles the GRE encapsulated packets belonging to the tunnel.
DSCP	The forced DSCP code point in the outer IP header of GRE encapsulated packets belonging to the tunnel.
Admn (Admin State)	Admin state of the tunnel (up/down).

Table 28 Show GRE Tunnel Output Fields (Continued)

Label	Description
Oper (Operational State)	Operational state of the tunnel (up/down).
Oper Rem Addr (Oper Remote Addr)	The destination address of the GRE tunnel (public/outer IP) that is currently being used.
Pkts Rx	Number of GRE packets received belonging to the tunnel.
Pkts Tx	Number of GRE packets transmitted belonging to the tunnel.
Bytes Rx	Number of bytes in received GRE packets associated with the tunnel.
Bytes Tx	Number of bytes in transmitted GRE packets associated with the tunnel.
Key Ignored Rx	Incremented every time a GRE packet is received with a GRE key field.
Too Big Tx	Incremented every time an IP packet with DF=1 is to be forwarded into the GRE tunnel and its size exceeds the interface IP MTU.
Seq Ignored Rx	Incremented every time a GRE packet is received with a sequence number.
Vers Unsup. Rx	Incremented every time a GRE packet is dropped because the GRE version is unsupported.
Invalid Chksum Rx	Incremented every time a GRE packet is dropped because the checksum is invalid.
Loops Rx	Incremented every time a GRE packet is dropped because the destination IP address of the un-encapsulated packet would cause it be re-encapsulated into the same tunnel.

Sample Output

```
dut-A# show gre tunnel
=====
GRE Tunnels
=====
TunnelName      LocalAddress  SvcId  Admn
SapId           RemoteAddress DlvrySvcId Oper
To             Bkup RemAddr  DSCP   Oper Rem Addr
-----
toce2           10.1.1.7     500    Up
  tunnel-1.private:1  10.1.1.3     500    Up
    20.1.1.2        10.1.2.7     None   10.1.1.3
toce2_backup    10.1.2.3     502    Up
  tunnel-1.private:3  10.1.1.3     502    Up
```

```

10.1.2.2          10.0.0.0          None          10.1.1.3
-----
GRE Tunnels: 2
=====

A:Dut-A# show gre tunnel "toce2"
=====
GRE Tunnel Configuration Detail
=====
Service Id       : 500                Sap Id          : tunnel-1.private:1
Tunnel Name      : toce2
Description      : None
Target Address   : 10.1.1.2           Delivery Service : 500
Admin State      : Up                 Oper State      : Up
Source Address   : 10.1.1.7           Oper Remote Addr : 10.1.1.3
Remote Address   : 10.1.1.3           Backup Address  : 10.1.2.7
DSCP             : None
Oper Flags       : None

=====
GRE Tunnel Statistics: toce2
=====
Errors Rx        : 0                  Errors Tx        : 0
Pkts Rx          : 165342804          Pkts Tx          : 605753463
Bytes Rx         : 84986201256        Bytes Tx         : 296819196870
Key Ignored Rx   : 0                  Too Big Tx       : 0
Seq Ignored Rx   : 0
Vers Unsup. Rx   : 0
Invalid Chksum Rx : 0
Loops Rx         : 0

=====
=====

```

ike-policy

Syntax	ike-policy <i>ike-policy-id</i> ike-policy
Context	show>ipsec
Description	This command displays
Parameters	<i>ike-policy-id</i> — Specifies the ID of an IKE policy entry. Values 1 to 2048
Output	The following is an example output for the show ipsec ike-policy command.

Sample Output

```

*A:ALA-48# show ipsec ike-policy 10
=====
IPsec IKE policy Configuration Detail
=====

```

```

Policy Id      : 10
DH Group       : Group2
PFS            : False
Auth Algorithm : Sha1
ISAKMP Lifetime : 86400
NAT Traversal  : Disabled
NAT-T Keep Alive : 0
DPD            : Disabled
DPD Interval   : 30
Description    : (Not Specified)
IKE Mode       : main
Auth Method    : psk
PFS DH Group   : Group2
Encr Algorithm : Aes128
IPsec Lifetime : 3600
Behind NAT Only : True
DPD Max Retries : 3
=====
*A:ALA-48#

```

ike-transform

Syntax	ike-transform [<i>ike-transform-id</i>]
Context	show>ipsec
Description	This command displays information for the specified IKE transform instance. Information for all IKE transform instances is displayed when an <i>ike-transform-id</i> is not specified.
Parameters	<i>ike-transform-id</i> — Specifies an existing IKE transform instance
Values	1 to 4096
Output	The following output is an example of IKE transform information.

Sample Output

```

Node# show ipsec ike-transform
=====
IKE Transforms
=====
ID      Diffie-Hellman  Authentication  Encryption  ISAKMP
      Group          Algorithm      Algorithm    Lifetime
-----
100     14                sha1           aes128       86400
-----
No. of IKE Transforms: 1
=====

```

lockout

Syntax	lockout router <i>router-id</i> local-gateway-address <i>local-gateway-address</i> mda <i>mda</i> lockout router <i>router-id</i> local-gateway-address <i>local-gateway-address</i> remote <i>ip-address[:port]</i> lockout router <i>router-id</i> mda <i>mda</i>
Context	show>ipsec

- Description** This command displays the lockout status for the specified IPsec clients. If remote address information is not specified, the system will display a list of clients that have been locked out on the specified ISA, along with the IPsec gateway if *local-gateway-address* is specified.
- Parameters**
- router-id* — Specifies the ID of the router where the IPsec gateway is configured
 - local-gateway-address* — Specifies the IP address of the local IPsec gateway
 - mda* — Specifies the MDA ID of the ISA
 - ip-address* — Specifies the IP address of the remote client
 - port* — Specifies the port of the remote client
- Output** The following output is an example of lockout information.

Sample Output

```
show ipsec lockout router 300 local-gateway-address 172.16.100.1 remote
192.168.61.100:500
=====
IPsec Lockout Client
=====
Lockout           : True
Router ID         : 300
Local Gateway Address : 172.16.100.1
Lockout Client Address: 192.168.61.100
Lockout Client Port   : 500
No. of Failed Attempts: 2
No. of Dropped Packets: 2
Remaining Block Time  : 289 seconds
=====
```

radius-accounting-policy

- Syntax** **radius-accounting-policy** [*name*]
- Context** show>ipsec
- Description** This command displays RADIUS accounting-policy related information.
- Parameters** *name* — Specifies an existing RADIUS accounting policy.
- Output** The following is an example output for the **show ipsec radius-accounting-policy** command.

Sample Output

```
show ipsec radius-accounting-policy
=====
Radius Accounting Policy
=====
Policy Name          Server Policy          Include Attribs      Upd Int
                                                                Jitter
```

```
-----
rad-acct-policy-1                               nasId nasPortId   20
                                                framedIpAddr
                                                10
=====
Number of entries: 1
=====

show ipsec radius-accounting-policy "rad-acct-policy-1"
=====
IPsec Radius Accounting Policy Detail
=====
Name           : rad-acct-policy-1
Server Policy  : (Not Specified)
Include Attr   : nasId nasPortId framedIpAddr
Update Interval : 20
Jitter         : 10 sec.
=====
```

radius-authentication-policy

Syntax	radius-authentication-policy [<i>name</i>]
Context	show>ipsec
Description	This command displays IPsec RADIUS authentication policy information.
Parameters	<i>name</i> — Specifies an existing RADIUS authentication policy.

security-policy

Syntax	security-policy service <i>service-id</i> [security-policy-id <i>security-policy-id</i>] security-policy
Context	show>ipsec
Description	This command displays
Parameters	<i>service-id</i> — Specifies the service-id of the tunnel delivery service. Values 1 to 214748364 svc-name: 64 char max <i>security-policy-id</i> — Specifies the IPsec security policy entry that this tunnel will use. Values 1 to 8192
Output	The following is an example output for the show ipsec security-policy command.

Sample Output

```
*A:ALA-48>show>ipsec# security-policy 1
=====
Security Policy Param Entries
=====
SvcId      Security  Policy    LocalIp      RemoteIp
      PlcyId    ParamsId
-----
1           1         1         0.0.0.0/0    0.0.0.0/0
-----
No. of IPsec Security Policy Param Entries: 1
=====
*A:ALA-48>show>ipsec#
```

service

- Syntax** **service** *service-id*
- Context** show>ipsec
- Description** This command displays service specific IPsec configuration.
- Parameters** *service-id* — The VPRN service ID or service name.

Values *service-id*: 1 to 2147483647
svc-name: up to 64 characters maximum
- Output** The following is an example output for the **service** command.

Sample Output

```
SHOW>IPSEC# SERVICE 400
=====
SERVICE-SPECIFIC IPSEC CONFIGURATIONS
=====
REVERSE ROUTE OVERRIDE: ENABLED
=====
```

static-sa

- Syntax** **static-sa**
static-sa name *sa-name*
static-sa spi *spi*
- Context** show>ipsec
- Description** This command displays IPsec static-SA information.
- Parameters** *sa-name* — Specifies the SA name.

Values 32 chars max

spi — Specifies the spi.

Values 256..16383

transform

Syntax **transform** [*transform-id*]

Context show>ipsec

Description This command displays information of the specified IPsec transform or lists all configured IKE transform information when the IKE transform ID is not specified.

Parameters *transform-id* — Specifies an IPsec transform entry.

Values 1 to 2048

Output The following is an example output for the **show ipsec transform** command.

Sample Output

```

NODE# show ipsec transform
=====
IPSEC TRANSFORMS
=====
TRANSFORMID      ESPAUTH      ESPENCRYPTION  PFS          IPSEC
                  ALGORITHM    ALGORITHM      DH GROUP     LIFETIME (SEC)
-----
1                 SHA256       AES128         INHERIT      INHERIT
10                SHA256       AES256         14           20000
99                SHA1         AES192         15           30000
100               SHA1         AES128         INHERIT      INHERIT
-----
NO. OF IPSEC TRANSFORMS: 4
=====
```

trust-anchor-profile

Syntax **trust-anchor-profile** [*trust-anchor-profile*] **association**
trust-anchor-profile [*trust-anchor-profile*]

Context show>ipsec

Description This command displays trust anchor profile information.

Parameters *trust-anchor-profile* — Specifies the trust anchor profile name up to 32 characters in length.

association — Displays information for which this trust anchor profile is associated.

Output The following is an example output for the **show ipsec trust-anchor-profile** command.

Sample Output

```
*A:Dut-A# show ipsec trust-anchor-profile
=====
Trust Anchor Profile Information
=====
Name                               CA Profiles Down
-----
CA0wCMPv2                          0
CA1wCMPv2                          0
CA2wCMPv2                          0
CA3wCMPv2                          0
CA4wCMPv2                          0
CA5wCMPv2                          0
CA6wCMPv2                          0
CA7wCMPv2                          0
CA8wCMPv2                          0
CA9wCMPv2                          0
CA10wCMPv2                         0
=====
*A:Dut-A#

*A:Dut-A# show ipsec trust-anchor-profile
=====
Trust Anchor CA-profile List
=====
CA Profile                         Admin/Oper State
-----
CA6                               up/up
CMPv2                             up/up
=====
*A:Dut-A#
```

ts-list

- Syntax** **ts-list** [*list-name*]
 ts-list *list-name* **association**
 ts-list *list-name* **local-entry** [1 to 32]
 ts-list *list-name* **remote-entry** [1 to 32]
 ts-list *list-name* {**local** | **remote**}

Context show>ipsec

Description This command displays IPsec traffic-selector list (TS-list) information.

 Entering this command without a parameter will list all configured TS-lists.

 Entering this command with the **association** parameter will list all IPsec gateways that use the specified TS-list.

 Entering this command with the **local** or **local-entry** parameter will list all or specified local entries of the specified TS-list.

Entering this command with the **remote** or **remote-entry** parameter will list all or specified remote entries of the specified TS-list.

Parameters

- list-name* — The traffic-selector list name
- association** — Displays all associations of the TS-list
- local-entry [1 to 32]** — The entry ID of a local entry
- remote-entry [1 to 32]** — The entry ID of a remote entry
- local** — Displays all local entries
- remote** — Displays all remote entries

Output The following output is an example of TS-list information.

Sample Output

```
show ipsec ts-list
=====
Traffic Selector List
=====
TS-List
-----
fullts
=====
*A:vsim-02-cpm# show ipsec ts-list "fullts"
=====
TS-List "fullts" Local Entries Information
=====
Entry ID      : 1
Status        : Invalid
Protocol ID   : Not Specified
Protocol Port Range: Not Specified
Prefix/Len    : 10.10.10.1/32
-----
Entry ID      : 2
Status        : Valid
Protocol ID   : tcp
Protocol Port Range: 80 - 80
Prefix/Len    : 10.10.10.2/32
-----
No. of entries: 2
=====
TS-List "fullts" Remote Entries Information
=====
Entry ID      : 1
Status        : Valid
Protocol ID   : tcp
Protocol Port Range: any
Prefix/Len    : 0.0.0.0/0
-----
No. of entries: 1
=====
```

tunnel

Syntax	tunnel <i>ipsec-tunnel-name</i> tunnel tunnel count tunnel state <i>state</i>
Context	show>ipsec
Description	This command displays IPsec tunnel information.
Parameters	<i>ipsec-tunnel-name</i> — Specifies the name of the tunnel up to 32 characters. <i>state</i> — Specifies one of up, down, or limited

tunnel-template

Syntax	tunnel-template [<i>ipsec-template-identifier</i>] tunnel-template <i>ipsec-template-identifier</i> association [all]
Context	show>ipsec
Description	This command displays IPsec tunnel template information.
Parameters	<i>ipsec template identifier</i> — Displays an existing IPsec tunnel template ID. Values 1 to 2048
Output	The following is an example output for the show ipsec tunnel-template command.

Sample Output

```
*A:ALA-48>config>ipsec# show ipsec tunnel-template 1
=====
IPsec Tunnel Template
=====
Id      Trnsfrm1  Trnsfrm2  Trnsfrm3  Trnsfrm4  ReverseRoute  ReplayWnd
-----
1       1         none     none     none     useSecurityPolicy 128
-----
Number of templates: 1
=====
*A:ALA-48>config>ipsec#
```

mc-ipsec

Syntax	mc-ipsec peer <i>ip-address</i> tunnel-group <i>tunnel-group-id</i> mc-ipsec peer <i>ip-address</i>
Context	show>redundancy>multi-chassis

- Description** This command displays the 7750 SR IPsec multi-chassis states. Optionally, only state of specified tunnel-group will be displayed.
- Parameters** *ip-address* — Specifies the peer address.
tunnel-group-id — Specifies the tunnel-group.
- Output** [Table 29](#) describes show **redundancy multi-chassis mc-ipsec** output fields.

Table 29 Show MC-IPsec Peer Output Fields

Label	Description
Admin State	Displays the admin state of mc-ipsec.
Mastership/Master State	Displays the current MIMP state.
Protection Status	Displays nominal or notReady . notReady means the system is not ready for a switchover. There could be major traffic impact if switchover happens in case of notReady. nominal means the tunnel-group is in a better situation to switchover than notReady. However there still might be traffic impact.
Installed	Displays the number of tunnels that has been successfully installed on MS-ISA
Installing	Displays the number of tunnels that are being installed on MS-ISA.
Awaiting Config	Displays the number of synced tunnels that do not have corresponding configuration ready
Failed	Displays the number of tunnels that have been failed to installed on MS-ISA.

Sample Output

```
show redundancy multi-chassis mc-ipsec peer 10.2.2.2
=====
Multi-Chassis MC-IPsec
=====
Peer Name       : (Not Specified)
Peer Addr       : 10.2.2.2
Keep Alive Intvl: 1.0 secs           Hold on Nbr Fail      : 3
Discovery Intvl : 300 secs           Discovery Boot Intvl  : 300 secs
BFD             : Disable
Last update     : 09/27/2012 00:44:23

=====
Multi-Chassis IPsec Multi Active Tunnel-Group Table
```

```
=====
ID           Peer Group      Priority  Admin State  Mastership
-----
1            2              100      Up           standby
-----
Multi Active Tunnel Group Entries found: 1
=====

show redundancy multi-chassis mc-ipsec peer 10.2.2.2 tunnel-group 1
=====
Multi-Chassis MC-IPsec Multi Active Tunnel-Group: 1
=====
Peer Ex Tnl Grp : 2              Priority           : 100
Master State    : standby        Protection Status  : nominal
Admin State     : Up             Oper State        : Up
=====
Multi-Chassis Tunnel Statistics
=====
                                Static           Dynamic
-----
Installed                1                0
Installing                0                0
Awaiting Config           0                0
Failed                    0                0
=====
```

statistics

Syntax	statistics
Context	show>isa
Description	This command enables the context to display ISA statistical information.

ip-tunnel-stats

Syntax	ip-tunnel-stats
Context	show>isa>stats
Description	This command enables the context to display IP tunnel statistical information. This includes statistics for non-IPsec tunnels supported on tunnel ISAs.

number-of-tunnels

Syntax	number-of-tunnels tunnel-type <i>tunnel-type</i> isa <i>mda</i> number-of-tunnels tunnel-type <i>tunnel-type</i> system number-of-tunnels tunnel-type <i>tunnel-type</i> tunnel-group <i>tunnel-group-id</i>
Context	show>isa>stats>ip-tunnel-stats
Description	This command displays the number of tunnels that are operationally up for the specified tunnel and scope. The following scope types are supported: • per ISA • per tunnel group • per system Note that L2TPv2 does not have a per-ISA scope. The system collects statistics every hour for the past 24 hours per wall clock. A current value is also included in the output.
Parameters	<i>tunnel-type</i> — Displays information about the tunnel type. Values gre, ip-in-ip, l2tpv3 <i>mda</i> — Displays information about the ISA ID. Values slot/mda system — Displays information about the system.

tunnel-group-id — Displays information about the tunnel group ID.

Values 1 to 16

throughput

Syntax **throughput** **tunnel-type** *tunnel-type* **system** [**history-stats-in-count** *count*] [**history-stats-in-min** *minutes*] [**current**]
throughput **tunnel-type** *tunnel-type* **type type** **system** [**history-stats-in-count** *count*] [**history-stats-in-min** *minutes*] [**current**] [**show-oid**]
throughput **tunnel-type** *tunnel-type* **isa mda** [**history-stats-in-count** *count*] [**history-stats-in-min** *minutes*] [**current**]
throughput **tunnel-type** *tunnel-type* **type type** **isa mda** [**history-stats-in-count** *count*] [**history-stats-in-min** *minutes*] [**current**] [**show-oid**]
throughput **tunnel-type** *tunnel-type* **tunnel-group** *tunnel-group-id* [**history-stats-in-count** *count*] [**history-stats-in-min** *minutes*] [**current**]
throughput **tunnel-type** *tunnel-type* **type type** **tunnel-group** *tunnel-group-id* [**history-stats-in-count** *count*] [**history-stats-in-min** *minutes*] [**current**] [**show-oid**]

Context show>isa>stats>ip-tunnel-stats

Description This command displays throughput statistics for the specified tunnel types and scope.

The following scopes are supported:

- per ISA
- per tunnel group
- per system

The statistics include the following information:

- total packet per second (encapsulated and decapsulated)
- encapsulated packets per second
- decapsulated packets per second
- total bits per second (encapsulated and decapsulated) in Mibits/s
- encapsulated bits per second in Mibits/s
- decapsulated bits per second in Mibits/s

Syntax notes:

- 1 Mibits/s equals 2²⁰ bit/s
- The bits per second counter is an integer which is a rounded down value from the measured value.

The system collects stats every 10 minutes for last the 24 hour per the wall clock. A current value is also included in the output. The value is an average derived value of 10 minutes. The start time indicates the starting timestamp of measurement. The sampling duration indicates the duration of measurement.

Parameters *tunnel-type* — Displays the type of tunnel.

Values gre, ip-in-ip, l2tpv3

mda — Displays the ISA ID.

Values slot/mda

tunnel-group-id — Displays the ID of the tunnel group.

Values 1 to 16

type — Displays the type of breakdown counter.

Values bidir-pps, bidir-bps, encap-pps, encap-bps, decap-pps, decap-bps

count — Displays the number historical values to be included in the output.

Values 1 to 24

minutes — Displays the number of minutes of historical values to be included in output.

Values 1 to 1440

current — Displays only the current values.

show-oid — Specifies to include the SNMP object identifier (OID) and the instance ID for the latest historical value in the output.

Output The following is an example output of the **show isa statistics throughput ip-tunnel-stats** command.

Sample Output

```
show>isa>stats>ip-tunnel-stats# throughput tunnel-type gre tunnel-group 1
=====
STATISTICS FOR ISA TUNNEL GROUP 1
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
ENCAPSULATED GRE TUNNEL THROUGHPUT (PKTS/SEC)
1 (CURRENT)    62              2017/05/22 21:50:00 MIN 6 SEC 24
2              62              2017/05/22 21:40:00 MIN 10
3              62              2017/05/22 21:30:00 MIN 10
4              62              2017/05/22 21:20:00 MIN 10
5              62              2017/05/22 21:10:00 MIN 10
6              87              2017/05/22 21:00:00 MIN 10
7              18              2017/05/22 20:50:00 MIN 10
8              0              2017/05/22 20:40:00 MIN 10
9              0              2017/05/22 20:30:00 MIN 10
10             0              2017/05/22 20:20:00 MIN 10
11             0              2017/05/22 20:10:00 MIN 10
12             0              2017/05/22 20:00:00 MIN 10
13             0              2017/05/22 19:50:00 MIN 10
```

14	0	2017/05/22 19:40:00 MIN 10
15	0	2017/05/22 19:30:00 MIN 10
16	0	2017/05/22 19:20:00 MIN 10
17	0	2017/05/22 19:10:00 MIN 10
18	0	2017/05/22 19:00:00 MIN 10
19	0	2017/05/22 18:50:00 MIN 10
20	0	2017/05/22 18:40:00 MIN 10
21	0	2017/05/22 18:30:00 MIN 10
22	0	2017/05/22 18:20:00 MIN 10
23	0	2017/05/22 18:10:00 MIN 10
24	0	2017/05/22 18:00:00 MIN 10
25	0	2017/05/22 17:50:00 MIN 10
26	0	2017/05/22 17:45:12 MIN 4 SEC 49
DECAPSULATED GRE TUNNEL THROUGHPUT (PKTS/SEC)		
1 (CURRENT)	249	2017/05/22 21:50:00 MIN 6 SEC 24
2	249	2017/05/22 21:40:00 MIN 10
3	249	2017/05/22 21:30:00 MIN 10
4	249	2017/05/22 21:20:00 MIN 10
5	249	2017/05/22 21:10:00 MIN 10
6	145	2017/05/22 21:00:00 MIN 10
7	18	2017/05/22 20:50:00 MIN 10
8	0	2017/05/22 20:40:00 MIN 10
9	0	2017/05/22 20:30:00 MIN 10
10	0	2017/05/22 20:20:00 MIN 10
11	0	2017/05/22 20:10:00 MIN 10
12	0	2017/05/22 20:00:00 MIN 10
13	0	2017/05/22 19:50:00 MIN 10
14	0	2017/05/22 19:40:00 MIN 10
15	0	2017/05/22 19:30:00 MIN 10
16	0	2017/05/22 19:20:00 MIN 10
17	0	2017/05/22 19:10:00 MIN 10
18	0	2017/05/22 19:00:00 MIN 10
19	0	2017/05/22 18:50:00 MIN 10
20	0	2017/05/22 18:40:00 MIN 10
21	0	2017/05/22 18:30:00 MIN 10
22	0	2017/05/22 18:20:00 MIN 10
23	0	2017/05/22 18:10:00 MIN 10
24	0	2017/05/22 18:00:00 MIN 10
25	0	2017/05/22 17:50:00 MIN 10
26	0	2017/05/22 17:45:12 MIN 4 SEC 49
ENCAPSULATED AND DECAPSULATED GRE TUNNEL THROUGHPUT (PKTS/SEC)		
1 (CURRENT)	312	2017/05/22 21:50:00 MIN 6 SEC 24
2	311	2017/05/22 21:40:00 MIN 10
3	311	2017/05/22 21:30:00 MIN 10
4	311	2017/05/22 21:20:00 MIN 10
5	311	2017/05/22 21:10:00 MIN 10
6	233	2017/05/22 21:00:00 MIN 10
7	37	2017/05/22 20:50:00 MIN 10
8	0	2017/05/22 20:40:00 MIN 10
9	0	2017/05/22 20:30:00 MIN 10
10	0	2017/05/22 20:20:00 MIN 10
11	0	2017/05/22 20:10:00 MIN 10
12	0	2017/05/22 20:00:00 MIN 10
13	0	2017/05/22 19:50:00 MIN 10
14	0	2017/05/22 19:40:00 MIN 10
15	0	2017/05/22 19:30:00 MIN 10
16	0	2017/05/22 19:20:00 MIN 10
17	0	2017/05/22 19:10:00 MIN 10
18	0	2017/05/22 19:00:00 MIN 10

19	0	2017/05/22 18:50:00 MIN 10
4	2	2017/05/22 21:20:00 MIN 10
5	2	2017/05/22 21:10:00 MIN 10
6	0	2017/05/22 21:00:00 MIN 10
7	0	2017/05/22 20:50:00 MIN 10
8	0	2017/05/22 20:40:00 MIN 10
9	0	2017/05/22 20:30:00 MIN 10
10	0	2017/05/22 20:20:00 MIN 10
11	0	2017/05/22 20:10:00 MIN 10
12	0	2017/05/22 20:00:00 MIN 10
13	0	2017/05/22 19:50:00 MIN 10
14	0	2017/05/22 19:40:00 MIN 10
15	0	2017/05/22 19:30:00 MIN 10
16	0	2017/05/22 19:20:00 MIN 10
17	0	2017/05/22 19:10:00 MIN 10
18	0	2017/05/22 19:00:00 MIN 10
19	0	2017/05/22 18:50:00 MIN 10
20	0	2017/05/22 18:40:00 MIN 10
21	0	2017/05/22 18:30:00 MIN 10
22	0	2017/05/22 18:20:00 MIN 10
23	0	2017/05/22 18:10:00 MIN 10
24	0	2017/05/22 18:00:00 MIN 10
25	0	2017/05/22 17:50:00 MIN 10
26	0	2017/05/22 17:45:12 MIN 4 SEC 49
DECAPSULATED GRE TUNNEL THROUGHPUT (MIBIT/SEC)		
1 (CURRENT)	2	2017/05/22 21:50:00 MIN 6 SEC 24
2	2	2017/05/22 21:40:00 MIN 10
3	2	2017/05/22 21:30:00 MIN 10
4	2	2017/05/22 21:20:00 MIN 10
5	2	2017/05/22 21:10:00 MIN 10
6	0	2017/05/22 21:00:00 MIN 10
7	0	2017/05/22 20:50:00 MIN 10
8	0	2017/05/22 20:40:00 MIN 10
9	0	2017/05/22 20:30:00 MIN 10
10	0	2017/05/22 20:20:00 MIN 10
11	0	2017/05/22 20:10:00 MIN 10
12	0	2017/05/22 20:00:00 MIN 10
13	0	2017/05/22 19:50:00 MIN 10
14	0	2017/05/22 19:40:00 MIN 10
15	0	2017/05/22 19:30:00 MIN 10
16	0	2017/05/22 19:20:00 MIN 10
17	0	2017/05/22 19:10:00 MIN 10
18	0	2017/05/22 19:00:00 MIN 10
19	0	2017/05/22 18:50:00 MIN 10
20	0	2017/05/22 18:40:00 MIN 10
21	0	2017/05/22 18:30:00 MIN 10
22	0	2017/05/22 18:20:00 MIN 10
23	0	2017/05/22 18:10:00 MIN 10
24	0	2017/05/22 18:00:00 MIN 10
25	0	2017/05/22 17:50:00 MIN 10
26	0	2017/05/22 17:45:12 MIN 4 SEC 49
ENCAPSULATED AND DECAPSULATED GRE TUNNEL THROUGHPUT (MIBIT/SEC)		
1 (CURRENT)	4	2017/05/22 21:50:00 MIN 6 SEC 24
2	4	2017/05/22 21:40:00 MIN 10
3	4	2017/05/22 21:30:00 MIN 10
4	4	2017/05/22 21:20:00 MIN 10
5	4	2017/05/
22	21:10:00 MIN 10	

```

6          1          2017/05/22 21:00:00 MIN 10
7          0          2017/05/22 20:50:00 MIN 10
8          0          2017/05/22 20:40:00 MIN 10
9          0          2017/05/22 20:30:00 MIN 10
10         0          2017/05/22 20:20:00 MIN 10
11         0          2017/05/22 20:10:00 MIN 10
12         0          2017/05/22 20:00:00 MIN 10
13         0          2017/05/22 19:50:00 MIN 10
14         0          2017/05/22 19:40:00 MIN 10
15         0          2017/05/22 19:30:00 MIN 10
16         0          2017/05/22 19:20:00 MIN 10
17         0          2017/05/22 19:10:00 MIN 10
18         0          2017/05/22 19:00:00 MIN 10
19         0          2017/05/22 18:50:00 MIN 10
20         0          2017/05/22 18:40:00 MIN 10
21         0          2017/05/22 18:30:00 MIN 10
22         0          2017/05/22 18:20:00 MIN 10
23         0          2017/05/22 18:10:00 MIN 10
24         0          2017/05/22 18:00:00 MIN 10
25         0          2017/05/22 17:50:00 MIN 10
26         0          2017/05/22 17:45:12 MIN 4 SEC 49
-----

```

NO. OF ENTRIES: 156

=====

traffic-forward

Syntax `traffic-forward tunnel-type tunnel-type [type type] isa mda`

Context `show>isa>stats>ip-tunnel-stats`

Description This command displays traffic forward statistics for the specified tunnel-type on the specified ISA.

The statistics includes the following information:

- The number of bidirectional (encapsulated and decapsulated) packets
- The number of encapsulated packets
- The number of decapsulated packets
- The number of bidirectional (encapsulated and decapsulated) kilobytes
- The number of kilobytes for encapsulated traffic
- The number of kilobytes for decapsulated traffic

In the output, 1 kilobyte equals 210 bytes.

Parameters *tunnel-type* — Displays the type of the tunnel.

Values gre, ip-in-ip, l2tpv3

mda — Displays the ISA ID.

Values slot/mda

type — Displays the type of breakdown counter.

Values *bidir-pkts, bidir-kbs, encap-pkts, encap-kbs, decap-pkts, decap-kbs*

Output The following is an example output of the **show router statistics ip-tunnel-stats traffic-forward** command.

Output Sample

```
show>isa>stats>ip-tunnel-stats# traffic-forward tunnel-type gre isa 1/2
=====
STATISTICS FOR ISA 1/2
=====
INDEX          VALUE                               START TIME          SAMPLING DURATION
-----
NUMBER OF ENCAPED GRE TUNNEL PACKETS
1 (CURRENT)    367,474                               2017/05/22 17:45:12 HRS 4 MIN 45 SEC 46
NUMBER OF DECAPED GRE TUNNEL PACKETS
                                           [0/1874]
1 (CURRENT)    1,310,402                             2017/05/22 17:45:12 HRS 4 MIN 45 SEC 46
NUMBER OF ENCAPED AND DECAPED GRE TUNNEL PACKETS
1 (CURRENT)    1,677,876                             2017/05/22 17:45:12 HRS 4 MIN 45 SEC 46
NUMBER OF KIBIBYTES IN THE ENCAPED GRE TUNNEL PACKETS
1 (CURRENT)    1,544,351                             2017/05/22 17:45:12 HRS 4 MIN 45 SEC 46
NUMBER OF KIBIBYTES IN THE DECAPED GRE TUNNEL PACKETS
1 (CURRENT)    1,573,014                             2017/05/22 17:45:12 HRS 4 MIN 45 SEC 46
NUMBER OF KIBIBYTES IN THE ENCAPED AND DECAPED GRE TUNNEL PACKETS
1 (CURRENT)    3,117,365                             2017/05/22 17:45:12 HRS 4 MIN 45 SEC 46
-----
NO. OF ENTRIES: 6
=====
```

ipsec-stats

Syntax **ipsec-stats**

Context show>isa>stats

Description This command enables the context to display IPsec tunnel statistics.

ike-exchange-failure-rate

Syntax **ike-exchange-failure-rate gateway name**
ike-exchange-failure-rate reason reason gateway name [show-oid]
ike-exchange-failure-rate isa mda
ike-exchange-failure-rate reason reason isa mda [show-oid]
ike-exchange-failure-rate system
ike-exchange-failure-rate reason reason system [show-oid]
ike-exchange-failure-rate tunnel-group tunnel-group-id [history-stats-in-count count]
[history-stats-in-min minutes] [current]

ike-exchange-failure-rate reason *reason* tunnel-group *tunnel-group-id* [history-stats-in-count *count*] [history-stats-in-min *minutes*] [current] [show-oid]

Context show>isa>stats>ipsec-stats

Description This command displays IKE exchange failure rate statistics of the specified scope.

This command supports following scopes:

- per system
- per ISA
- per tunnel group
- per IPsec GW

The rate includes the following reasons:

- authentication failure
- non-proposal chosen
- internal address assignment failure
- invalid traffic selector (TS)
- invalid key exchange (KE)
- DPD timeout
- Others

The start time value indicates the starting timestamp of measurement. The sampling duration indicates the duration of the measurement.

If a record has non-zero value, the system also shows the timestamp and local or remote tunnel endpoint for the first and last occurrence in the sampling duration.

Parameters *name* — Displays information about the specified IPsec GW name up to 32 characters in length.

tunnel-type — Displays information about the specified the tunnel type.

Values all, sl2l, dl2l, ra

reason — Displays information for the cause of the failure.

Values auth-failure, non-proposal-chosen, internal-addr-assignment-failure, invalid-ts, invalid-ke, dpd-timeout, other

system — Displays information about the system.

mda — Displays information about the specified ISA ID.

Values slot/mda

tunnel-group-id — Displays information about the specified tunnel group ID.

Values 1 to 16

name — Displays information about the specified IPsec GW name up to 32 characters in length.

count — Displays information for the number of statistics intervals to be displayed (starting with the most recent).

Values 1 to 96

minutes — Displays information about the specified period covered by the statistics to be displayed (starting with the most recent).

Values 1 to 1440

current — Displays information about the current statistic value. The values of count and minutes are ignored by the system once this parameter is specified.

show-oid — Displays information about the Object Identifier (OID) of the current statistical value.

Output The following is an example output of the **show isa stats ipsec-stats ike-exchange-failure-rate** command.

Sample Output

```
show>isa>stats>ipsec-stats# ike-exchange-failure-
rate gateway "rw2"
=====
STATISTICS FOR IPSEC GATEWAY "RW2"
=====
INDEX          VALUE          INFO          START TIME          SAMPLING DURATION
FAILURE TM
-----
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - AUTHENTICATION FAILURE
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.02          2017/07/31 22:52:15 MIN 7 SEC 40
FST: 2017/07/31 22:54:30 RMT:10.1.1.100:[500]
LCL:172.16.200.1:[500]
LST: 2017/07/31 22:54:33 RMT:10.1.1.100:[500]
LCL:172.16.200.1:[500]
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - NON-PROPOSAL CHOSEN
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.00          2017/07/31 22:52:15 MIN 7 SEC 40
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - ADDRESS ASSIGNMENT FAILURE
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.00          2017/07/31 22:52:15 MIN 7 SEC 40
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - INVALID TRAFFIC SELECTOR
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.00          2017/07/31 22:52:15 MIN 7 SEC 40
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - INVALID KEY EXCHANGE
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.00          2017/07/31 22:52:15 MIN 7 SEC 40
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - DPD TIMEOUT
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.00          2017/07/31 22:52:15 MIN 7 SEC 40
IKE EXCHANGE FAILURE RATE (FAILURES/SEC) - OTHER FAILURE REASONS
1 (CURRENT)  0.00          2017/07/31 23:00:00 MIN 4 SEC 51
2          0.00          2017/07/31 22:52:15 MIN 7 SEC 40
-----
NO. OF ENTRIES: 18
=====
```

ikev2-msg-drop

Syntax	ikev2-msg-drop message-type message-type isa mda [show-oid]
Context	show>isa>stats>ipsec-stats
Description	This command displays the early drop counter for received IKEv2 messages on the specified ISA. These counters reflect the number of packets dropped early in the process when ISA is congested.
Parameters	message-type — Specifies the exchange type of the packet to display. Values ike-sa-init, ike-auth, create-child-and-info mda — Specifies the slot and MDA in the format <i>slot/mda</i>. Values <i>slot</i> — 1 to 10 <i>mda</i> — 1 or 2 show-oid — Displays the SNMP object ID of the counter.
Output	The following is an example output of the ikev2-msg-drop message-type command.

Sample Output

```
show>isa>stats>ipsec-stats# ikev2-msg-drop message-type ike-sa-init isa 1/2 show-oid
-----
Current Statistic Info
-----
OID: tmmxIPsecIsaHistStatsValue32.1.1.2.700.1
-----
Statistics for ISA 1/2
=====
Index          Value                      Start Time          Sampling Duration
-----
Number of IKE-SA-INIT exchange packet drops
1 (current)    0                          2018/03/06 21:28:37 min 3 sec 59
-----
No. of entries: 1
```

number-of-tunnels

Syntax	number-of-tunnels gateway name [history-stats-in-count count] [history-stats-in-min minutes] [current]
	number-of-tunnels tunnel-type tunnel-type gateway name [history-stats-in-count count] [history-stats-in-min minutes] [current] [show-oid]
	number-of-tunnels isa mda [history-stats-in-count count] [history-stats-in-min minutes] [current]
	number-of-tunnels tunnel-type tunnel-type isa mda [history-stats-in-count count] [history-stats-in-min minutes] [current] [show-oid]


```

number-of-tunnels system [history-stats-in-count count] [history-stats-in-min minutes]
[current]
number-of-tunnels tunnel-type tunnel-type system [history-stats-in-count count]
[history-stats-in-min minutes] [current] [show-oid]
number-of-tunnels tunnel-group tunnel-group-id [history-stats-in-count count] [history-
stats-in-min minutes] [current]
number-of-tunnels tunnel-type tunnel-type tunnel-group tunnel-group-id [history-stats-
in-count count] [history-stats-in-min minutes] [current] [show-oid]

```

Context show>isa>stats>ipsec-stats

Description This command displays information for the number of IPsec tunnel statistics of the specified tunnel type and scope. The system collects statistics every hour for the last 24 hour according to the wall clock. The current value is also included in the output.

This command supports following scopes:

- per system
- per ISA
- per tunnel group
- per IPsec GW

The **start time** value in the output indicates the time when the results are collected.

Parameters *tunnel-type* — Displays information about the specified the tunnel type.

Values all, sl2l, dl2l, ra

mda — Displays information about the specified ISA ID.

Values slot/mda

tunnel-group-id — Displays information about the specified tunnel group ID.

Values 1 to 16

name — Displays information about the specified IPsec GW name up to 32 characters in length.

count — Displays information for the number of statistics intervals to be displayed (starting with the most recent).

Values 1 to 96

minutes — Displays information about the specified period covered by the statistics to be displayed (starting with the most recent).

Values 1 to 1440

current — Displays information about the current value. The values of count and minutes are ignored by the system once this parameter is specified.

show-oid — Displays information about the Object Identifier (OID) of the current statistical value.

Output The following is an example output of the **show isa statistics ipsec-stats number** of tunnels command.

Sample Output

```
show>isa>stats>ipsec-stats# number-of-tunnels tunnel-group 1
=====
STATISTICS FOR ISA TUNNEL GROUP 1
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
NUMBER OF TOTAL IPSEC TUNNELS
1 (CURRENT)    1          2017/05/23 00:30:13 N/A
2              1          2017/05/23 00:00:00 N/A
3              1          2017/05/22 23:00:00 N/A
4              0          2017/05/22 22:00:00 N/A
5              0          2017/05/22 21:00:00 N/A
6              0          2017/05/22 20:00:00 N/A
7              0          2017/05/22 19:00:00 N/A
8              1          2017/05/22 18:00:00 N/A
NUMBER OF IPSEC STATIC LAN-TO-LAN (SL2L) TUNNELS
1 (CURRENT)    0          2017/05/23 00:30:13 N/A
2              0          2017/05/23 00:00:00 N/A
3              0          2017/05/22 23:00:00 N/A
4              0          2017/05/22 22:00:00 N/A
5              0          2017/05/22 21:00:00 N/A
6              0          2017/05/22 20:00:00 N/A
7              0          2017/05/22 19:00:00 N/A
8              0          2017/05/22 18:00:00 N/A
NUMBER OF IPSEC DYNAMIC LAN-TO-LAN (DL2L) TUNNELS
1 (CURRENT)    0          2017/05/23 00:30:13 N/A
2              0          2017/05/23 00:00:00 N/A
3              0          2017/05/22 23:00:00 N/A
4              0          2017/05/22 22:00:00 N/A
5              0          2017/05/22 21:00:00 N/A
6              0          2017/05/22 20:00:00 N/A
7              0          2017/05/22 19:00:00 N/A
8              0          2017/05/22 18:00:00 N/A
NUMBER OF IPSEC REMOTE ACCESS (RA) TUNNELS
1 (CURRENT)    1          2017/05/23 00:30:13 N/A
2              1          2017/05/23 00:00:00 N/A
3              1          2017/05/22 23:00:00 N/A
4              0          2017/05/22 22:00:00 N/A
5              0          2017/05/22 21:00:00 N/A
6              0          2017/05/22 20:00:00 N/A
7              0          2017/05/22 19:00:00 N/A
8              1          2017/05/22 18:00:00 N/A
-----
NO. OF ENTRIES: 32
=====
SHOW>ISA>STATS>IPSEC-STATS# NUMBER-OF-TUNNELS TUNNEL-GROUP 1 SHOW-OID TUNNEL-
TYPE ALL
-----
CURRENT STATISTIC INFO
-----
OID: TMNXIPSECTNLGRPHISTSTATSVALUE10.1.1.2
=====
```

STATISTICS FOR ISA TUNNEL GROUP 1			
INDEX	VALUE	START TIME	SAMPLING DURATION
NUMBER OF TOTAL IPSEC TUNNELS			
1 (CURRENT)	1	2017/05/23 00:32:04	N/A
2	1	2017/05/23 00:00:00	N/A
3	1	2017/05/22 23:00:00	N/A
4	0	2017/05/22 22:00:00	N/A
5	0	2017/05/22 21:00:00	N/A
6	0	2017/05/22 20:00:00	N/A
7	0	2017/05/22 19:00:00	N/A
8	1	2017/05/22 18:00:00	N/A
NO. OF ENTRIES: 8			

throughput

Syntax

```
throughput gateway name [history-stats-in-count count] [history-stats-in-min min]
[current]
throughput type type gateway name [history-stats-in-count count] [history-stats-in-min min]
[current] [show-oid]
throughput isa mda [history-stats-in-count count] [history-stats-in-min min] [current]
throughput type type isa mda [history-stats-in-count count] [history-stats-in-min min]
[current] [show-oid]
throughput system [history-stats-in-count count] [history-stats-in-min min] [current]
throughput type type system [history-stats-in-count count] [history-stats-in-min min]
[current] [show-oid]
throughput tunnel-group tunnel-group-id [history-stats-in-count count] [history-stats-in-min min]
[current]
throughput type type tunnel-group tunnel-group-id [history-stats-in-count count]
[history-stats-in-min min] [current] [show-oid]
```

Context show>isa>stats>ipsec-stats

Description This command displays IPsec throughput statistics for the specified scope.

The system collects statistics every 10 minutes for last 24 hour per wall clock. A current value is included in the output.

This command supports following the scopes:

- per system
- per ISA
- per tunnel group
- per IPsec GW

The statistics include:

- The number of bidirectional encrypted and decrypted per second
- The number of encrypted packets per second
- The number of decrypted packets per second
- The number of bidirectional (encrypted and decrypted) bits per second (in Mibits/s)
- The number of bidirectional encrypted bits per second (in Mibits/s)
- The number of bidirectional decrypted bits per second (in Mibits/s)

Syntax notes:

- 1 Mibits/s equals 2²⁰ bit/s
- The bits per second counter is an integer, which is a value rounded down from the measured value.

Parameters *mda* — Displays information about the specified ISA.

Values slot/mda

tunnel-group-id — Displays information about the specified tunnel group ID.

Values 1 to 16

name — Displays information about the name of the IPsec GW up to 32 characters in length.

count — Displays information about the number of historical values to be included in the output

Values 1 to 24

min — Displays information about the number of minutes of historical values to be included in output

Values 1 to 1440

current — Displays information about the current value.

show-oid — Displays information about include SNMP OID and instance ID for the latest historical value in the output, for a specified type of counter.

Output The following output is an example of the show isa stats ipsec-stats throughput command.

Sample Output

```
show>isa>stats>ipsec-stats# throughput tunnel-group 1
=====
STATISTICS FOR ISA TUNNEL GROUP 1
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
ENCRYPTED IPSEC TRAFFIC THROUGHPUT (PKTS/SEC)
1 (CURRENT)    99              2017/05/23 22:00:00 MIN 7 SEC 51
2              72              2017/05/23 21:50:00 MIN 10
3              0               2017/05/23 21:40:00 MIN 10
4              0               2017/05/23 21:30:00 MIN 10
5              0               2017/05/23 21:20:00 MIN 10
```

6	0	2017/05/23 21:10:00 MIN 10
7	0	2017/05/23 21:00:00 MIN 10
8	0	2017/05/23 20:50:00 MIN 10
9	0	2017/05/23 20:40:00 MIN 10
10	0	2017/05/23 20:30:00 MIN 10
11	0	2017/05/23 20:20:00 MIN 10
12	0	2017/05/23 20:10:00 MIN 10
13	0	2017/05/23 20:00:00 MIN 10
14	0	2017/05/23 19:50:00 MIN 10
15	0	2017/05/23 19:40:00 MIN 10
16	0	2017/05/23 19:30:00 MIN 10
17	0	2017/05/23 19:20:00 MIN 10
18	0	2017/05/23 19:10:00 MIN 10
19	0	2017/05/23 19:00:00 MIN 10
20	0	2017/05/23 18:50:00 MIN 10
21	0	2017/05/23 18:40:00 MIN 10
22	0	2017/05/23 18:30:00 MIN 10
23	0	2017/05/23 18:20:00 MIN 10
24	0	2017/05/23 18:10:00 MIN 10
25	0	2017/05/23 18:00:00 MIN 10
26	0	2017/05/23 17:50:48 MIN 9 SEC 12
DECRYPTED IPSEC TRAFFIC THROUGHPUT (PKTS/SEC)		
1 (CURRENT)	99	2017/05/23 22:00:00 MIN 7 SEC 51
2	72	2017/05/23 21:50:00 MIN 10
3	0	2017/05/23 21:40:00 MIN 10
4	0	2017/05/23 21:30:00 MIN 10
5	0	2017/05/23 21:20:00 MIN 10
6	0	2017/05/23 21:10:00 MIN 10
7	0	2017/05/23 21:00:00 MIN 10
8	0	2017/05/23 20:50:00 MIN 10
9	0	2017/05/23 20:40:00 MIN 10
10	0	2017/05/23 20:30:00 MIN 10
11	0	2017/05/23 20:20:00 MIN 10
12	0	2017/05/23 20:10:00 MIN 10
13	0	2017/05/23 20:00:00 MIN 10
14	0	2017/05/23 19:50:00 MIN 10
15	0	2017/05/23 19:40:00 MIN 10
16	0	2017/05/23 19:30:00 MIN 10
17	0	2017/05/23 19:20:00 MIN 10
18	0	2017/05/23 19:10:00 MIN 10
19	0	2017/05/23 19:00:00 MIN 10
20	0	2017/05/23 18:50:00 MIN 10
21	0	2017/05/23 18:40:00 MIN 10
22	0	2017/05/23 18:30:00 MIN 10
23	0	2017/05/23 18:20:00 MIN 10
24	0	2017/05/23 18:10:00 MIN 10
25	0	2017/05/23 18:00:00 MIN 10
26	0	2017/05/23 17:50:48 MIN 9 SEC 12
ENCRYPTED AND DECRYPTED IPSEC TRAFFIC THROUGHPUT (PKTS/SEC)		
1 (CURRENT)	199	2017/05/23 22:00:00 MIN 7 SEC 51
2	145	2017/05/23 21:50:00 MIN 10
3	0	2017/05/23 21:40:00 MIN 10
4	0	2017/05/23 21:30:00 MIN 10
5	0	2017/05/23 21:20:00 MIN 10
6	0	2017/05/23 21:10:00 MIN 10
7	0	2017/05/23 21:00:00 MIN 10
8	0	2017/05/23 20:50:00 MIN 10
9	0	2017/05/23 20:40:00 MIN 10
10	0	2017/05/23 20:30:00 MIN 10

11	0	2017/05/23 20:20:00 MIN 10
12	0	2017/05/23 20:10:00 MIN 10
4	0	2017/05/23 21:30:00 MIN 10
5	0	2017/05/23 21:20:00 MIN 10
6	0	2017/05/23 21:10:00 MIN 10
7	0	2017/05/23 21:00:00 MIN 10
8	0	2017/05/23 20:50:00 MIN 10
9	0	2017/05/23 20:40:00 MIN 10
10	0	2017/05/23 20:30:00 MIN 10
11	0	2017/05/23 20:20:00 MIN 10
12	0	2017/05/23 20:10:00 MIN 10
13	0	2017/05/23 20:00:00 MIN 10
14	0	2017/05/23 19:50:00 MIN 10
15	0	2017/05/23 19:40:00 MIN 10
16	0	2017/05/23 19:30:00 MIN 10
17	0	2017/05/23 19:20:00 MIN 10
18	0	2017/05/23 19:10:00 MIN 10
19	0	2017/05/23 19:00:00 MIN 10
20	0	2017/05/23 18:50:00 MIN 10
21	0	2017/05/23 18:40:00 MIN 10
22	0	2017/05/23 18:30:00 MIN 10
23	0	2017/05/23 18:20:00 MIN 10
24	0	2017/05/23 18:10:00 MIN 10
25	0	2017/05/23 18:00:00 MIN 10
26	0	2017/05/23 17:50:48 MIN 9 SEC 12
DECRYPTED IPSEC TRAFFIC THROUGHPUT (MIBIT/SEC)		
1 (CURRENT)	3	2017/05/23 22:00:00 MIN 7 SEC 51
2	2	2017/05/23 21:50:00 MIN 10
3	0	2017/05/23 21:40:00 MIN 10
4	0	2017/05/23 21:30:00 MIN 10
5	0	2017/05/23 21:20:00 MIN 10
6	0	2017/05/23 21:10:00 MIN 10
7	0	2017/05/23 21:00:00 MIN 10
8	0	2017/05/23 20:50:00 MIN 10
9	0	2017/05/23 20:40:00 MIN 10
10	0	2017/05/23 20:30:00 MIN 10
11	0	2017/05/23 20:20:00 MIN 10
12	0	2017/05/23 20:10:00 MIN 10
13	0	2017/05/23 20:00:00 MIN 10
14	0	2017/05/23 19:50:00 MIN 10
15	0	2017/05/23 19:40:00 MIN 10
16	0	2017/05/23 19:30:00 MIN 10
17	0	2017/05/23 19:20:00 MIN 10
18	0	2017/05/23 19:10:00 MIN 10
19	0	2017/05/23 19:00:00 MIN 10
20	0	2017/05/23 18:50:00 MIN 10
21	0	2017/05/23 18:40:00 MIN 10
22	0	2017/05/23 18:30:00 MIN 10
23	0	2017/05/23 18:20:00 MIN 10
24	0	2017/05/23 18:10:00 MIN 10
25	0	2017/05/23 18:00:00 MIN 10
26	0	2017/05/23 17:50:48 MIN 9 SEC 12
ENCRYPTED AND DECRYPTED IPSEC TRAFFIC THROUGHPUT (MIBIT/SEC)		
1 (CURRENT)	7	2017/05/23 22:00:00 MIN 7 SEC 51
2	5	2017/05/23 21:50:00 MIN 10
3	0	2017/05/23 21:40:00 MIN 10
4	0	2017/05/23 21:30:00 MIN 10
5	0	2017/05/23 21:20:00 MIN 10
6	0	2017/05/23 21:10:00 MIN 10

7	0	2017/05/23 21:00:00 MIN 10
8	0	2017/05/23 20:50:00 MIN 10
9	0	2017/05/23 20:40:00 MIN 10
10	0	2017/05/23 20:30:00 MIN 10
11	0	2017/05/23 20:20:00 MIN 10
12	0	2017/05/23 20:10:00 MIN 10
13	0	2017/05/23 20:00:00 MIN 10
14	0	2017/05/23 19:50:00 MIN 10
15	0	2017/05/23 19:40:00 MIN 10
16	0	2017/05/23 19:30:00 MIN 10
17	0	2017/05/23 19:20:00 MIN 10
18	0	2017/05/23 19:10:00 MIN 10
19	0	2017/05/23 19:00:00 MIN 10
20	0	2017/05/23 18:50:00 MIN 10
21	0	2017/05/23 18:40:00 MIN 10
22	0	2017/05/23 18:30:00 MIN 10
23	0	2017/05/23 18:20:00 MIN 10
24	0	2017/05/23 18:10:00 MIN 10
25	0	2017/05/23 18:00:00 MIN 10
26	0	2017/05/23 17:50:48 MIN 9 SEC 12

NO. OF ENTRIES: 156

=====

show>isa>stats>ipsec-stats# throughput type bidir-bps isa 1/2 show-oid

CURRENT STATISTIC INFO-----
OID: TMNXIPSECISAHISTSTATSVALUE10.1.1.2.105.2-----
STATISTICS FOR ISA 1/2

=====

INDEX	VALUE	START TIME	SAMPLING DURATION

ENCRYPTED AND DECRYPTED IPSEC TRAFFIC THROUGHPUT (MIBIT/SEC)

1 (CURRENT)	7	2017/05/23 22:10:00 MIN 1 SEC 9
2	7	2017/05/23 22:00:00 MIN 10
3	5	2017/05/23 21:50:00 MIN 10
4	0	2017/05/23 21:40:00 MIN 10
5	0	2017/05/23 21:30:00 MIN 10
6	0	2017/05/23 21:20:00 MIN 10
7	0	2017/05/23 21:10:00 MIN 10
8	0	2017/05/23 21:00:00 MIN 10
9	0	2017/05/23 20:50:00 MIN 10
10	0	2017/05/23 20:40:00 MIN 10
11	0	2017/05/23 20:30:00 MIN 10
12	0	2017/05/23 20:20:00 MIN 10
13	0	2017/05/23 20:10:00 MIN 10
14	0	2017/05/23 20:00:00 MIN 10
15	0	2017/05/23 19:50:00 MIN 10
16	0	2017/05/23 19:40:00 MIN 10
17	0	2017/05/23 19:30:00 MIN 10
18	0	2017/05/23 19:20:00 MIN 10
19	0	2017/05/23 19:10:00 MIN 10
20	0	2017/05/23 19:00:00 MIN 10
21	0	2017/05/23 18:50:00 MIN 10
22	0	2017/05/23 18:40:00 MIN 10
23	0	2017/05/23 18:30:00 MIN 10
24	0	2017/05/23 18:20:00 MIN 10

```

25          0          2017/05/23 18:10:00 MIN 10
26          0          2017/05/23 18:00:00 MIN 10
27          0          2017/05/23 17:50:48 MIN 9 SEC 12
-----

```

```

NO. OF ENTRIES: 27
=====

```

traffic-forward

Syntax **traffic-forward** [*type type*] *gateway name*
traffic-forward [*type type*] *isa mda*
traffic-forward [*type type*] *gateway name dynamic-tunnel ip-address:port*
traffic-forward [*type type*] *tunnel ipsec-tunnel-name*

Context show>isa>stats>ipsec-stats

Description This command displays traffic forward statistics of the specified scope.

This command supports following scopes:

- per system
- per ISA
- per tunnel group
- per IPsec GW

The statistics include:

- The number of bidirectional encrypted and decrypted packets
- The number of encrypted packets
- The number of decrypted packets per second
- The number of bidirectional (encrypted and decrypted) in kilobytes
- The number of bidirectional encrypted bits in kilobytes
- The number of bidirectional decrypted bits in kilobytes

1 kilobyte equals 2^{10} bytes

The start time indicates the starting timestamp of the measurement. The sampling duration indicates the duration of the measurement.

Parameters *name* — Displays information about the name of the IPsec GW up to 32 characters in length.

mda — Displays information about the specified ISA.

Values slot/mda

tunnel-group-id — Displays information about the specified tunnel group ID.

Values 1 to 16

ip-address:port — Displays information about the IP address and port of the peer for dynamic tunneling.

ipsec-tunnel-name — Specifies the name of the static LAN-to-LAN tunnel up to 32 characters in length.

Output The following output is an example of the **show isa stats ipsec-stats traffic forward isa** command.

Sample Output

```
show>isa>stats>ipsec-stats# traffic-forward isa 1/2
=====
STATISTICS FOR ISA 1/2
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
NUMBER OF ENCRYPTED IPSEC PACKETS
1 (CURRENT)  770,881          2017/05/23 17:50:48 HRS 6 MIN 33 SEC 57
NUMBER OF DECRYPTED IPSEC PACKETS
1 (CURRENT)  770,881          2017/05/23 17:50:48 HRS 6 MIN 33 SEC 57
NUMBER OF ENCRYPTED AND DECRYPTED IPSEC PACKETS
1 (CURRENT)  1,541,762        2017/05/23 17:50:48 HRS 6 MIN 33 SEC 57
NUMBER OF KIBIBYTES IN THE ENCRYPTED IPSEC PACKETS
1 (CURRENT)  3,785,141        2017/05/23 17:50:48 HRS 6 MIN 33 SEC 57
NUMBER OF KIBIBYTES IN THE DECRYPTED IPSEC PACKETS
1 (CURRENT)  3,785,141        2017/05/23 17:50:48 HRS 6 MIN 33 SEC 57
NUMBER OF KIBIBYTES IN THE ENCRYPTED AND DECRYPTED IPSEC PACKETS
1 (CURRENT)  7,570,282        2017/05/23 17:50:48 HRS 6 MIN 33 SEC 57
-----
NO. OF ENTRIES: 6
=====

show>isa>stats>ipsec-stats# traffic-forward gateway "rw" dynamic-
tunnel 10.1.1.100:500
=====
STATISTICS FOR IPSEC REMOTE USER TUNNEL "10.1.1.100:500"
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
NUMBER OF ENCRYPTED IPSEC PACKETS
1 (CURRENT)  676,774          2017/05/23 22:36:15 HRS 1 MIN 52 SEC 49
NUMBER OF DECRYPTED IPSEC PACKETS
1 (CURRENT)  676,774          2017/05/23 22:36:15 HRS 1 MIN 52 SEC 49
NUMBER OF ENCRYPTED AND DECRYPTED IPSEC PACKETS
1 (CURRENT)  1,353,548        2017/05/23 22:36:15 HRS 1 MIN 52 SEC 49
NUMBER OF KIBIBYTES IN THE ENCRYPTED IPSEC PACKETS
1 (CURRENT)  3,323,066        2017/05/23 22:36:15 HRS 1 MIN 52 SEC 49
NUMBER OF KIBIBYTES IN THE DECRYPTED IPSEC PACKETS
1 (CURRENT)  3,323,066        2017/05/23 22:36:15 HRS 1 MIN 52 SEC 49
NUMBER OF KIBIBYTES IN THE ENCRYPTED AND DECRYPTED IPSEC PACKETS
1 (CURRENT)  6,646,132        2017/05/23 22:36:15 HRS 1 MIN 52 SEC 49
-----
NO. OF ENTRIES: 6
=====
```

tunnel-setup-rate

Syntax	tunnel-setup-rate gateway <i>name</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] tunnel-setup-rate tunnel-type <i>tunnel-type</i> gateway <i>name</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] [show-oid] tunnel-setup-rate isa <i>mda</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] tunnel-setup-rate tunnel-type <i>tunnel-type</i> isa <i>mda</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] [show-oid] tunnel-setup-rate system [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] tunnel-setup-rate tunnel-type <i>tunnel-type</i> system [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] [show-oid] tunnel-setup-rate tunnel-group <i>tunnel-group-id</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] tunnel-setup-rate tunnel-type <i>tunnel-type</i> tunnel-group <i>tunnel-group-id</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] [show-oid]
Context	show>isa>stats>ipsec-stats
Description	This command displays IPsec tunnel setup rate statistics of the specified scope. The system collects statistics every hour for the last 24 hour period per wall clock. A current value is also included in the output. This command supports following scopes: • per system • per ISA • per tunnel group • per IPsec GW The statics include the following setup rates: • static tunnel • dynamic LAN-to-LAN tunnel • remote access tunnel • all types of tunnel The start time indicates the starting timestamp of measurement. The sampling duration indicates the duration of measurement.
Parameters	<i>name</i> — Displays information about the name of the IPsec GW up to 32 characters in length. <i>mda</i> — Displays information about the specified ISA.
Values	slot/mda

tunnel-group-id — Displays information about the specified tunnel group ID.

Values 1 to 16

count — Displays information for the number of statistics intervals to be displayed (starting with the most recent).

Values 1 to 24

minutes — Displays information about the specified period covered by the statistics to be displayed (starting with the most recent).

Values 1 to 1440

type — Displays information about the specified tunnel type associated with this IPsec GW.

Values all, sl2l, dl2l, ra

current — Displays information about the current statistic value. The values of count and minutes are ignored by the system once this parameter is specified.

show-oid — Displays information about the OID of the current statistical value.

tunnel-isa

Syntax	tunnel-isa
Context	show>isa>stats
Description	This command enables the context to display tunnel ISA statistics including ISA CPU usage and memory allocation failure rates.

cpu-usage

Syntax	cpu-usage mda [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] cpu-usage mda [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] [show-oid] type {control-plane data-plane}
Context	show>isa>stats>tunnel-isa
Description	This command displays the CPU usage of the specified ISA. The information includes control plane usage and data plane usage. The data plane usage collection depends on the configuration of config>isa>tunnel-grp>stats-collection>isa-dp-cpu-usage system collects usage every 5 minutes for the last 24 hours. The output also includes the current value.
Parameters	<i>count</i> — Displays information for the number of statistics intervals to be displayed (starting with the most recent). Values 1 to 24

minutes — Displays information about the specified period covered by the statistics to be displayed (starting with the most recent).

Values 1 to 1440

current — Displays information about the current statistic value. The values of count and minutes are ignored by the system once this parameter is specified.

show-oid — Displays information about the Object Identifier (OID) of the current statistical value.

mda — Displays information about the specified ISA.

Values slot/mda

control-plane — Displays information about the control plane.

data-plane — Displays information about the data plane

Output The following is an example output of the **show isa stats tunnel-isa cpu-usage** configuration.

Sample Output

```
show>isa>stats>tunnel-isa# cpu-usage 1/2
=====
STATISTICS FOR ISA 1/2
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
ISA CONTROL PLANE CPU USAGE PERCENTAGE (%)
16             0.05             2017/05/24 02:30:00 MIN 5
17             0.00             2017/05/24 02:25:00 MIN 5
18             0.03             2017/05/24 02:20:00 MIN 5
19             0.06             2017/05/24 02:15:00 MIN 5
20             0.05             2017/05/24 02:10:00 MIN 5
21             0.07             2017/05/24 02:05:00 MIN 5
22             0.06             2017/05/24 02:00:00 MIN 5
23             0.05             2017/05/24 01:55:00 MIN 5
24             0.00             2017/05/24 01:50:00 MIN 5
25             0.07             2017/05/24 01:45:00 MIN 5
26             0.01             2017/05/24 01:40:00 MIN 5
27             0.04             2017/05/24 01:35:00 MIN 5
28             0.01             2017/05/24 01:30:00 MIN 5
29             0.00             2017/05/24 01:25:00 MIN 5
30             0.01             2017/05/24 01:20:00 MIN 5
31             0.01             2017/05/24 01:15:00 MIN 5
32             0.01             2017/05/24 01:10:00 MIN 5
33             0.06             2017/05/24 01:05:00 MIN 5
34             0.01             2017/05/24 01:00:00 MIN 5
35             0.02             2017/05/24 00:55:00 MIN 5
36             0.03             2017/05/24 00:50:00 MIN 5
37             0.03             2017/05/24 00:45:00 MIN 5
38             0.01             2017/05/24 00:40:00 MIN 5
39             0.01             2017/05/24 00:35:00 MIN 5
40             0.02             2017/05/24 00:30:00 MIN 5
41             0.01             2017/05/24 00:25:00 MIN 5
42             0.03             2017/05/24 00:20:00 MIN 5
43             0.02             2017/05/24 00:15:00 MIN 5
```

44	0.06	2017/05/24 00:10:00 MIN 5
45	0.05	2017/05/24 00:05:00 MIN 5
46	0.00	2017/05/24 00:00:00 MIN 5
47	0.02	2017/05/23 23:55:00 MIN 5
48	0.04	2017/05/23 23:50:00 MIN 5
49	0.03	2017/05/23 23:45:00 MIN 5
50	0.06	2017/05/23 23:40:00 MIN 5
51	0.00	2017/05/23 23:35:00 MIN 5
52	0.05	2017/05/23 23:30:00 MIN 5
53	0.02	2017/05/23 23:25:00 MIN 5
54	0.03	2017/05/23 23:20:00 MIN 5
55	0.02	2017/05/23 23:15:00 MIN 5
56	0.06	2017/05/23 23:10:00 MIN 5
57	0.04	2017/05/23 23:05:00 MIN 5
58	0.00	2017/05/23 23:00:00 MIN 5
59	0.00	2017/05/23 22:55:00 MIN 5
60	0.04	2017/05/23 22:50:00 MIN 5
61	0.03	2017/05/23 22:45:00 MIN 5
62	0.03	2017/05/23 22:40:00 MIN 5
63	0.04	2017/05/23 22:35:00 MIN 5
64	0.05	2017/05/23 22:30:00 MIN 5
65	0.02	2017/05/23 22:25:00 MIN 5
66	0.05	2017/05/23 22:20:00 MIN 5
67	0.03	2017/05/23 22:15:00 MIN 5
68	0.01	2017/05/23 22:10:00 MIN 5
69	0.02	2017/05/23 22:05:00 MIN 5
70	0.01	2017/05/23 22:00:00 MIN 5
71	0.05	2017/05/23 21:55:00 MIN 5
72	0.02	2017/05/23 21:50:00 MIN 5
73	0.02	2017/05/23 21:45:00 MIN 5
74	0.00	2017/05/23 21:40:00 MIN 5
75	0.00	2017/05/23 21:35:00 MIN 5
76	0.01	2017/05/23 21:30:00 MIN 5
77	0.06	2017/05/23 21:25:00 MIN 5
78	0.01	2017/05/23 21:20:00 MIN 5
79	0.01	2017/05/23 21:15:00 MIN 5
80	0.00	2017/05/23 21:10:00 MIN 5
81	0.06	2017/05/23 21:05:00 MIN 5
82	0.06	2017/05/23 21:00:00 MIN 5
83	0.00	2017/05/23 20:55:00 MIN 5
84	0.02	2017/05/23 20:50:00 MIN 5
85	0.00	2017/05/23 20:45:00 MIN 5
86	0.00	2017/05/23 20:40:00 MIN 5
87	0.06	2017/05/23 20:35:00 MIN 5
88	0.01	2017/05/23 20:30:00 MIN 5
89	0.01	2017/05/23 20:25:00 MIN 5
90	0.02	2017/05/23 20:20:00 MIN 5
91	0.03	2017/05/23 20:15:00 MIN 5
92	0.04	2017/05/23 20:10:00 MIN 5
93	0.05	2017/05/23 20:05:00 MIN 5
94	0.05	2017/05/23 20:00:00 MIN 5
95	0.05	2017/05/23 19:55:00 MIN 5
96	0.05	2017/05/23 19:50:00 MIN 5
97	0.06	2017/05/23 19:45:00 MIN 5
98	0.06	2017/05/23 19:40:00 MIN 5
99	0.05	2017/05/23 19:35:00 MIN 5
100	0.05	2017/05/23 19:30:00 MIN 5
101	0.04	2017/05/23 19:25:00 MIN 5
102	0.04	2017/05/23 19:20:00 MIN 5

103	0.04	2017/05/23 19:15:00 MIN 5
104	0.05	2017/05/23 19:10:00 MIN 5
105	0.04	2017/05/23 19:05:00 MIN 5
106	0.03	2017/05/23 19:00:00 MIN 5
107	0.03	2017/05/23 18:55:00 MIN 5
108	0.01	2017/05/23 18:50:00 MIN 5
109	0.02	2017/05/23 18:45:00 MIN 5
110	0.02	2017/05/23 18:40:00 MIN 5
111	0.02	2017/05/23 18:35:00 MIN 5
112	0.01	2017/05/23 18:30:00 MIN 5
113	0.02	2017/05/23 18:25:00 MIN 5
114	0.02	2017/05/23 18:20:00 MIN 5
115	0.01	2017/05/23 18:15:00 MIN 5
116	0.02	2017/05/23 18:10:00 MIN 5
117	0.01	2017/05/23 18:05:00 MIN 5
118	0.02	2017/05/23 18:00:00 MIN 5
119	0.01	2017/05/23 17:55:00 MIN 5
120	0.08	2017/05/23 17:50:48 MIN 4 SEC 12
ISA DATA PLANE CPU USAGE PERCENTAGE (%)		
1 (CURRENT)	13.13	2017/05/24 03:45:00 SEC 25
2	13.24	2017/05/24 03:40:00 MIN 5
3	13.43	2017/05/24 03:35:00 MIN 5
4	13.30	2017/05/24 03:30:00 MIN 5
5	13.26	2017/05/24 03:25:00 MIN 5
6	13.16	2017/05/24 03:20:00 MIN 5
7	13.16	2017/05/24 03:15:00 MIN 5
8	13.22	2017/05/24 03:10:00 MIN 5
9	13.31	2017/05/24 03:05:00 MIN 5
10	13.95	2017/05/24 03:00:00 MIN 5
11	13.71	2017/05/24 02:55:00 MIN 5
12	14.00	2017/05/24 02:50:00 MIN 5
13	13.26	2017/05/24 02:45:00 MIN 5
14	13.11	2017/05/24 02:40:00 MIN 5
15	13.09	2017/05/24 02:35:00 MIN 5
16	13.22	2017/05/24 02:30:00 MIN 5
17	13.91	2017/05/24 02:25:00 MIN 5
18	13.53	2017/05/24 02:20:00 MIN 5
19	13.83	2017/05/24 02:15:00 MIN 5
20	13.05	2017/05/24 02:10:00 MIN 5
21	13.10	2017/05/24 02:05:00 MIN 5
22	13.09	2017/05/24 02:00:00 MIN 5
23	13.72	2017/05/24 01:55:00 MIN 5
24	13.65	2017/05/24 01:50:00 MIN 5
25	13.81	2017/05/24 01:45:00 MIN 5
26	13.31	2017/05/24 01:40:00 MIN 5
27	13.10	2017/05/24 01:35:00 MIN 5
28	13.10	2017/05/24 01:30:00 MIN 5
29	13.31	2017/05/24 01:25:00 MIN 5
30	13.92	2017/05/24 01:20:00 MIN 5
31	13.58	2017/05/24 01:15:00 MIN 5
32	13.64	2017/05/24 01:10:00 MIN 5
33	13.11	2017/05/24 01:05:00 MIN 5
34	13.18	2017/05/24 01:00:00 MIN 5
35	13.27	2017/05/24 00:55:00 MIN 5
36	13.90	2017/05/24 00:50:00 MIN 5
37	13.59	2017/05/24 00:45:00 MIN 5
38	13.79	2017/05/24 00:40:00 MIN 5
39	13.16	2017/05/24 00:35:00 MIN 5
40	13.24	2017/05/24 00:30:00 MIN 5

41	13.28	2017/05/24 00:25:00 MIN 5
42	14.02	2017/05/24 00:20:00 MIN 5
43	13.65	2017/05/24 00:15:00 MIN 5
44	13.66	2017/05/24 00:10:00 MIN 5
45	13.07	2017/05/24 00:05:00 MIN 5
46	13.12	2017/05/24 00:00:00 MIN 5
47	13.32	2017/05/23 23:55:00 MIN 5
48	13.80	2017/05/23 23:50:00 MIN 5
49	13.69	2017/05/23 23:45:00 MIN 5
50	13.37	2017/05/23 23:40:00 MIN 5
51	13.05	2017/05/23 23:35:00 MIN 5
52	13.07	2017/05/23 23:30:00 MIN 5
53	13.58	2017/05/23 23:25:00 MIN 5
54	13.55	2017/05/23 23:20:00 MIN 5
55	13.80	2017/05/23 23:15:00 MIN 5
56	13.18	2017/05/23 23:10:00 MIN 5
57	13.13	2017/05/23 23:05:00 MIN 5
58	13.12	2017/05/23 23:00:00 MIN 5
59	13.80	2017/05/23 22:55:00 MIN 5
60	13.55	2017/05/23 22:50:00 MIN 5
61	13.77	2017/05/23 22:45:00 MIN 5
62	13.08	2017/05/23 22:40:00 MIN 5
63	9.77	2017/05/23 22:35:00 MIN 5
64	0.02	2017/05/23 22:30:00 MIN 5
65	0.02	2017/05/23 22:25:00 MIN 5
66	0.01	2017/05/23 22:20:00 MIN 5
67	0.00	2017/05/23 22:15:00 MIN 5
68	7.08	2017/05/23 22:10:00 MIN 5
69	13.09	2017/05/23 22:05:00 MIN 5
70	13.58	2017/05/23 22:00:00 MIN 5
71	13.63	2017/05/23 21:55:00 MIN 5
72	6.34	2017/05/23 21:50:00 MIN 5
73	0.00	2017/05/23 21:45:00 MIN 5
74	0.00	2017/05/23 21:40:00 MIN 5
75	0.00	2017/05/23 21:35:00 MIN 5
76	0.00	2017/05/23 21:30:00 MIN 5
77	0.00	2017/05/23 21:25:00 MIN 5
78	0.00	2017/05/23 21:20:00 MIN 5
79	0.00	2017/05/23 21:15:00 MIN 5
80	0.00	2017/05/23 21:10:00 MIN 5
81	0.00	2017/05/23 21:05:00 MIN 5
82	0.00	2017/05/23 21:00:00 MIN 5
83	0.00	2017/05/23 20:55:00 MIN 5
84	0.00	2017/05/23 20:50:00 MIN 5
85	0.00	2017/05/23 20:45:00 MIN 5
86	0.00	2017/05/23 20:40:00 MIN 5
87	0.00	2017/05/23 20:35:00 MIN 5
88	0.00	2017/05/23 20:30:00 MIN 5
89	0.00	2017/05/23 20:25:00 MIN 5
90	0.00	2017/05/23 20:20:00 MIN 5
91	0.00	2017/05/23 20:15:00 MIN 5
92	0.00	2017/05/23 20:10:00 MIN 5
93	0.00	2017/05/23 20:05:00 MIN 5
94	0.00	2017/05/23 20:00:00 MIN 5
95	0.00	2017/05/23 19:55:00 MIN 5
96	0.00	2017/05/23 19:50:00 MIN 5
97	0.00	2017/05/23 19:45:00 MIN 5
98	0.00	2017/05/23 19:40:00 MIN 5
99	0.00	2017/05/23 19:35:00 MIN 5

100	0.00	2017/05/23 19:30:00 MIN 5
101	0.00	2017/05/23 19:25:00 MIN 5
102	0.00	2017/05/23 19:20:00 MIN 5
103	0.00	2017/05/23 19:15:00 MIN 5
104	0.00	2017/05/23 19:10:00 MIN 5
105	0.00	2017/05/23 19:05:00 MIN 5
106	0.00	2017/05/23 19:00:00 MIN 5
107	0.00	2017/05/23 18:55:00 MIN 5
108	0.00	2017/05/23 18:50:00 MIN 5
109	0.00	2017/05/23 18:45:00 MIN 5
110	0.00	2017/05/23 18:40:00 MIN 5
111	0.00	2017/05/23 18:35:00 MIN 5
112	0.00	2017/05/23 18:30:00 MIN 5
113	0.00	2017/05/23 18:25:00 MIN 5
114	0.00	2017/05/23 18:20:00 MIN 5
115	0.00	2017/05/23 18:15:00 MIN 5
116	0.00	2017/05/23 18:10:00 MIN 5
117	0.00	2017/05/23 18:05:00 MIN 5
118	0.00	2017/05/23 18:00:00 MIN 5
119	0.00	2017/05/23 17:55:00 MIN 5
120	0.00	2017/05/23 17:50:48 MIN 4 SEC 12

NO. OF ENTRIES: 240		
=====		

memory-allocation-failure-rate

Syntax	memory-allocation-failure-rate <i>mda</i> [history-stats-in-count <i>count</i>] [history-stats-in-min <i>minutes</i>] [current] [show-oid]
Context	show>isa>stats>tunnel-isa
Description	This command displays memory allocation failure rate of the specified ISA. The system collects usage information every hour for last 24 hours. The output also includes a current value.
Parameters	<i>mda</i> — Displays information about the specified ISA. Values slot/mda <i>count</i> — Displays information for the number of statistics intervals to be displayed (starting with the most recent). Values 1 to 24 <i>minutes</i> — Displays information about the specified period covered by the statistics to be displayed (starting with the most recent). Values 1 to 1440 current — Displays information about the current statistic value. The values of count and minutes are ignored by the system once this parameter is specified. show-oid — Displays information about the Object Identifier (OID) of the current statistical value.

Output The following is an example output of the **show isa stats tunnel-isa memory-allocation-failure-rate** configuration.

Sample Output

```
show>isa>stats>tunnel-isa# memory-allocation-failure-rate 1/2
=====
STATISTICS FOR ISA 1/2
=====
INDEX          VALUE          START TIME          SAMPLING DURATION
-----
ISA MEMORY ALLOCATION FAILURE RATE (FAILURES/HOUR)
1 (CURRENT)    0          2017/05/24 03:00:00 MIN 47 SEC 47
2              0          2017/05/24 02:00:00 HRS 1
3              0          2017/05/24 01:00:00 HRS 1
4              0          2017/05/24 00:00:00 HRS 1
5              0          2017/05/23 23:00:00 HRS 1
6              0          2017/05/23 22:00:00 HRS 1
7              0          2017/05/23 21:00:00 HRS 1
8              0          2017/05/23 20:00:00 HRS 1
9              0          2017/05/23 19:00:00 HRS 1
10             0          2017/05/23 18:00:00 HRS 1
11             0          2017/05/23 17:50:48 MIN 9 SEC 12
-----
NO. OF ENTRIES: 11
=====
```

4.14.2.18 Debug Commands

gateway

Syntax	gateway name name tunnel ip-address[:port] [nat-ip nat-ip[:port]] [detail] [no-dpd-debug] [display-keys] no gateway name name tunnel ip-address[:port] [nat-ip nat-ip[:port]] gateway name name tunnel-subnet ip-prefix/ip-prefix-length [port port] [detail] [no-dpd-debug] [display-keys] no gateway name name tunnel-subnet ip-prefix/ip-prefix-length
Context	debug>ipsec
Description	This command enables debugging for dynamic IPsec tunnels that terminate on the specified IPsec gateway. The tunnel to be debugged can be specified by either its source address or source subnet. If a subnet is specified, the system will enable debugging for all tunnels with source addresses in the specified subnet.
Parameters	<i>name</i> — The name of the IPsec gateway up to 32 characters.

- ip-address:port* — The tunnel IP address of the remote peer and, optionally, the remote UDP port of IKE.
- nat-ip:port* — The inside IP address of the NAT tunnel and, optionally, the port.
- detail** — Specifies to display detailed debug information.
- no-dpd-debug** — Specifies to stop logging IKEv1 and IKEv2 DPD events during debug in order to produce less noise.
- ip-prefix/ip-prefix-length* — The subnet of the peer's tunnel address.
- display-keys** — Specifies the IKE-SA and CHILD-SA keys for inclusion in the debug output.

tunnel

Syntax	tunnel <i>ipsec-tunnel-name</i> [detail] [no-dpd-debug] [display-keys] no tunnel <i>ipsec-tunnel-name</i>
Context	debug>ipsec
Description	This command enables debugging for specified IPsec tunnel.



Note: Up to 16 IPsec tunnels are allowed, to enable debugging, at a time.

Parameters	<i>ipsec-tunnel-name</i> — Specifies the name of ipsec-tunnel, up to 32 characters. detail — Displays detailed debug information. no-dpd-debug — Stops logging IKEv1 and IKEv2 DPD events for less noise during debug. display-keys — Specifies the IKE-SA and CHILD-SA keys for inclusion in the debug output.

certificate

Syntax	certificate
Context	debug
Description	This command enables debug for certificate chain computation in cert-profile.

auto-crl-updates

Syntax	[no] auto-crl-updates
Context	debug>certificate
Description	This command enables trace for automated and manual CRL updates.

ca-profile

Syntax	[no] ca-profile <i>profile-name</i>
Context	debug>certificate>auto-crl-updates debug>certificate>cmpv2 debug>certificate>ocsp
Description	This command debugs output of the specified CA profile. • Protection method of each message is logged. • All HTTP messages are logged. Format allows offline analysis using Wireshark. • In the event of failed transactions, saved certificates are not deleted from file system for further debug and analysis. • The system allows CMPv2 debugging for multiple ca-profile at the same time.
Parameters	<i>profile-name</i> — Specifies the name of the CA profile, up to 32 characters.

cmpv2

Syntax	[no] cmpv2
Context	debug>certificate
Description	This command enables the context to perform CMPv2 operations.

ocsp

Syntax	[no] ocsp
Context	debug>certificate
Description	This command enables debug output of OCSP protocol for the specified CA.
Default	no ocsp

certificate

Syntax	certificate <i>filename</i>
Context	debug>ipsec
Description	This command enables debug for certificate chain computation in cert-profile.
Parameters	<i>filename</i> — Displays the filename of imported certificate, up to 95 characters.

client-db

Syntax	[no] no client-db <i>db-name</i>
Context	debug>ipsec
Description	This command enables debugging for the specified IPsec client-db.
Parameters	<i>db-name</i> — Specifies the IPsec client database name, up to 32 characters.

4.14.2.19 Tools Commands

stats

Syntax	stats
Context	tools>dump>ipsec
Description	This command enables the context do dump ipsec statistics.

ike-stats

Syntax	ike-stats gateway <i>name</i> [dynamic-tunnel <i>ip-address:port</i>] ike-stats isa <i>mda</i> ike-stats ipsec-tunnel-name
Context	tools>dump>ipsec>stats
Description	This command dumps various internal IKE statistics for the specified scope: • per ISA • per static LAN-to-LAN tunnel • per dynamic tunnel

The start time indicates the time of the last reset.

- Parameters**
- name* — Dumps information about the name of the IPsec GW, up to 32 characters.
 - ip-address:port* — Dumps information about the IP address and port of the peer for dynamic tunneling.
 - mda* — Dumps information about the specified ISA.
- Values** slot/mda
- ipsec-tunnel-name* — Dumps the name of the static LAN-to-LAN tunnel, up to 32 characters.

mc-ipsec

- Syntax** **mc-ipsec**
- Context** tools>perform>redundancy>multi-chassis
- Description** This command enables the 7750 SR mc-ipsec context.

force-switchover

- Syntax** **force-switchover tunnel-group** *local-group-id* [**now**] [**to {master | standby}**]
- Context** tools>perform>redundancy>multi-chassis>mc-ipsec
- Description** This command manually switches over the 7750 SR mc-ipsec mastership of specified tunnel-group.
- Parameters**
- local-group-id* — Specifies the local tunnel-group id configured in the **config>redundancy>multi-chassis>peer>mc-ipsec** context.
 - now** — This optional parameter removes the prompt of confirmation.
 - to {master | standby}** — specifies the desired mastership state to be achieved following a forced switch between this tunnel group and its redundant peer. If the target state matches the current state when the switch is attempted, then no switch will occur.

client-db

- Syntax**
- client-db** *db-name* **lookup peer-ip** *peer-ip-address*
 - client-db** *db-name* **lookup idi string-type** {fqdn | rfc822} *string-value* *string-value* [**peer-ip** *peer-ip-address*]
 - client-db** *db-name* **lookup idi address** *idi-ip-address* [**peer-ip** *peer-ip-address*]
- Context** tools>perform>ipsec

Description This command performs a lookup in the specified client-db by using specified input and displays the matching result.

Sample Output

```
tools perform ipsec client-db "test" lookup idi string-type rfc822 string-
value client-1@examplebm.com peer-ip 10.10.10.100
Result                : Ok
Database              : test
Criterion - Ike Idi   : RFC822 "client-1@examplebm.com"
Criterion - Peer IP   : 10.10.10.100
Matched Record       : 1 "client-1"
Elapsed Time (us)    : 2
```

Parameters *db-name* — Specifies the name of the client-db.

peer-ip *peer-ip-address* — Specifies the peer's tunnel IP address as input, either v4 or v6.

string-type — Specifies the peer's IDi as input.

Values fqdn, rfc822

idi-ip-address — Specifies the peer's IDi of address type as input, either v4 or v6

string-value *string-value* — Specifies the value of FQDN or RFC822 IDi.

ike-initiate

Syntax **ike-initiate tunnel-group-id** *ipsec-group-id*
ike-initiate tunnel-name *ipsec-tunnel-name*

Context tools>perform>ipsec

Description This command initiates tunnel setup for the specified LAN-to-LAN tunnel or for all static LAN-to-LAN tunnels in the specified tunnel group. This command initiates tunnel setup regardless of the configuration of the ipsec-responder-only command under the specified tunnel group.

The command only initiates tunnel setup when the tunnel group is in the MC-IPsec master state, or if MC-IPsec is not enabled for the tunnel group. If MC-IPsec is enabled and the tunnel group is not in the master state, the system will abort tunnel setup if MIMP goes down or if mastership changes during the tunnel setup.

Operationally up tunnels are not affected by this command. The system will not try to initiate a tunnel setup if the tunnel's operation flags are not clear.

The system does not automatically retry tunnel setup if a tunnel setup fails.

Parameters *ipsec-group-id* — The ID of the tunnel group where all static LAN-to-LAN tunnels are initiated.

ipsec-tunnel-name — The name of the IPsec tunnel to be initiated.

4.14.2.20 Clear Commands

gateway

Syntax	gateway name <i>name</i> tunnel <i>ip-address:port</i> [statistics] [saved-key] gateway name <i>name</i> tunnel <i>ip-address:port</i> gateway name <i>name</i> [saved-key] gateway name <i>name</i> tunnel <i>ip-address:port</i> [saved-key]															
Context	clear>ipsec															
Description	This command clears dynamic IPsec tunnel states. The system will clear the stats counter for the specified tunnel when the statistics parameter option is specified. The system will clear the saved IKE and ESP keys for the specified tunnel, or for all tunnels on the specified gateway if no tunnel is specified when the saved-key parameter option is specified. The system will remove the specified tunnel when the statistics or saved-key parameters are not specified.															
Parameters	<i>name</i> — Specifies the name of the IPsec GW up to 32 characters. <i>ip-address</i> — Specifies the IP address and port of the remote peer. Values <table><tr><td><ip-address></td><td>ip-address</td><td>a.b.c.d</td></tr><tr><td></td><td>ipv6-address</td><td>x::x::x::x::x::x</td></tr><tr><td></td><td></td><td>x::x::x::x::x::d.d.d.d</td></tr><tr><td></td><td></td><td>x - [0 to FFFF]H</td></tr><tr><td></td><td></td><td>d - [0 to 255]D</td></tr></table> <i>port</i> — The port of the remote peer. Values 0 to 65535 statistics — Clears the stats counter. saved-key — Removes the saved IKE and ESP keys.	<ip-address>	ip-address	a.b.c.d		ipv6-address	x::x::x::x::x::x			x::x::x::x::x::d.d.d.d			x - [0 to FFFF]H			d - [0 to 255]D
<ip-address>	ip-address	a.b.c.d														
	ipv6-address	x::x::x::x::x::x														
		x::x::x::x::x::d.d.d.d														
		x - [0 to FFFF]H														
		d - [0 to 255]D														

lockout

Syntax	lockout router <i>router-id</i> lockout router <i>router-id</i> local-gateway-address <i>local-gateway-address</i>

lockout router *router-id* **local-gateway-address** *local-gateway-address* **remote** *ip-address[:port]*

Context	clear>ipsec
Description	This command clears the lockout state for the specified clients. If remote address information is not specified, the system will clear the lockout state for all clients within the specified routing instance, along with all clients within the specified IPsec gateway if <i>local-gateway-address</i> is specified.
Parameters	<i>router-id</i> — The ID of the router where the IPsec gateway is configured. <i>local-gateway-address</i> — The IP address of the local IPsec gateway. <i>ip-address</i> — The IP address of the remote client. <i>port</i> — The port of the remote client.

stats

Syntax	stats
Context	clear>ipsec
Description	This command enables the context to clear IKE statistics.

ike-stats

Syntax	ike-stats gateway <i>name</i> [dynamic-tunnel <i>ip-address:port</i>] ike-stats isa <i>mda</i> ike-stats ipsec-tunnel-name
Context	clear>ipsec>stats
Description	This command clears various internal IKE statistics for the specified scope: • per ISA • per static LAN-to-LAN tunnel • per dynamic tunnel The start time indicates the time of the last reset.
Parameters	<i>name</i> — Clears information about the name of the IPsec GW up to 32 characters. <i>ip-address:port</i> — Clears information about the IP address and port of the peer for dynamic tunneling. <i>mda</i> — Clears information about the specified ISA. Values slot/mda

ipsec-tunnel-name — Clears the name of the static LAN-to-LAN tunnel up to 32 characters.

tunnel

Syntax	tunnel <i>ipsec-tunnel-name</i> tunnel <i>ipsec-tunnel-name</i> [saved-key] tunnel <i>ipsec-tunnel-name</i> [stats] [saved-key] tunnel isa <i>mda</i> [saved-key]
Context	clear>ipsec
Description	This command clears static IPsec tunnel states. The system will clear the stats counter for the specified tunnel when the stats parameter option is specified. The system will clear the saved IKE and ESP keys for the specified tunnel, when the saved-key parameter option is specified. The system will remove the specified tunnel when the stats or saved-key parameters are not specified.
Parameters	<i>ipsec-tunnel-name</i> — Specifies the name of the IPsec tunnel up to 32 characters. saved-key — Removes the saved IKE and ESP keys. stats — Clears the stats counter. <i>mda</i> — Clear all static tunnels terminated on the specified ISA.

4.14.2.21 Admin Commands

display-key

Syntax	display-key type {ike esp} gateway name <i>name</i> dynamic-tunnel <i>ip-address:port</i> display-key type {ike esp} tunnel <i>ipsec-tunnel-name</i>
Context	admin>ipsec
Description	This command displays existing IKE-SA or CHILD-SA keys. .



Note: This command does not work if **config>ipsec>no show-ipsec-keys** or **no max-history-{esp|ike}-key-records** is configured under corresponding **ipsec-gw** or **ipsec-tunnel**.

Parameters *name* — The name, up to 32 characters.
ip-address — The IP address of the remote client.

Values

<ip-address>	ip-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x
		x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D

port — The port of the remote client.

Values 0 to 65535

ipsec-tunnel-name — The IPsec tunnel name, up to 32 characters.

Output The following outputs are examples of the **admin ipsec display-key** command.

Sample Output

```
admin ipsec display-key type ike gateway name "rw" dynamic-tunnel 11.1.1.100:500
=====
IKE-SA history: max-num-records 3 current-num-saved-records 1
                local: 172.16.100.1 remote: 11.1.1.100
record [0]: established time: 01/25/2018 20:51:55
  Initiator-SPI: d67ac71d73656496 Responder-SPI: d67ac71d73656496 Ike Version: 2
  SK_er: aes128, len: 16, val: a5dalc57f09a7eb7dbe9526cd52e2189
  SK_ar: sha1, len: 20, val: c11797bb8ebe5a1fadb46363bf5e763552bb45d0
  SK_ei: aes128, len: 16, val: 467124009cc577a8b23882a81ab9df70
  SK_ai: sha1, len: 20, val: 7dfef89bad31cb72d1ca8da2c04a9521993c7f9
```

Sample Output

```
admin ipsec display-key type esp gateway name "rw" dynamic-
tunnel 11.1.1.100:500
ESP-SA history: max-num-records 48 current-num-saved-records 2dynamic-
tunnel 11.1.1.100:500
                local: 172.16.100.1 remote: 11.1.1.100
record [0]: established time: 01/25/2018 20:54:56
  InSpi: 154532(0x00025ba4)
    encr-alg: aes128 len: 16 val: 0xd26aa32d8bd328b1e8332fa5c7b5eeaa
    auth-alg: sha1 len: 20 val: 0x0b37ddb824a43921d3b0ee81a6910eed065a9845
  OutSpi: 3286259439(0xc3e056ef)
    encr-alg: aes128 len: 16 val: 0x3acd95376ce04fcded2e0c80cc4289cf
    alg: sha1 len: 20 val: 0x9f5a46b5cdc572972b44cddb36b5f824ab060634
record [1]: established time: 01/25/2018 20:51:55
```

```
InSpi: 261186(0x0003fc42)
      encr-alg: aes128 len: 16 val: 0x8bf97675d37de3e3f6e634e3e11fc3aa
      auth-alg: sha1 len: 20 val: 0xf10c0f0821488cc14f8715cc323441fc967a79dd
OutSpi: 3246917342(0xc18806de)
      encr-alg: aes128 len: 16 val: 0xf36aaaa7a3a09734fe4fc6cd0ac9043e
      alg: sha1 len: 20 val: 0x40c13a444e4fb1d42a13812f70b17041ed0f56ee
```

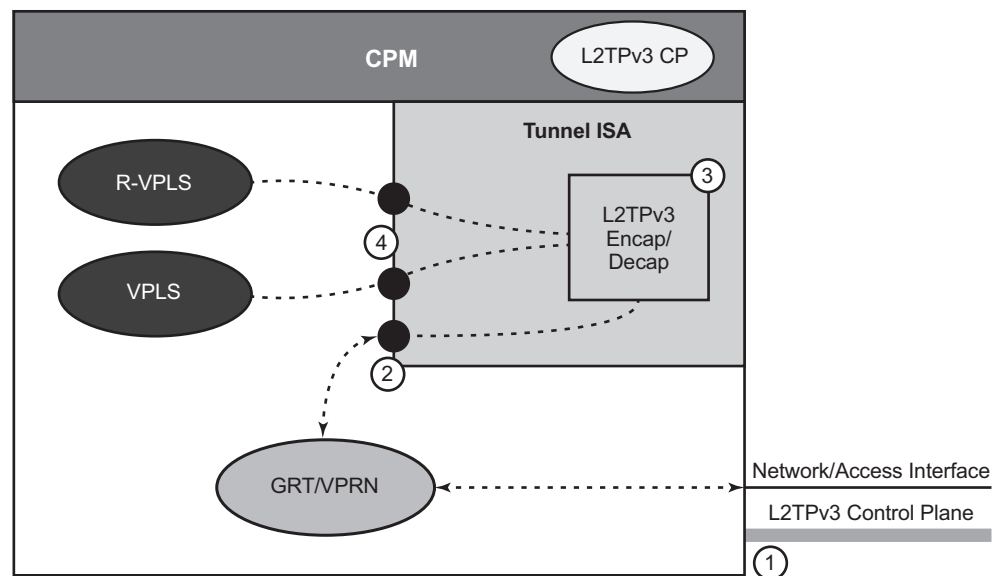

5 L2TPV3 Tunnels

5.1 L2TPv3 Overview

Layer 2 Tunneling Protocol version 3 (L2TPv3) is a mechanism for the tunneling of Ethernet traffic over an IP network. For this application, the MS-ISA/MS-ISA2 functions as a resource module for the system, performing the L2TPv3 encapsulation and decapsulation functions.

Figure 44 shows L2TPv3 support for the IP transport model. Table 30 describes the tunnel processing steps in the figure.

Figure 44 L2TPv3 Support for IP Transport



1037

Table 30 L2TPv3 Support for IP Transport — Tunnel Processing Steps

Step Number	Description
1	The L2TPv3 control plane can run within either the base routing or VPRN contexts.
2	L2TPv3 encapsulated packets ingress and egress through the public interface, which can be in either the base routing or VPRN contexts.

Table 30 L2TPv3 Support for IP Transport — Tunnel Processing Steps

Step Number	Description
3	L2TPv3 encapsulation and decapsulation processing is handled within the tunnel ISA.
4	Unencapsulated packets pass between the tunnel ISA and the associated service via the configured private SAP.

5.2 Control Plane

The configuration of the L2TPv3 control plane is similar to that of L2TPv2. A number of the same commands are used for both, but there are new commands specific to L2TPv3. The L2TPv3-specific commands are located in a separate L2TPv3 context in both the general configuration area as well as within the group configuration context.

L2TPv3 control plane parameters can be configured at either the global level within the **config>router>l2tp** context, which may include some L2TPv3-specific parameters. This should be used for parameters that are the same for the majority of L2TPv3 tunnels. The same parameters can be configured on a per-tunnel group basis. The tunnel group can be configured within either the base router context or a VPRN service context. The following is a simple example for an L2TPv3 tunnel group configured within the base routing context.

CLI Syntax:

```
configure
router
l2tp
l2tpv3
    cookie-length 8
    digest-type sha1
    nonce-length 64
    transport-type ip
    exit
group "base l2tpv3 left" protocol v3draft
create
    avp-hiding never
    eth-tunnel
        reconnect-timeout 60
    exit
l2tpv3
    pw-cap-list ethernet ethernet-
        vlan
```

```
password "AbkdpF.rY1FgcK4qAYmim
sykdmwbAucq" hash2
exit
password "rhXAlJTUjuliBn8lVUf
KJywztX9cKOEb/rbWUR/e4ow" hash2
tunnel "base l2tpv3 tunnel" create
local-address 172.16.0.100
peer 192.168.0.100
no shutdown
exit
no shutdown
exit
```

5.3 Public SAP

The public SAP is the access interface to the L2TPv3 tunnel over which encapsulated traffic is sent to or received from the far end. The IP address bound to this SAP is on the same subnet as the local L2TPv3 tunnel endpoint.

The public SAP must be configured in the same routing context as the L2TPv3 tunnel group configuration. As shown in [Figure 44](#), the public SAP can be associated with an IES or VPRN service to connect to the outside or public access network.

Below is a simple example for an L2TPv3 public SAP configured within the base routing context.

CLI Syntax:

```
configure
service
ies 10
interface "l2tp-public-interface" create
address 172.16.0.1/24
sap tunnel-1.public:2 create
exit
exit
```

5.4 Private SAP

The private SAP is the access interface to the L2TPv3 over which unencapsulated traffic is sent to or received from the far end. The public SAP must be configured within an Ethernet service, such as an Epipe, VPLS, or I-VPLS service.

The private SAP configuration includes the configuration of the following L2TPv3 session parameters:

- VC-ID
- PW-Type
- L2TPv3 tunnel group association

Below is a simple example for an L2TPv3 private SAP configured within the base routing context.

CLI Syntax:

```
configure
service
    vpls 100 customer 1 create
    ...
        sap tunnel-1.private:100 create
            l2tpv3-session create
                router 2 group "base l2tpv3
                    left"
                vc-id 100
                pw-type ethernet
                no shutdown
                exit
            no shutdown
        exit
    no shutdown
exit
```


6 Video Services

6.1 Video Services

6.1.1 Video Groups

The MS-ISA, MS-ISA2, and MS-ISM (2 MS-ISA2 on a single line card) support video service. These three MS-ISA variants are referred to as MS-ISAs in this section. The MS-ISA2 (IMM ISA2 variants and ISM) only supports FCC/RET and VQM functionality. When configured in the router, MS-ISAs are logically grouped into video groups for video services. A video group allows a maximum of four MS-ISAs to be treated as a single logical entity for a given application where the system performs a load balancing function when assigning tasks to a member of the group. It is not recommended to mix MS-ISA and MS-ISA2 within the same video group. All video group members are active members, so there is no concept of a “standby” MS-ISA. There can be a maximum of six MS-ISAs within a chassis for the video application.

Video groups provide a redundancy mechanism to guard against hardware failure within a group where the system will automatically re-balance tasks to the group excluding the failed MS-ISA. Video groups also pool the processing capacity of all the group members and will increase the application throughput because of the increased packet processing capability of the group. The buffer usage is typically identical for all members of the video group, so increasing the number of members in a group will not increase the scaling numbers for parameters bounded by available buffering, but there will still be the increase in performance gained from the pooled packet processor capacity. A video service must be enabled at the video group level before that service can be used.

A maximum of six MS-ISAs can be supported in a single video group. A given video application may restrict the number of members supported in a video group to a smaller number. Refer to specific sections in this guide for video application additional information.

A maximum of four video groups are supported in a router. There is a chassis limit of eight MS-ISAs per router which constrains the number and members of video groups.



Note: MS-ISA in a single video group cannot be on the same IOM. An IOM can accommodate two MS-ISA modules provided that the MS-ISA are members of different video groups.

6.1.2 Video SAP

The video group logically interfaces to a service instance with a video Service Access Point (SAP). Like a SAP for connectivity services, the video SAP allows the assignment of an ingress and egress filter policy and QoS policy.

Ingress and egress directions for the filter and QoS policy are named based on the perspective of the router which is the opposite perspective of the ISA. An “egress” policy is one that applies to traffic egressing the router and ingressing the ISA. An “ingress” policy is one that applies to traffic ingressing the router and egressing the video. Although potentially confusing, the labeling of ingress and egress for the ISA policies was chosen so that existing policies for connectivity services can be reused on the ISA unchanged.

If no filter or QoS policy is configured, the default policies are used.

One of the key attributes of a video SAP is a video group association. The video SAP’s video group assignment is what determines which video group will service on that video SAP. The video groups configuration determines what video services are available.

6.1.3 Video Interface

A video interface is a logical IP interface associated with a video SAP and provide the IP addressing for a video SAP.

A video interface can have up to 16 IP addresses assigned in a Layer 3 service instance. A video interface can have only one IP address assigned in a Layer 2 service instance.

6.1.4 Multicast Information Policies

Multicast information policies on the 7750 SR and 7450 ESS serve multiple purposes. In the context of a service with video services, the multicast information policy assigned to the service provides configuration information for the multicast channels and defines video policy elements for a video interface.

This section describes the base elements of a multicast information policy in support of a video service. Specific video service features will require additional configuration in the multicast information policy which are described in the sections dedicated to the video feature.

Multicast information policies are named hierarchically structured policies composed of channel bundles which contain channels which contain source-overrides.

- Bundles are assigned a name and contain a collection of channels. Attributes not defined for a named bundle are inherited from the special default bundle named "default".

```
*A:ALA-48configmcast-mgmtmcast-info-plcy# info
-----
bundle "default" create
exit
-----
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

- Channels are ranges of IP multicast address identified by a start IP multicast address (Gstart) and optional end IP multicast address (Gend), so the channels encompasses (*,Gstart) through (*,Gend). A channel attribute is inherited from its bundle unless the attribute is explicitly assigned in which case the channel attribute takes precedence.
- A source-override within a channel are IP multicast addresses within the channel with a specific source IP address (Soverride), so the source-override encompass (Soverride,Gstart) through (Soverride,Gend). A source-override attribute is inherited from its channel unless the attribute is explicitly assigned in the source-override channel in which case the source-override channel attribute takes precedence.

For a given IP multicast channel (*,G) or (S,G), the most specific policy element in the hierarchy that matches applies to that channel.

A multicast information policy is assigned to a service instance. For video services, the multicast information policy assigned to the service determines the video group for a given IP multicast channel. When a channel is assigned to a video group, the channel is sent to the video group for buffering and/or processing as appropriate depending on the video services enabled on the video group. If no video group is assigned to a given channel, the channel will still be distributed within the service instance, but no video services will be available for that channel.

In addition to bundles, channels and source-overrides, multicast information policies also include video policies. Video policies define attributes for the video interfaces within the service instance.

Video policy attributes are specific to the video feature and will be covered in detail in the applicable video feature section. Video policies are mentioned here because they are an element of the multicast information policy and provide the link to configuration for a video interface.

6.1.5 Duplicate Stream Protection

While H-RET can protect against minor amounts of packet loss, it is limited in the number of packets that can be recovered (currently 32). This can be from approximately 125 ms of a 3 Mb/s stream to only 18 ms for a 20 Mb/s stream. These times are short for a network reconvergence event which will typically be in the order of 300-1200 ms. Further, retransmission will cause incremental bandwidth spikes in the network as the lost packets are sent to the client as quickly as possible.

Rather than invoke a retransmission event to protect against network interruption or reconvergence, it is often more efficient to protect the stream via an alternate transmission path. This can be a separate physical interface, transmission link, system or even technology.

Duplicate-stream protection allows an operator to split a single multicast stream (single S,G and common SSRC) into two different transmission paths that may have different transmission characteristics (latency/jitter). Rather than select one stream for retransmission to the client the Duplicate Stream protection feature evaluates each stream packet-by-packet, selecting the packet that first arrives (and is valid) for retransmission.

A circular buffer is used for duplicate-stream protection which incorporates both packet-by-packet selection (based on RTP sequence number/timestamp and SSRC) and a re-ordering function whereby any out-of-sequence packets will be placed into the buffer in order, thus creating a corrected, in-order stream.

Similar to the H-RET re-sequencing feature playout rate is a function in ingest rate, however because the two streams may be delayed between one-another a few assumptions are made:

- The first arriving packet is always put into the buffer, allowing for the backup medium to wander in terms of latency and jitter.
- Because the source is the same, the rate at which a packet is put into the buffer (from either stream) can be assumed to be the normal bitrate.

The output RTP stream is always maintained in-sequence and the playout speed is user-controlled. Either with constant-delay (i.e., packet ingress time + 500 ms = packet egress time) or can be a moving window average to smooth jitter that may occur between packets or the two contributing streams. The operator can specify the size of this window where zero (0) is a constant-delay.

The buffer size is similarly configurable and is the higher of the inter-stream phase (i.e., one stream ahead of another) or the expected jitter.

6.1.6 Duplicate Stream Selection

6.1.6.1 Stream Identification

Stream selection is a simple selection algorithm that is applicable to any number of input streams. It is a prerequisite for stream selection that RTPv2 encapsulation be used in UDP.

Each service is identified by multicast source, group/destination address and current synchronization source (SSRC). Once this has been identified, the ISA monitors its ingress for:

- Traffic with a DA of the multicast group, or;
- Traffic with a DA of the ISA (unicast)

Traffic is further checked as having RTP-in-UDP payload, RTP version 2.

The SSRC of each incoming RTP packet is learned as unique sources. Only one SSRC is supported for each stream, however as SSRC may change during abnormal situations (such as encoder failover), it can be updated.

A SSRC can only be updated when a Loss of Transport (LoT) occurs, as other duplicate streams (with the original SSRC) may still be operational. When an LoT occurs the SSRC is deleted, the buffers are purged and the RTP sequence counters are reset. The SSRC will be extracted from the next valid RTP packet and the sequence will start over.

Individual streams are not tracked by the ISA. There may be one, two, or ten duplicate streams, the number is of no consequence to the selection algorithm (however bandwidth and/or video quality monitoring (VQM) may be impacted). Irrespective of the number of duplicate streams, one RTP packet is selected for insertion into the video ISA buffer. Once a packet is selected the RTP sequence counter is incremented and any further RTP packets received by the ISA with the previous sequence number are discarded.

In summary, duplicate stream selection is a FIFO algorithm for RTP packet selection, this is considered optimal because:

- All stream sources are identical, thus for any given sequence number the payload should also be identical.
- Most bit errors should be detected by the CRC-32 algorithm applied to Ethernet, SDH, ATM, etc. These devices will typically discard frames where bit errors occur with the net result being the video ISA will receive a bit error-free stream (though packet loss may/does occur).

- UDP checksum is verified by the video ISA (after input VQM) and any failures result in a silent discard of the packet.

6.1.6.2 Initial Sequence Identification

When a service is defined and is enabled (**no shutdown**), the video ISA will monitor for valid RTP packets and on first receipt of a valid RTP packet learn the following information:

- SSRC
- Sequence number
- Timestamp (as timestamp is profile-specific, MPEG2-TS are assumed)

The packet will be inserted into the video ISA playout buffer associated with that particular service and playout when directed (playout algorithm).

6.1.6.3 Packet Selection

For each valid RTP packet received for a given service will be inserted into the buffer if there is no existing RTP packet that matches the sequence number. Because sequence number and timestamp discontinuities may occur the video ISA makes a limited attempt at validating either as they are not required for MPEG. The video ISA code adopts a philosophy that for the most part sequence number and timestamp increment correctly, but should they prove to be non-contiguous, the packet selection algorithm adapts.

Duplicate packets are detected by sequence number (or timestamp unless M-bit reset it), so should a packet already exist in the buffer with the same sequence number as one received (or one recently played out) it will be discarded. For the purpose of determining recent playout if an incoming sequence number is within 6.25% (- 4096) the packet is considered late and is discarded.

In a multiprogram transport stream (MPTS) timestamp is set uniquely for every RTP packet, this is because any RTP packet may contain a number of multiplexed elementary streams. As a result playout is based on the embedded timestamp in each RTP packet. In a single-program transport stream the inverse occurs, many RTP packets can share the same timestamp as it is referenced from the start of picture (and a picture can span many RTP packets). As a SPTS does not contain audio its application is limited to content production and so only MPTS are supported.

Timestamp discontinuities do occur and are normally represented with the Marker bit (M) being set.

Playout time is determined by an internal playout timestamp. The playout timestamp is set independently from the actual timestamp in the packet. The recovered clock is used to determine expected timestamp for every incoming RTP packet.

When a packet is received it is first compared to existing packets in the buffer based on sequence number (assuming here that a stream may be delay hundreds of milliseconds by a backup path yet still be valid); only if this packet is determined to be new RTP packet eligible for buffer insertion will jitter tolerance be evaluated. If jitter tolerance is exceeded then a timestamp discontinuity is assumed and instead of setting playout timestamp based on the contained RTP timestamp, the actual received time (offset by playout-buffer) is set for the RTP packet playout timestamp.

In normal operation clock is recovered from the timestamp field in the RTP header, is offset by the playout buffer configuration parameter and used to schedule playout of the packet. The playout clock is synchronized with the sender by using an adaptive clock recovery algorithm to correct for wander.

Algorithm summary

- Is the service marked LoT — If a loss of transport occurred, purge the buffer and reset all counters/timers.
- If the service is UP, check the RTP packet sequence number. Compare to sequence numbers contained in the buffer. If no match then check last played sequence number. If the sequence number of this packet is between last played and last played + 4096 then consider this packet late and discard.
- Check the expected timestamp recovered clock value and compare to RTP timestamp: If the expected timestamp is $(-ve)jitter\ tolerance < timestamp < (+ve)jitter\ tolerance$ then the packet is admitted to the buffer with a playout timestamp per the embedded RTP timestamp. If jitter tolerance is not maintained this marks a discontinuity event. Set playout timestamp to current clock + playout buffer and enqueue.

6.1.6.4 Clock Recovery

RFC 2250, *RTP Payload Format for MPEG1/MPEG2 Video*, defines the timestamp format for MPEG2 video streams (which may carry H.264 video): a 90kHz clock referenced to the PCR. Each ingest RTP packet has it's timestamp inspected and it is used in an adaptive clock recovery algorithm. Importantly, these adjustments occur on ingress (not on playout). This serves as a long-term, stable, ingress stream recovered clock.

The 90kHz ingress stream recovered clock is adjusted for each service to account for the encoder's reference clock/difference between the clock in the 7750 SR. This input timestamp is derived from the same RTP packet that is inserted into the buffer, and thus may be subjected to significant jitter. The clock adjustment algorithm must only adjust clock in extremely small increments (in the order of microseconds) over a very long sample period (not bitrate) of at least 30 minutes.

6.1.6.5 Playout

Playout is the process of regenerating the stream based on playout timestamp.

For each service the operator defines a fixed playout buffer. This serves as an exact offset to the ingress stream recovered clock and serves as playout time for the video ISA. Because timestamp is used for buffer playout, CBR, capped VBR and VBR streams are all supported without pre-configuration. The playout buffer mechanism effectively removes network-induced jitter and restores the output to the rate of the original encoder.

6.1.6.6 Loss of Transport

In the circumstance that the playout buffer is emptied an LoT is indicated. The video ISA will reset playout timestamp, clock, sequence number, etc., on this event and await the next valid RTP packet for this service.

6.1.7 Video Quality Monitoring

The following terminology is used in this section:

- TNC: Technically non-conformant
- QoS: Quality of Service
- POA: Program Off Air
- TNC event (also known as Impaired event) — A trap/alarm that an impairment event is detected and is termed as TNC. An impaired event is said to have occurred if:
 - PAT/PMT Syntax error occurs in that second
 - Continuity counter errors were detected

- PAT /PMT/PCR PIDs were not present in the video stream for a time period equal to or greater than the configured TNC value in the respective alarm.
The default value of the impaired threshold in terms of milliseconds is:
 - PAT : 100 ms
 - PCR : 100 ms
 - PMT : 400 ms
- an unreferenced PID is seen in the video stream which has not been referred in the PMT
- TNC seconds (Impaired seconds) — The number of seconds an impaired event was detected before a TNC SNMP trap was sent. Although multiple TNC events may have occurred within a second, counters in the **show>video>channel>analyzer** command only increment once per second.
- QoS event (also known as Degraded event) — A trap/alarm that a degraded event is detected and is termed as QoS.
A QoS event is said to have occurred if:
 - Absence of PAT/PMT/PCR PIDs in the video stream for a time period equal to or greater than the configured QoS value in their respective alarms.
The default value of the degraded threshold in terms of milliseconds is:
 - PAT : 200 ms
 - PCR : 200 ms
 - PMT : 800 ms
- QoS seconds (Degraded seconds) — The number of seconds a degraded event was detected before a QoS SNMP trap was sent. Although multiple QoS events may have occurred within a second, counters in the **show>video>channel>analyzer** command only increment once per second.
- POA event (Error event) — A trap/alarm that an error event is detected and is termed as POA.
- A POA event has occurred if:
 - a synchronization loss error has occurred for that particular second. A synchronization loss is said to have occurred if more than 1 consecutive synchronization byte error is seen in the stream.
 - Absence of PAT/PMT/PCR PIDs in the video stream for a time period equal to or greater than the configured POA value.
The default value of the degraded threshold in terms of milliseconds is:
 - PAT : 500 ms
 - PCR : 500 ms
 - PMT : 2000 ms
 - Traffic loss has occurred for that particular second.

- A transport error indicator or TEI indicator is set in the transport stream packet header for that particular second in the video stream.
- POA seconds (Error seconds) — The number of seconds an errored event was detected before a POA SNMP trap was sent. Although multiple POA events may have occurred within a second, counters in the **show>video>channel>analyzer** command only increment once per second.
- Good seconds — The number of seconds where there are no impaired, degraded, or error events.

PID Stats:

- PID: Displays the value of the PID.
- Is PCR PID : Can be set to Yes or No. If set to Yes, then it indicates that the PID is the PCR PID.
- TEI Err Sec : Counts the number of seconds TEI was set for that particular PID.
- Absent Err Secs: The number of seconds for which the PID was not seen for a particular interval of time which is decided by the alarms set for the Non-Vid PID Absent and Video PID Absent.
- PID bitrate: Calculated by counting the number of times the PID occurred in the last second x 188 x 8.
 - 188 = TS packet size
 - 8 = Number of bits in a byte
- CC Err Secs: Number of seconds Continuity Counter errors were seen for that particular PID in the stream.
- PID Type: Specifies that the PID is either video, audio, PAT, PMT, or PCR.
- MPEG Stream Type: If the PID is video or audio, this field indicates how the video or audio is encoded.

For example:

- For video : H.265, H.264, or MPEG2 (only the decimal equivalent defined by the MPEG standard is displayed and not the string)
- For Audio : E-AC3, DTS-HD, AC-3, or MPEG-2 (only the decimal equivalent defined by the MPEG standard is displayed and not the string)

Interval Statistics

- Except for the PID statistics all other statistics explained above have interval statistics. Information can be obtained about stream status for the last 1 minute, 5 minute, and 15 minute interval.

MDI - Media Delivery Index (RFC 4445, *A Proposed Media Delivery Index (MDI)*)

- Delay Factor (RFC 4445) — The delay factor is a value which indicates the minimum amount of time a STB buffers to resolve network jitter (i.e., it is the minimum STB buffer depth in ms). RTP timestamp will be used as the definitive time indicator (the notional drain rate).
- Loss Rate (RFC 4445) — The Media Loss Rate is the number of media (Transport Stream) packets lost over a certain time interval. This is reported in TS/sec. Each RTP packet lost is assumed to have 7 TS packets lost.
- In absence of traffic MDI values will be reported as N/A. These stats are reported over current (current second) , 1 minute, 5 minutes and 15 minutes intervals

In many instances IPTV operators are unable to identify the cause of visual impairments which are present in almost every video distribution network because the IPTV network has so many moving parts While head end transport-stream monitoring; full reference video analysis (comparing the source content to the encoded output), and; STB probes allow an operator to establish whether the contribution source, the encoder, or the network is the problem the network is a very complex thing.

Operators can use another measurement point in the network, just prior to the last mile such that network faults can be characterized as being between the head end and last mile (transport) or in the last-mile itself.

The multicast video quality monitoring solution provides an inspection point for the multicast video stream that is combined with other analysis methods to create a full view of video issues and help troubleshoot the part of the network causing the issue.

Video quality monitoring is one part of a video assurance program and is combined with:

- TS analysis on the encoder output (to detect encoder errors);
- Full-reference PSNR and PQR on the encoder output (to detect over-encoding, noise and other contribution or encoding artifacts)
- STB reporting (such as packet-loss, RET events, packet errors) from the entire STB population
- STB probes performing full-reference monitoring (against test streams)
- STB probes performing channel-change times, estimated PSNR, etc

Multicast video monitoring within the network can be positioned as complementary to STB reporting and head end analysis, and but should not attempt to perform either of these functions. Because the network node is not capable of decrypting a MPEG transport stream is primarily used to identify correctable and uncorrectable network errors, correlate them with network events (i.e., routing re-convergence, interface failure, etc.) and provide summary reports and alarms.

For operators who do not have existing STB probes or reporting, a network-based VQM solution can provide insight into quality issues the network may be contributing to, possibly reducing the amount of STB probe investment that is needed. (i.e., both probes and the 7750 SR VQM reports many of the same issues in terms of picture quality, fewer probes are needed to test channel change delay, etc).

The metrics which VQM can report are based on the use of RTP streams which provide per-packet sequencing and an indication of picture type. These two parameters along with measured bitrate allow VQM to produce estimated MOSv scores for both stream ingress (uncorrected) and stream egress (corrected) outputs.

Reportable metrics include:

- Relevant SCTE-143 error counters
 - PAT
 - PMT
 - PCR
 - Transport errors, etc
- ETSI TR 101 290
 - PID
 - SI repetition
 - Degraded blocks/intervals, etc
- MDI (RFC 4445)
- Forwarded and impaired I-/B-/P-frame counts
- GOP length
- Video/audio/stream bitrate

These metrics are collected per stream and have relevant parameters (such as profile and PIDs) pre-defined. These will be collected into a so-called stream ID. Reports (containing numeric metrics) and alarms (log, SNMP or syslog) can be generated.

For each group, reports contain:

- Stream ID (S,G / SSRC)
 - Stream A (ingress)
 - Statistics
 - Stream B (ingress)
 - Statistics
 - Output
 - Statistics

Event alarms are reported by log, syslog, or SNMP. The following is an example of a trap:

```
1 2017/02/11 18:11:20.42 UTC WARNING: VIDEO #2009 Base Video[1/video-300]
Service Id - 300, Video interface - video-300, Group address -
192.0.2.6, Source address -
10.20.13.2 Last 10 seconds of analyzer state is good good good good good good good good
good good poa
```

A trap is only raised when a POA, QoS, or TNC event occurs within the last 10 seconds. The trap captures events within the last 10 seconds. In the example above, the first nine seconds were “good”, which indicates that no events occurred and that every single RTP packet was received. At the 10-second mark, a POA event occurred, which triggered the SNMP trap. This sampling continues every 10 seconds. If an event (POA, QoS, or TNC) continues to be detected, an SNMP trap is raised every 10 seconds.

When the analyzer detects 10 seconds of a “good” condition, another trap is raised to clear the alarm for the multicast (S,G). Subsequent alarms are raised and SNMP traps are triggered only when the analyzer detects another event (POA, QoS, or TNC).

```
61 2016/10/18 15:40:56.83 UTC WARNING: VIDEO #2010 Base Video[1/video-300]

Analyzer state is cleared for - Service Id - 300, Video interface - video-
300, Group address - 192.0.2.6, Source address - 10.20.13.2
```

VQM is an optional module available on the input side, or output side of the video ISA. On input, it is applied prior to ad-insertion, H-RET, and duplicate stream protection. Conversely when on the output side it is applied only to multicast streams after ad-insertion, H-RET and duplicate stream protection.

Because of the large number of channels and the nature of measuring input and output sides, VQM is highly reliant on the use of RTP extensions to provide relevant transmission metrics to the VQM analysis module. In a typical head end a multicast stream will be scrambled to encrypt its video and/or audio. When this encryption occurs, it is typical for the entire payload of the transport stream (for the nominated PID) to be completely scrambled. The consequence of such is that the video and audio PES headers, which reveal much about the picture and timing information, are unavailable to the VQM program.

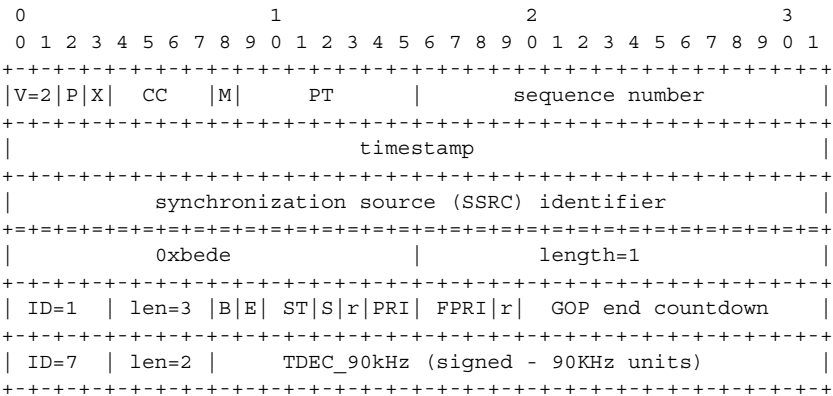
VQM utilizes intelligent RTP re-wrapping. RTP re-wrapping is a prerequisite for ad insertion and Fast Channel Change (FCC) and involves marking packets before encryption based on the picture type (most importantly, the start of the I frame of IDR frame in H.264).

The VSA as currently defined, re-multiplexes each transport stream into a new RTP packet. By doing so it allows the separation of different picture types into their own respective RTP packets, and the separation of audio packets from video packets to allow different synchronization in events of FCC. In effect, it pulls the elementary streams back into their component forms while retaining the syntax and structure of the MPTS.

For information about VSAs, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.

Meanwhile, additional information can be made available, prior to scrambling, of the picture information for quality analysis. The quality analysis performed by the VQM module emphasizes impairments caused by network issues and transport stream syntax given the relative proximity of the router to the customer.

When the video ISA is deployed alongside the ALU VSA re-wrapper, a custom RTP header extension is sent with each RTP packet. The RTP header is shown below.



Where:

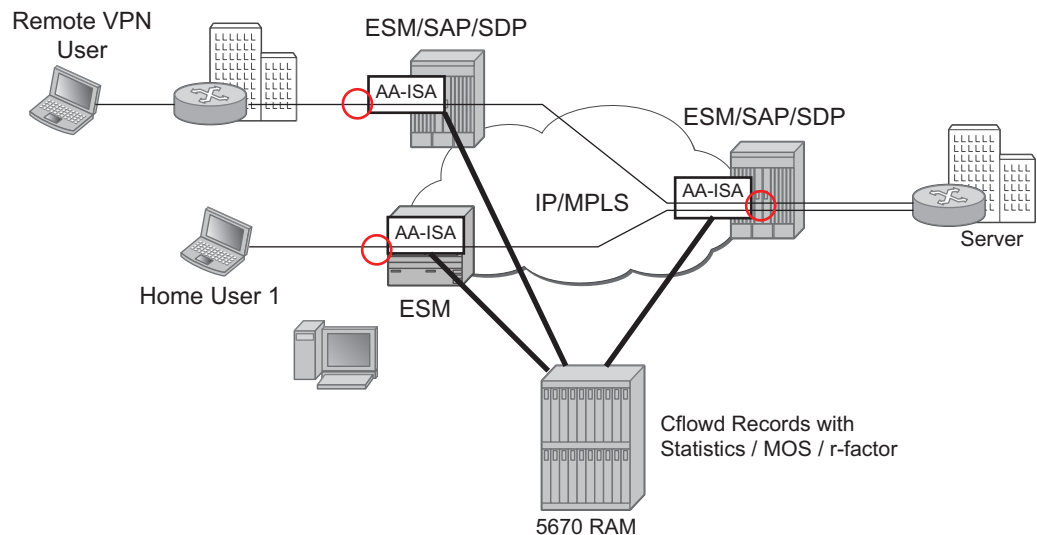
- B (Frame Begin Flag): set if a frame starts in this packet
- E (Frame End Flag): set if a frame finishes in this packet
- ST (Stream Type)
 - 00 video
 - 01 audio
 - 10 data/padd/other
 - 11 Reserved
- S (Switch bit): set to 1 in all RTP packets from the moment the client should do the IGMP join (rewrap does not fill it)
- r: reserved (set to 1)
- PRI: Packet Priority (coarse)
- FPRI: Fine-grained priority
- PRI FPRI dec DSCP
- --- ---
- 3 7 31 AF41 Video IDR frame
- 3 0 24 AF41 Audio
- 2 0 16 AF41 Reference frame (P in MPEG2, I or P or some Bs in AVC)
- 1 7 15 AF42 Non-reference frame (most Bs in MPEG2, some Bs in AVC)

1 5 13 AF42 Trans-GOP frames, undecodable in some circumstances (some Bs in MPEG2)
0 4 4 AF43 Rest of cases (data, secondary videos, etc)
0 1 1 AF43 Padding packets
where AF41=100010, AF42=100100, AF43=100110 (DSCP bits in the IP header)

6.1.7.1 VoIP/Video/Teleconferencing Performance Measurements

The feature provides ability to measure and provide statistics to allow reporting on voice and video quality for VoIP and teleconferencing (A/V) applications. A sampled deployment is shown in the picture below (Figure 45). Although a distributed model is shown, a hub-and spoke model, with AA-ISA deployed only on one side of the traffic flow, is also supported.

Figure 45 Voice/Video Monitoring Deployment Example



Because of network-based AA, the operator has an ability to monitor voice, video, teleconferencing applications for a given AA subscriber regardless of the type of that subscriber (a residential subscriber vs. a user of a business VPN service). AA-ISA monitors UDP/RTP/RTCP/SDP headers for each initiated call/application session (sampling may be provided – although, it is expected that a sampling rate will be smaller than that of TCP-applications due to the nature of the voice/video applications – longer lasting and smaller number of sessions/calls per subscriber). AA ISA gathers statistics and computes MOS-scores/R-factor results per each call/application session. At the end of a call (/application session closure), AA-ISA sends the statistics and computed scores to a Cflowd collector (the Cflowd infrastructure was introduced for TCP-performance but modified to carry voice/video specific data is used). The collector summarizes and presents the results to the operator/end user.

6.1.7.2 Mean Opinion Score (MOS) Performance Measurements Solution Architecture

AA-ISA integrates a third party MOS software stack to perform VoIP and video MOS measurements. This software provides:

- Call quality analysis using optimized ITU-T G.107
- Measurements of perceptual effects of burst packet loss and recency using ETSI TS 101 329-5 Annex E Extensions
- Measurements and analysis of RTCP XR (RFC3611) VoIP metrics payloads.

AA software monitors the associated SDP channel and passes codec information (when available) to the subsystem which monitors VoIP. The video bearer channels traffic generates a wide variety of A/V performance metrics such as:

- Call quality metrics
 - Listening and conversational quality MOS scores – MOS-LQ, MOS-CQ
 - Listening and conversational quality R-factors – R-LQ, R-CQ
 - Estimated PESQ scores – MOS-PQ
 - Separate R-factors for burst and gap conditions – R-Burst, R-Gap
 - Video MOS-V and Audio MOS-A
 - Video Transmission Quality - VSTQ
- Video stream metrics
 - Good and impaired I, B, P, SI, SP frame counts
 - Automatic detection of GoP structure and other key video stream attributes such as image size, bit rate, codec type
- Transport (IP/RTP) metrics
 - Packet loss rate, packet discard rate, burst/gap loss rates
 - Packet delay variation/ jitter
- Degradation factors
 - degradation due to loss, jitter, codec, delay, signal level, noise level, echo, recency

Once a flow terminates, AA software retrieve the flow MOS parameters from the subsystems, formats the info into a Cflowd record and forwards the record to a configured Cflowd collector (RAM).

RAM collects Cflowd records, summarizes these records using route of interest information (source/destinations). In addition, RAM provides the user with statistics (min/max/ avg values) for the different performance parameters that are summarized.

6.2 Retransmission and Fast Channel Change

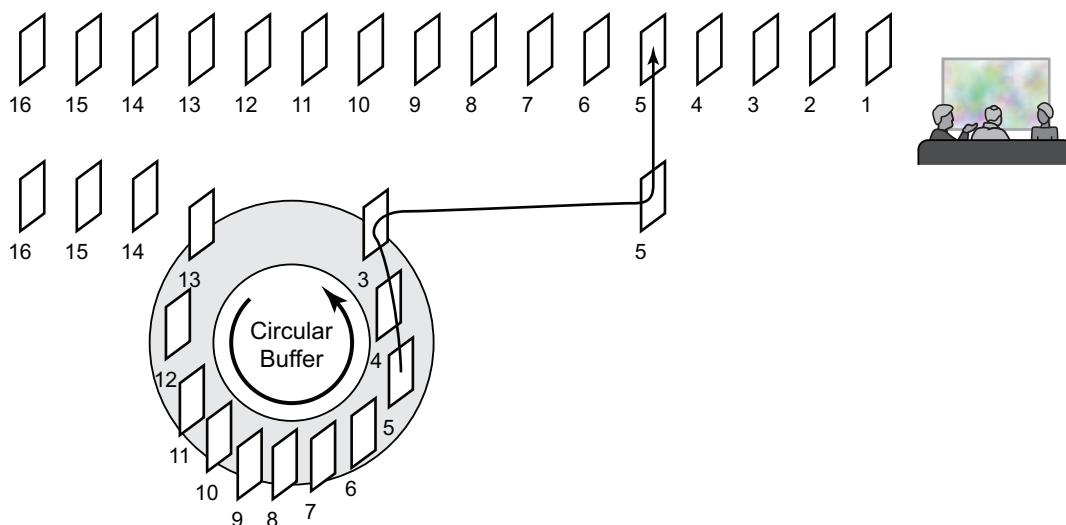
6.2.1 RET and FCC Overview

The following sections provide an overview of RET and FCC.

6.2.1.1 Retransmission

Retransmission (RET) for RTP (RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*) is based on a client/server model where the client sends negative acknowledgments (NACKs) using Real-time Transport Control Protocol (RTCP) (RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*) to a RET server when the client detects missing sequence numbers in the RTP stream. The RET server which caches the RTP stream, for example in a circular buffer, detects missing sequence numbers in the replies to the NACKs by resending the missing RTP packets as illustrated in [Figure 46](#).

Figure 46 RET Server Retransmission of a Missing Frame



OSSG321

The format of the reply must be agreed upon by the RET client and server and can be an exact copy (Payload Type 33 as defined in RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*) or sent with a different Payload Type using an encapsulating RET header format (RFC 4588, *RTP Retransmission Payload Format*).

RET has been defined in standards organizations by the IETF in the above-noted RFCs and Digital Video Broadcasting (DVB) in “Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks (DVB-IPTV Phase 1.4)” which describes the STB standards.

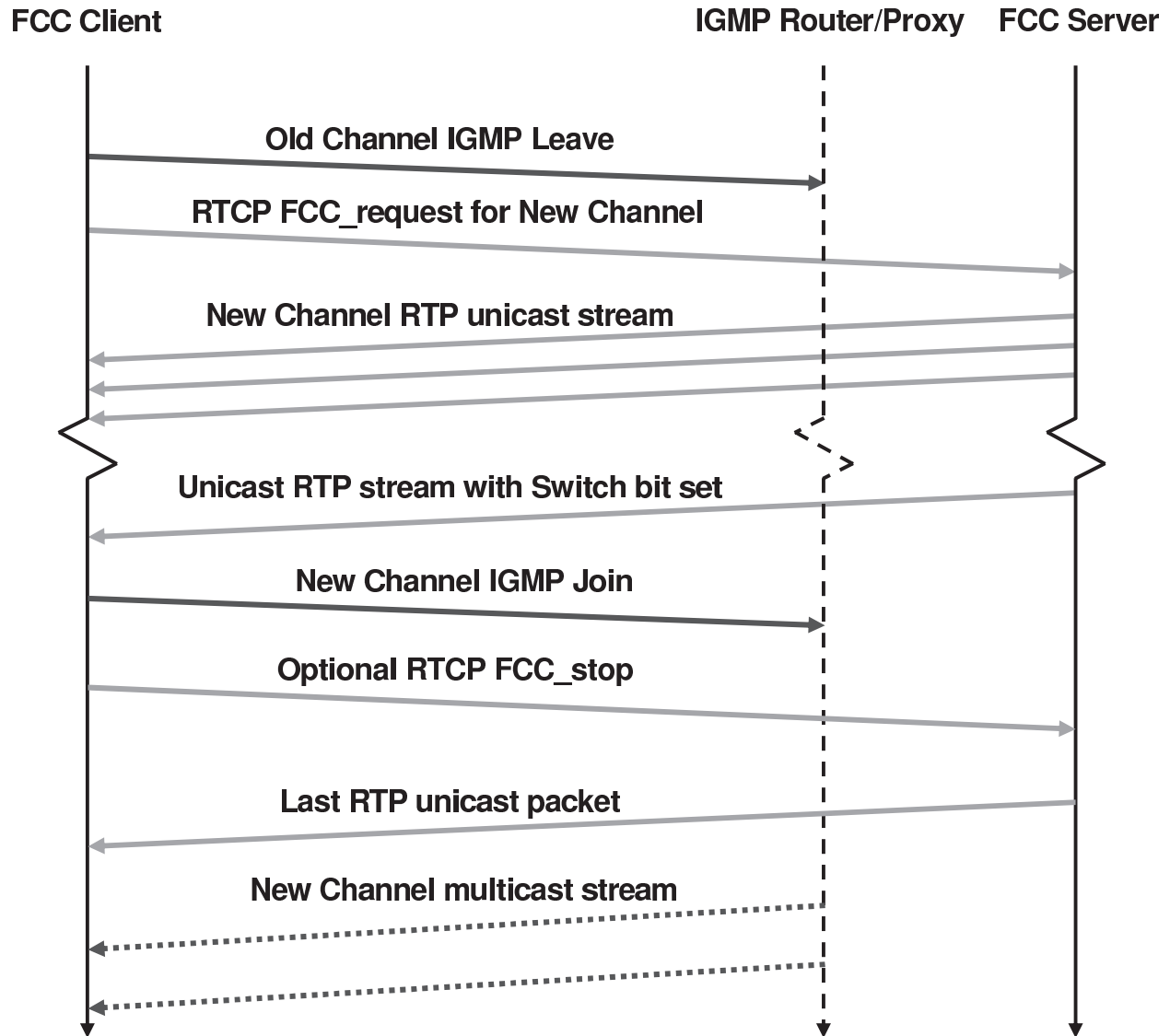
STBs that have a port of the Nokia RET/FCC Client SDK are an example of a standards-compliant RET Client implementation.

6.2.1.2 Fast Channel Change (FCC)

FCC is an Nokia method based on a client/server model for providing fast channel changes on multicast IPTV networks distributed over RTP. During a fast channel change, the FCC client initiates a unicast FCC session with the FCC server where the FCC server caches the video stream and sends the channel stream to the FCC client starting at the beginning of a Group of Pictures (GOP). Beginning at a GOP in the past minimizes the visual channel transition on the client/STB, but the FCC unicast stream must be sent at an accelerated rate in the time domain to allow the unicast stream to catch up to the main multicast stream, at which point, the FCC server signals to the client to join the main RTP stream.

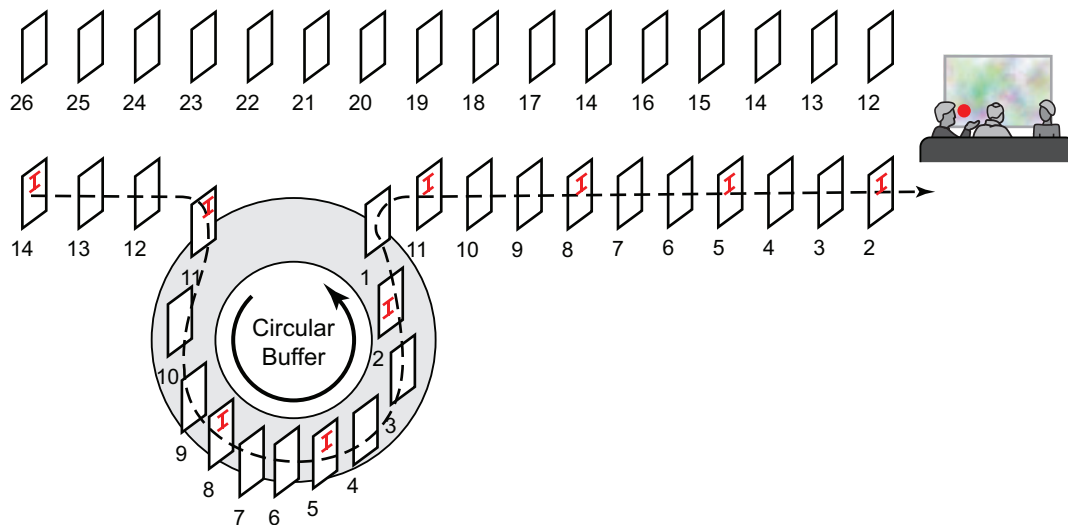
[Figure 47](#) illustrates the FCC client and server communication.

Figure 47 FCC Client/Server Protocol

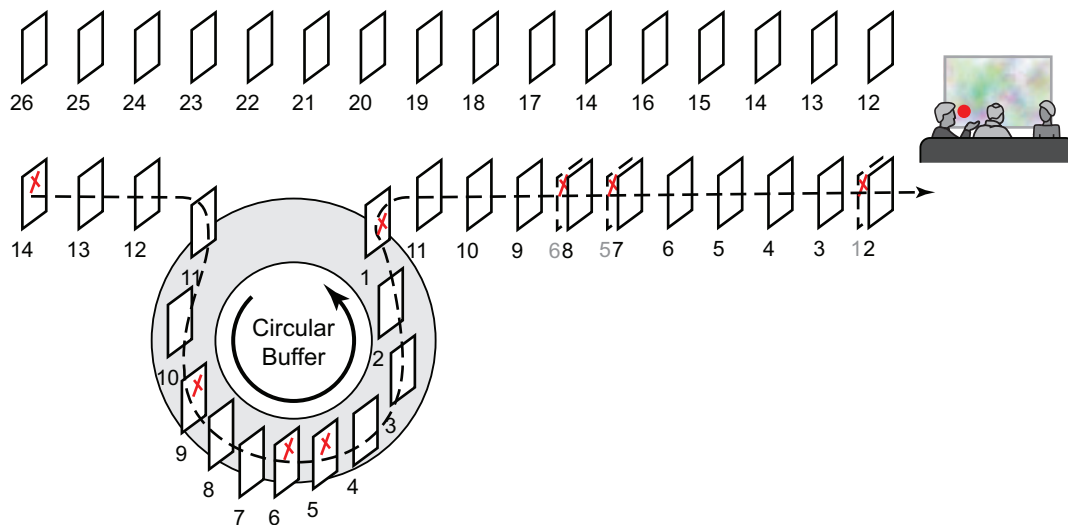


There are two techniques for compressing the FCC unicast stream in time to allow the unicast session to catch up to the multicast stream: bursting and denting. When bursting, the stream is sent at a rate faster than multicast stream, for example, the stream can be “burst” at 130% (or 30% over the nominal) multicast rate. “Denting” is a technique where less important video frames are dropped by the FCC server and not sent to the FCC client. Hybrid mode combines bursting and denting.

Bursting is illustrated in [Figure 48](#) and denting is illustrated in [Figure 49](#).

Figure 48 FCC Bursting Sent Faster Than Nominal Rate

OSSG322

Figure 49 FCC Danting Removing Less Important Frames

OSSG323

When the unicast session has caught up to the multicast session, the FCC server signals to the FCC client to join the main multicast stream. The FCC server will then send the unicast session at a lower rate called the “handover” rate until the unicast session is terminated.

The FCC server functionality requires the Nokia 5910 Video Services Appliance (VSA) Re-Wrapper which is used to encapsulate and condition the multicast channel streams into RTP, adding important information in the RTP extension header. Also, the ISA FCC server requires an STB FCC client based on the Nokia FCC/RET Client SDK.

6.2.1.2.1 Retransmission Client

The ISA RET client is used in hierarchical RET deployments and performs upstream corrections for missing packets in the RTP multicast stream to ensure that the RET server has all the packets for the stream.

The RET client is supported within a VPLS, IES or VPRN service context as applicable to the platform. The RET client source address is explicitly assigned. In a VPLS, the RET client IP appears to be an IP host within the service, and like a host, the RET client is also configured with a gateway IP address to provide a default route to reach the upstream RET server.

Whenever the RET client receives a retransmission from an upstream RET server, the replies are sent downstream as multicast in the multicast service using Payload Type 33 which is the Payload Type for an original stream.

Whether the RET client is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the RET client within the policy is an explicit enable/disable of the RET client and the IP address and UDP port for the upstream RET server for the channel.

The ISA RET server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network, for example, where an access node provides the multicast service cross connect and replication at the last mile. If there are separate multicast and unicast service instances, the multicast service instance must be configured in the unicast service, and the unicast and multicast services must use the same multicast information policy.

6.2.1.2.2 Retransmission Server

The ISA RET server is supported within a VPLS, IES or VPRN service context as applicable to the platform.

Whether the RET server is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the RET server within the policy is an explicit enable/disable of the local RET server (that is, whether the channel should be buffered), the RET buffer size for the channel in the ISA and a channel type (Picture-in-Picture (PIP), Standard Definition (SD) or High Definition (HD)). The RET buffer should be large enough to account for the round trip delay in the network; typically, a few hundred milliseconds is sufficient.

In a VPLS service, a single IP address is assigned to the RET server, and it acts like an IP host within the service.

In an IES or VPRN service, up to 16 IP addresses can be assigned to a video interface.

The video policy within the multicast information policy defines the characteristics for the how the RET server should respond to NACKs received on an IP address. The different characteristics defined in a RET server “profile” are for each channel type (PIP, SD and HD):

- Enable/disable for the RET server (that is, whether requests should be serviced or dropped).
- The RET rate (as a percentage of the nominal channel rate).

Typically, RET replies are sent below line rate because most dropped packets occur in the last mile and sending RET replies at a high rate may compound any last mile drop issues.

The IP address(es) of the RET server are defined in the unicast service instance, whereas the UDP port for the RET server is defined in the “default” bundle in the multicast information policy. The same UDP port is used for all RET server IP addresses that use the particular multicast information policy.

The ISA RET server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network. If there are separate multicast and unicast service instances, the unicast and multicast services must use the same multicast information policy.

6.2.1.2.3 Fast Channel Change Server

The ISA FCC server is supported within a VPLS, IES or VPRN service context as applicable to the platform. VPRN services are not supported on the 7450 ESS.

Whether the FCC server is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the FCC server within the policy is an explicit enable/disable of the local FCC server (that is, whether the channel should be buffered) and a channel type PIP, SD or HD. When FCC is enabled, three (3) GOPs are stored in the buffer. the channel also defines an optional fcc tuning parameter called the fcc Minimum Duration which is used by the FCC server to determine which GOP to start the FCC unicast session. If there are too few frames of the current GOP stored in the fcc server buffer (based on number of milliseconds of buffering), the FCC server will start the FCC session from the previous GOP.

In a VPLS service, a single IP address is assigned to the FCC server, and it acts like a IP host within the service.

In an IES or VPRN service, up to 16 IP addresses can be assigned to a video interface.

The Video Policy within the multicast information policy defines the characteristics for the how the FCC server should respond to FCC requests received on an IP address. The different characteristics defined in an FCC server “profile” are for each channel type (PIP, SD and HD):

- Enable/disable for the FCC server (for example, should the requests be serviced or dropped).
- The FCC mode: burst, dent or hybrid.
- The burst rate (as a percentage above the nominal channel rate) for PIP, SD and HD channel types.
- The multicast handover rate (as a percentage of the nominal channel rate) used by the server after it has signaled the client to join the main multicast channel.

Different FCC rates are allowed for each of the channel types because the channel types have different nominal bandwidths. For example, the last mile may only be able to reliably send a 25% burst (above nominal) for HD whereas the equivalent bit rate for SD is a 75% burst. The profiles are designed to provide flexibility.

The IP address of the FCC server is defined in the unicast service instance, whereas the UDP port for the FCC server is defined in the “default” bundle in the multicast information policy. The same UDP port is used for all FCC server IP addresses that use the particular multicast information policy.

The ISA FCC server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network. If there are separate multicast and unicast service instances, the unicast and multicast services must use the same multicast information policy.

6.2.1.2.4 Logging and Accounting for RET and FCC

Statistics and accounting is available for:

- RET Server sessions stats
- FCC session stats

6.2.1.3 RET and FCC Server Concurrency

Even though the previous sections discussed the RET server and FCC server as separate entities, the ISA can support RET and FCC servers at the same service at the same time. As such, the configuration commands and operational commands for the services are intermingled. If both the RET server and FCC server are enabled for a given channel, a single buffer is used for caching of the channel.

A maximum bandwidth limit for all server requests can be defined for a given “subscriber” which is equated with the source IP address. Before an ISA server processes a request, the ISA calculates the bandwidth to the subscriber required, and will drop the request if the subscriber bandwidth limit will be exceeded.

The ISA services RET and FCC requests on a first in, first out (FIFO) basis. Before servicing any request, the ISA calculates whether its egress bandwidth can handle the request. If there is insufficient egress bandwidth to handle the service request, the request is dropped. Near the ISA’s egress limits, RET requests will generally continue to be serviced whereas FCC requests will be dropped because RET sessions are generally a fairly small percentage of the nominal rate and FCC sessions are slightly below to above the nominal channel rate.

6.2.1.3.1 Prerequisites and Restrictions

This section summarizes some key prerequisites and restrictions for the RET client, RET server and FCC server.

- Both RET and FCC require RTP as the transport stream protocol.
- FCC requires the Nokia 5910 VSA Re-Wrapper.
- FCC requires an implementation of the Nokia 5910 STB Client.
- The multicast information policies must be the same on multicast and unicast services which are cross connected downstream.
- Support for up to four ISA-MSs in a video group
- Only a single IP address and profile are supported within a VPLS service for RET or FCC, so only a single Profile can be supported in a VPLS service.

- Up to 16 IP addresses can be configured for a Layer 3 service video interface (IES or VPRN) with each supporting a distinct profile.
- There can be a maximum of 32 IP addresses across all Layer 3 service video interfaces per chassis.

6.2.2 Separate Timers for FCC and RET

For each fast channel change, a new RTCP session is initialized, whereas for retransmission, the same RTCP session is always reused, with the same source and destination ports. The RTCP session duration is based on a timeout configuration, and a separate timeout parameter is available for FCC and RET under **config>mcast-mgmt>mcast-info-policy>video-policy>video-interface**, namely the **fcc-session-timeout** and **ret-session-timeout** parameters. As the FCC RTCP session timeout is generally shorter than the RET session timeout, the recommendation is to configure the FCC RTCP session timeout to a lower timeout value, accounting for the time required to complete a fast channel change and complete the multicast handoff. This strategy frees up RTCP sessions for other subscribers and improves efficiency.

6.2.3 Peak Bandwidth and Sessions per ISA

The CLI command **show isa video-group *video-group-id*** displays the peak egress bandwidth and sessions per ISA. Each peak value is also marked with a timestamp.

There are configurable watermarks for bandwidth and session consumption. The watermarks generate SNMP traps or log events when the ISA has reached the bandwidth or session thresholds. The egress bandwidth and session watermarks are configurable for FCC and RET separately, and also for FCC and RET together. The SNMP trap or log event is generated as the configured watermark is exceeded and is cleared if it falls below 10% of the watermark. For example, if the maximum egress rate is 10 Gb/s and the watermark is set at 90%, the alarm is generated when the egress rate exceeds 9 Gb/s (90% of 10 Gb/s) and the alarm is cleared if the egress rate falls below 10% at 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s).

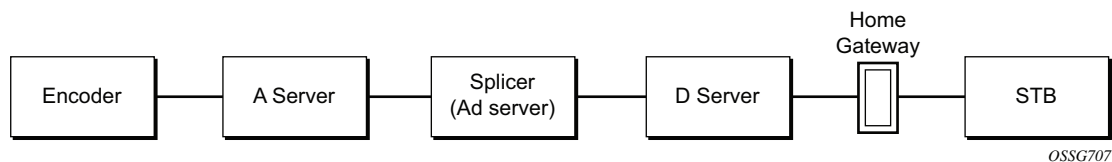
6.3 Ad Insertion

6.3.1 Local/Zoned Ad Insertion

6.3.1.1 Transport Stream Ad Splicing

Nokia's Local/Zoned ADI feature allows a 7750 SR with the ISA-MS (the "splicer") to perform ad splicing in an MSTV environment. The splicer is a post-A server transport stream (TS) splicer and can splice into encrypted or unencrypted transport streams. The splicer is positioned between the A-server and the D-server. [Figure 50](#) shows an ad insertion model displaying components.

Figure 50 Ad Insertion Model

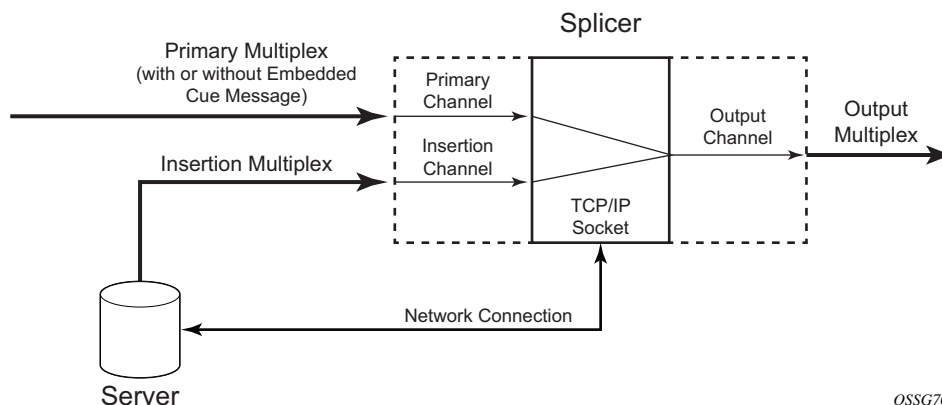


The ad insertion process is initiated when the splicer detects the SCTE 35 cue signal that identifies the upcoming start and end of the advertising time slot. The splicer communicates with the ad server using SCTE 30 standard messaging and will be instructed by the ad server:

- To take advantage of an ad insertion opportunity or avail and
- Determine the ad to be spliced into the main stream, if applicable.

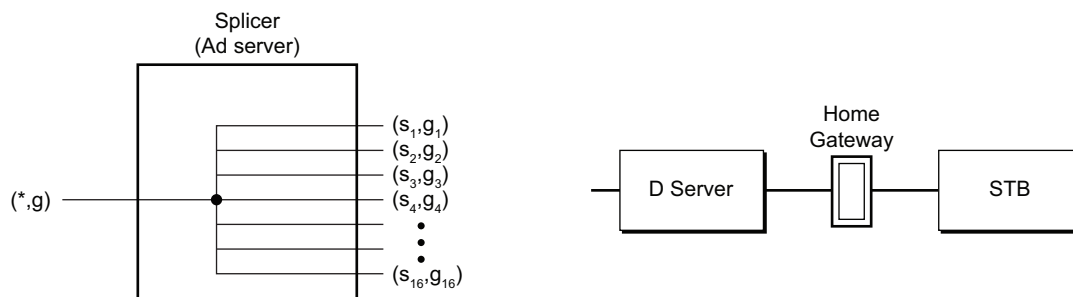
The ad servers must be configured for ad content to match encoder configurations for video/audio streams. The ad server sends the ad stream to the ad splicer and the ad splicer will switch it into the main stream as dictated by the digital splice points ([Figure 51](#)). The ad splicer can splice multiple ads into multiple channels simultaneously.

Figure 51 Transport Stream Ad Splicing



OSSG708

Figure 52 Splicer Model



OSSG709

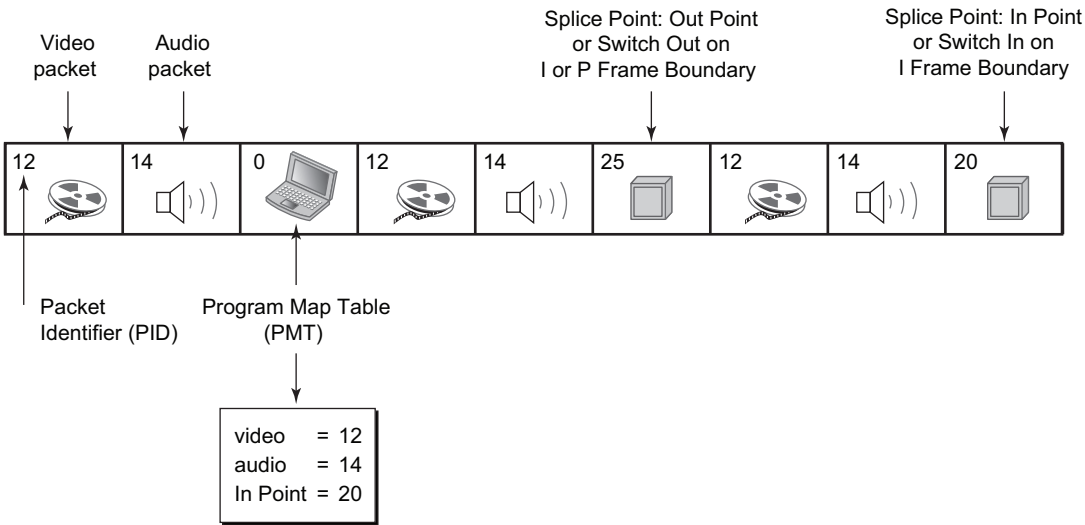
IPTV encryption and Digital Rights Management (DRM) can be applied to the transport stream payload but not to the transport stream (TS) header which allows a TS splicer to splice into encrypted streams, although the spliced ad content will in all cases be unencrypted. TS splicing does not put any requirements on the middleware platform as ad insertion will be outside the middleware's knowledge and control.

The [Figure 53](#) depicts a TS flow with various MUXed elementary streams (ES) identified by a unique Packet Identifier (PID). The Program Map Table (PMT) is used as the legend to map PID to elementary streams. The digital cue points are also identified by separate unique PID also defined in the PMT that is used by the TS splicer to know when to splice-in and splice-out of the stream.



Note: The only important thing that a TS splicer needs are the headers of the TS packets, and the underlying payload of each ES is not needed. This gives the splicer flexibility and makes it agnostic to the ES payload types.

Figure 53 Transport Stream Flow Example



OSSG710

6.3.1.2 Ad Zones

Within the splicer, zones are created by taking an ingress main channel multicast group, for example (*,G) or (S,G), and creating one or more egress “zone channels” on distinct source-specific multicast (SSM) groups (S1,G1), (S2,G2), etc. Up to 16 zones can be configured for each ingress multicast channel. The group multicast address for the zone channels need not be unique and can actually be the same as the ingress channel, but the SSM sources for the zone channels must be distinct.

Within SCTE 30, the main channel and zone channel are identified by an ASCII string name. These names must be unique and will be used when the splicer communicates with the ad server.

The input stream can be depicted through the following semantics diagram.

CHANNEL1	CHANNEL1_North (S1, G1)
(S, G)	CHANNEL1_South (S2, G2)
	CHANNEL1_East (S3, G3)
	CHANNEL1_West (S4, G4)
	CHANNEL1_Central (S5, G5)

where (S,G) is the input main channel stream mapping into five (5) (Sx, Gx) which are zone channel streams.

S1..S16 must be IP addresses in the video interface subnet but not the video interface address itself. This implies that traffic for the zones will be sourced from the ISA-MS.

To facilitate traffic from (S,G) to go to the ISA-MS, a static IGMP (S,G) must be configured on the video interface.

6.3.1.3 Local/Zoned ADI Prerequisites and Restrictions

This section describes prerequisites and restrictions for the local/zoned ADI feature:

- Network Time Protocol (NTP) is required to keep time synchronized between the ad server and the splicer. The time synchronization system helps keep the splicer and the server within +/-15 ms of each other.
- ADI is only supported within a Layer 3 IES or VPRN service.
- Splicing an SD advertisement into an HD main stream is supported, but splicing of an HD advertisement into an SD is not supported.
- The SCTE 30 connection between the ad server and the splicer must be maintained on separate IP addresses on the splicer within the video service.
- Up to 2 ad servers can be configured for redundancy.
- ADI only supports a single ISA-MS member in a video group.
- Up to 16 zone channels can be configured for a main channel.
- The audio re-ordering value in the multicast information policy must match the audio re-ordering configured on the A Server for reliable audio splicing.
- For best results, the ad should start/end with few frames of muted audio.
- The frequency of IDR frames in the network and ad streams must be less than one IDR frame every 1.3 seconds.
- Only the **splice_insert** command of SCTE-35 cue message is supported. The **splice_immediate** command is not supported.

6.4 Configuring Video Service Components with CLI

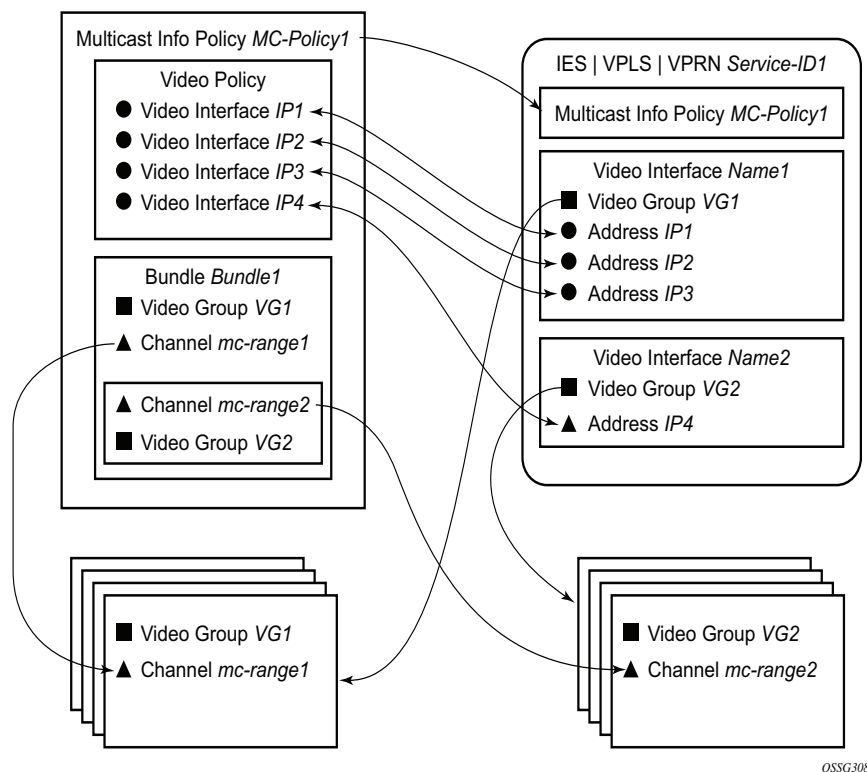
This section provides information to configure RET/FCC using the command line interface.

6.4.1 Video Services Overview

There can be a maximum of eight ISA-MSs in a given system. The main entities of video configurations are:

- Video group
- Multicast information policy
 - A video policy to configure video interface properties
 - Multicast bundles and channels to associate bundles/channels with video groups
- Within a service, configuring a video interfaces and their associations with video groups.

[Figure 54](#) shows various configuration elements and how they are associated by configuration.

Figure 54 Video Services Configuration Elements

OSSG308

A video interface within a service can have multiple IP address, and their association with the video interfaces within the video policy are based on IP addresses. Support for multiple video interface IP addresses for a given video interface allows video characteristics (burst rate, retransmission format, etc.) for the channels associated with the video interface to be based on the IP address on which the request is received.

Both the bundle/channel configuration and the video interface configuration within the service are associated with a specific video group. If the request is received on a video interface for a channel not serviced by the video group associated with the video interface, the request is invalid and is dropped. [Figure 54](#) displays an example of this is a request for mc-range2 received on IP1, IP2 or IP3. A request for mc-range2 would only be valid on IP4.

As with other multicast information policies, the bundle name default is a special bundle and is reserved for setting of default values. If a video parameter is not explicitly set in a bundle/channel, the value set in the default bundle is used.

6.4.1.1 Configuring an ISA-MS Module

The ISA-MS hardware has an MDA form factor and is provisioned in the same manner as other MDAs in the **config>card>mda>mda-type** context.

Use the following commands to configure a ISA-MS module.

CLI Syntax:

```
config
card slot-number
    mda slot-number
        mda-type isa-ms
```

The following output displays an ISA-MS configuration example:

```
*A:Dut-C>config>card# info
-----
card-type iom3-xp-c
mda 1
    mda-type isa-ms
exit
mda 2
    mda-type isa-ms
exit
-----
*A:Dut-C>config>card#
```

6.4.1.2 Configuring a Video Group

When used for video services, ISA-MSes are logically grouped into video groups that pool the ISA buffering and processing resources into a single logical entity.

Use the following commands to configure a video group.

CLI Syntax:

```
config
isa
    video-group video-group-id [create]
        description description-string
        primary mda-id
        [no] shutdown
```

The example shown below shows video-group 1 with a single ISA configured in slot 2/MDA 1.

```
*A:Dut-C>config>isa# info
=====
video-group 1 create
    description "Video Group 1"
    primary 7/2
```

```

        no shutdown
    exit
=====
*A:Dut-C>config>isa#

```

Within the video group configuration, there are specific video application commands to enable features. These commands are described in the configuration examples for the application. Depending on the video application, more than one primary ISA-MS is allowed increasing the egress capacity of the video group.

ISA-MS in a single video group cannot be on the same IOM. An IOM can accommodate two ISA-MS modules provided that the ISA-MS are members of different video groups.

6.4.1.3 Configuring a Video SAP and Video Interface in a Service

Video features in a VPLS service require the creation of a video SAP and a video interface. A video SAP is similar to other SAPs in the system in that QoS and filter policies can be associated with the SAP on ingress (traffic leaving the ISA and ingressing the system) and egress (traffic leaving system and entering the ISA).

The video SAP is associated with a video group. Channels are also associated with a video group which is what establishes the link between what channels can be referenced through the video SAP. The multicast information policy associated with the service is where the channel to video group association is defined.

For unicast VPLS services that have an associated multicast service that is cross connected downstream of the router, the multicast service needs to be identified by the service ID in the unicast VPLS service.

The video commands for are identical in the IES and VPRN service contexts. The basic IES and VPRN commands are similar to the video commands in the VPLS context and follow the same logic of associating the video SAP with a video group and the multicast information policy defining the channel to video group association.

Another parameter defined for a channel in the multicast information policy that is important for video services is the administrative bandwidth defined for the channel. Many video applications use the bandwidth to determine if sufficient ISA egress bandwidth exists to service or drop a service request.

The following output displays an example video interface configuration.

```

A:IPTV-SR7>config>service>ies# info
-----
        video-interface "video-100" create
        video-sap 4

```

```
exit
address 10.1.1.254/8
address 192.168.0.254/8
address 192.168.1.254/24
adi
    channel 192.168.5.228 source 192.168.9.10 channel-name "228"
    scte35-action drop
    zone-channel 192.168.5.228 source 192.168.100.1 adi-channel-
name
"228-1"

    exit
    scte30
    ad-server 10.200.14.2
    local-address control 10.1.1.2 data 10.1.1.3
    exit
exit
-----
A:IPTV-SR7>config>service>ies#
```

6.4.1.4 Basic Multicast Information Policy Configuration

Multicast information policies are used by the video applications to define multicast channel attributes and video policies which contains application-specific configuration for a video interface IP address.

It is within the multicast information policy bundles, channels and source-overrides that a video group is assigned to a channel. The video group association is inherited from the more general construct unless it is explicitly disabled.

The administrative bandwidth for channels at the bundle, channel or source-override level is also defined in the multicast information policy. Video applications use the administrative bandwidth here when a channel rate estimate is needed.

A video policy is defined within the multicast information policy for a specific video interface IP address. The IP address for the video policy is the key value that associates it with a specific video interface IP address within a service associated with overall multicast information policy.

Refer to the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide* for CLI command descriptions and syntax usage information to configure multicast info policies.

The following output displays a policy example.

```
A:IPTV-SR7>config>mcast-mgmt># info
-----
multicast-info-policy "ies100" create
    bundle "5.6.140" create
        admin-bw 8000
        video
```

```

        video-group 1
        local-rt-server
        rt-buffer-size 3000
    exit
    channel "10.5.6.140" "10.5.6.140" create
    exit
exit
bundle "default" create
exit
bundle "5.6.241-5.6.243" create
    admin-bw 12000
    video
        video-group 1
        rt-buffer-size 4000
    exit
    channel "10.5.6.241" "10.5.6.243" create
    exit
exit
exit
exit
-----
A:IPTV-SR7>config>router#

```

6.4.2 Sample Configurations

The following output displays configurations of VQM with packet selection.

```

*A:SR-7/Dut-C>config>mcast-mgmt># info
-----
    multicast-info-policy "vqm" create
        bundle "ixia" create
            channel "10.5.5.6" "10.5.5.7" create
                admin-bw 20000
                video
                    video-group 4
                    rt-buffer-size 1000
                    analyzer
                        alarms
                            cc-error
                            pat-repetition tnc 400 qos 600 poa 700
                            pat-syntax
                            pid-pmt-unref
                            pmt-repetition tnc 2300 qos 2500 poa 2700
                            pmt-syntax
                            vid-pid-absent 5000
                            non-vid-pid-absent 5000
                            pcr-repetition tnc 400 qos 600 poa 700
                            scte-35
                            tei-set
                            ts-sync-loss
                        exit
                    exit
                stream-selection source1 192.168.2.1 intf1 "ineo-
ingress1"
                source2 192.168.2.1 intf2 "ineo-ingress2"
            exit
        exit
    exit

```

```

        source-override "192.168.2.1" create
        exit
    exit
    exit
    bundle "default" create
    exit
    exit
-----
*A:SR-7/Dut-C>config>service# info
-----
    customer 1 create
        description "Default customer"
    exit
    ies 300 customer 1 vpn 300 create
        description "Default Ies description for service id 300"
        video-interface "video-300" create
            video-sap 4
            exit
            address 10.20.255.254/16
            channel 10.5.5.6 source 192.168.2.1 channel-name "Ineoquest-1"
            zone-channel 10.5.5.6 source 10.20.0.1 adi-channel-
name "Ineoquest-
1-1"
            exit
            adi
            exit
            no shutdown
        exit
        service-name "XYZ Ies 300"
        no shutdown
    exit
-----
*A:SR-7/Dut-C>config>service#

*A:SR-7/Dut-C>config>router# info
-----
#-----
echo "IP Configuration"
#-----
    interface "ineo-ingress1"
        address 10.200.16.1/24
        port 3/2/12
        ingress
            filter ip 100
        exit
    exit
    interface "ineo-ingress2"
        address 10.200.17.1/24
        port 5/1/1
        ingress
            filter ip 200
        exit
    exit
    interface "ixia-egress"
        address 10.200.15.1/24
        port 3/2/15
    exit
    interface "system"
        address 10.20.3.1/32

```

```
exit
ecmp 2
multicast-info-policy "vqm"
static-route 192.168.2.1/32
    next-hop 10.200.16.2
    no shutdown
exit
next-hop 10.200.17.2
    no shutdown
exit
exit
exit
#-----
echo "IGMP Configuration"
#-----
igmp
    interface "video-300-D"
        static
            group 10.5.5.6
            source 192.168.2.1
        exit
    exit
exit
interface "video-300-D2"
    static
        group 10.5.5.6
        source 192.168.2.1
    exit
exit
exit
interface "ixia-egress"
    static
        group 10.5.5.6
        source 10.20.0.1
    exit
exit
exit
exit
exit
#-----
echo "PIM Configuration"
#-----
pim
    rpf-table rtable-m
    interface "video-300"
        exit
    interface "ineo-ingress1"
        multicast-senders always
    exit
    interface "ineo-ingress2"
        multicast-senders always
    exit
rp
    static
    exit
    bsr-candidate
        shutdown
    exit
    rp-candidate
        shutdown
    exit
```

```

        exit
    exit
-----
*A:SR-7/Dut-C>config>router#
*A:SR-7/Dut-C>config>isa# info
-----
        video-group 4 create
        analyzer
        stream-selection
        primary 3/1
        no shutdown
    exit
-----
*A:SR-7/Dut-C>config>isa#

```

The following output displays configurations of VQM without packet selection.

```

-----
*A:SR-7/Dut-C>config>service# info
-----
        customer 1 create
        description "Default customer"
    exit
    ies 300 customer 1 vpn 300 create
        description "Default Ies description for service id 300"
        interface "linux-ingress" create
            address 10.10.33.228/24
            sap 3/2/17 create
                description "sap-300-10.10.33.228"
            exit
        exit
        interface "linux-egress" create
            address 10.10.34.228/24
            sap 3/2/7 create
                description "sap-300-10.10.34.228"
            exit
        exit
        video-interface "video-300" create
            video-sap 2
            exit
            address 10.20.13.1/24
            channel 10.5.5.6 source 192.168.2.1 channel-name "A2-SP3"
                zone-channel 10.5.5.6 source 10.20.13.2 adi-channel-name "A2-
SP3-1"
            exit
            adi
            exit
            no shutdown
        exit
        service-name "XYZ Ies 300"
        no shutdown
    exit
-----
*A:SR-7/Dut-C>config>service# /configure router
*A:SR-7/Dut-C>config>router# info
-----
#-----

```

```
echo "IP Configuration"
#-----
    interface "system"
        address 10.20.1.1/32
    exit
    multicast-info-policy "A-server"
#-----
echo "Static Route Configuration"
#-----
    static-route 128.251.33.0/24
        next-hop 10.10.33.229
        no shutdown
    exit
    static-route 192.168.2.0/24
        next-hop 10.10.33.229
        no shutdown
    exit
exit
#-----
echo "IGMP Configuration"
#-----
    igmp
        interface "video-300-D"
            static
                group 10.5.5.6
                source 192.168.2.1
            exit
        exit
    exit
    interface "linux-egress"
        static
            group 10.5.5.6
            source 10.20.13.2
        exit
    exit
exit
#-----
echo "PIM Configuration"
#-----
    pim
        interface "linux-ingress"
            hello-interval 0
            multicast-senders always
        exit
        interface "linux-egress"
            hello-interval 0
        exit
    apply-to all
    rp
        static
        exit
        bsr-candidate
            shutdown
        exit
        rp-candidate
            shutdown
        exit
    exit
```



```

exit
-----
*A:SR-7/Dut-C>config>router# /configure isa
*A:SR-7/Dut-C>config>isa# info
-----
    video-group 2 create
        analyzer
        primary 2/1
        no shutdown
    exit
-----
*A:SR-7/Dut-C>config>isa# /configure mcast-management
*A:SR-7/Dut-C>config>mcast-mgmt># info
-----
    multicast-info-policy "A-server" create
        bundle "LiveTv" create
            channel "10.5.6.243" "10.5.6.243" create
                admin-bw 3000
                video
                    video-group 2
                    rt-buffer-size 1000
                exit
            exit
            channel "10.5.5.6" "10.5.5.6" create
                admin-bw 5000
                video
                    video-group 2
                    rt-buffer-size 1000
                    analyzer
                        alarms
                            cc-error
                            pat-repetition tnc 200 qos 400 poa 600
                            pat-syntax
                            pid-pmt-unref
                            pmt-repetition
                            pmt-syntax
                            vid-pid-absent 1000
                            non-vid-pid-absent 1000
                            pcr-repetition tnc 200 qos 400 poa 600
                            scte-35
                            tei-set
                            ts-sync-loss
                            report-alarm severity tnc
                        exit
                    exit
                exit
            source-override "192.168.33.37" create
            exit
        exit
    exit
    bundle "default" create
    exit
    bundle "mp2ts-ads" create
        channel "10.4.5.1" "10.4.5.254" create
            admin-bw 5000
            video
                video-group 2
                rt-buffer-size 1000
            exit

```

```
exit
exit
exit
-----
*A:SR-7/Dut-C>config>mcast-mgmt>#
```

6.5 Configuring RET/FCC Video Components with CLI

This section provides information to configure RET/FCC using the command line interface.

6.5.1 Configuring RET/FCC Video Features in the CLI

The following sections provide configuration examples for the RET client, RET server and FCC server.

6.5.1.1 Configuring the RET Client

This section provides an example configuration for the RET client. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1
- A single channel 192.0.2.1 within multicast bundle “b1” with an administrative bandwidth of 2700 kb/s defined in **multicast-info-policy** *multicastinfopolicyname*.
- The upstream RET server for the channel is 10.4.4.4 on UDP port 4096
- A single video interface named “v1” in the service with IP address 10.3.3.3/24
- A RET client address of 10.3.3.4 for a VPLS and 10.3.3.3 for IES and VPRN case.

The first step in the configuration is to configure video group 1 and the ISA-MS hardware.

CLI Syntax:

```
config>isa
video-group video-group-id [create]
primary mda-id
no shutdown
```

```
*A:ALA-48config>isa# info
```

```
-----
video-group 1 create
primary 2/1
no shutdown
exit
```

```
-----
*A:ALA-48config>isa#
```

CLI Syntax: config# card *slot-number*
 mda *mda-slot*
 mda-type *mda-type*

```
*A:ALA-48config>card>mda#  info
-----
```

```
          mda-type isa-ms
-----
```

```
*A:ALA-48config>card>mda#
```

The channel parameters for 192.0.2.1 are configured in **multicast-info-policy** *multicastinfopolicyname*. The channel configuration includes the administrative bandwidth, the channel's association with video group 1 and the upstream RET server configuration for the channel (10.4.4.4 UDP port 4096). The following output displays the configuration. Refer to the CLI tree for a complete list of CLI commands.

```
*A:ALA-48config>mcast-mgmt>mcast-info-plcy#  info
-----
```

```
          bundle "b1" create
                  admin-bw 2700
                  video
                         video-group 1
                         rt-server 10.4.4.4 port 4096
                  exit
                  channel "192.0.2.1" "192.0.2.1" create
                  exit
          exit
          bundle "default" create
          exit
          video-policy
                  video-interface 10.3.3.3 create
                  exit
          exit
-----
```

```
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

The channel parameters are actually defined for the channel bundle “b1” and the channel inherits those values based on the multicast information policy inheritance rules.

For the RET client in a VPLS, the following commands within the service instance perform the following tasks to complete the RET client configuration:

- Associate the VPLS with **multicast-info-policy** *multicastinfopolicyname*.
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.

- Assigns a RET client address and gateway.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 192.0.2.1.



Note: SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48config>service>vpls# info
-----
      igmp-snooping
        no shutdown
      exit
    video-interface "vi" create
      video-sap 1
      exit
      address 10.3.3.3/24
      gateway-ip 10.3.3.253
      rt-client-src-address 10.3.3.4
      no shutdown
    exit
-----
*A:ALA-48config>service>vpls#

*A:ALA-48config>router# info
-----
...
      multicast-info-policy multicastinfopolicyname
      sap 3/2/13:21 create
        igmp-snooping
          static
            group 192.0.2.1
            starg
          exit
        exit
      exit
    exit
  exit
...
-----
*A:ALA-48config>router#
```



Note: The RET client address is 10.3.3.4 which must be within the IP subnet assigned to the video interface (10.3.3.3/24).

For the RET client in an IES or VPRN, the following commands within the service instance perform these tasks to complete the RET client configuration:

- Associate the service with **multicast-info-policy** *multicastinfopolicyname*.

- Create the video interface “vi” and assign IP address 10.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on the video interface for the channel 192.0.2.1. (7750 SR only)

```
*A:ALA-48config>service>ies# info
-----
        video-interface "vi" create
            video-sap 1
            exit
            address 10.3.3.3/32
            no shutdown
        exit
...
-----
*A:ALA-48config>service>ies#

*A:ALA-48config>router# info
-----
...
    multicast-info-policy multicastinfopolicyname
    pim (7750 only)
        interface "vi"
        exit
    exit
    igmp (7750 only)
        interface "vi"
            static
                group 192.0.2.1
                starg
            exit
        exit
    exit
-----
*A:ALA-48config>router#
```

The RET client address is 10.3.3.3 which is the address assigned to the video interface in the video policy portion of the multicast information policy.

6.5.1.2 Configuring the RET Server

This section provides an example configuration for the RET server. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1
- A single channel 192.0.2.1 within multicast bundle “b1” with an administrative bandwidth of 2700 kb/s defined in **multicast-info-policy** *multicastinfopolicyname*.

- A retransmission buffer for the channel set to 300 milliseconds.
- The RET rate is 5% of nominal.
- Local RET server address is 10.3.3.3 with destination port is UDP 4096.

The first step in the configuration is to configure video group 1 enabling the RET server and the ISA-MS hardware.

CLI Syntax:

```
config>isa
video-group video-group-id [create]
local-rt-server
no shutdown
```

```
*A:ALA-48config>isa# info
-----
video-group 1 create
local-rt-server
primary 2/1
no shutdown
exit
-----
*A:ALA-48config>isa#
```

```
*A:ALA-48config>card 2>mda 1# info
-----
mda-type isa-ms
-----
*A:ALA-48config>card>mda#
```

The **local-rt-server** command in the above output enables the local RET server on the video group.

The channel parameters for 192.0.2.1 are configured in **multicast-info-policy** *multicastinfopolicyname*. The channel configuration includes the administrative bandwidth and the channel's association with video group 1.

```
*A:ALA-48config>mcast-mgmt>mcast-info-plcy# info
-----
bundle "default" create
local-rt-port 4096
exit
bundle "b1" create
admin-bw 2700
video
video-group 1
local-rt-server
rt-buffer-size 300
exit
channel "192.0.2.1" "192.0.2.1" create
exit
exit
```

```

video-policy
  video-interface 10.3.3.3 create
    rt-rate 5
    hd
      local-rt-server
    exit
    sd
      local-rt-server
    exit
    pip
      local-rt-server
    exit
  exit
exit
exit
-----
*A:ALA-48config>mcast-mgmt>mcast-info-plcy#

```

The **local-rt-port** command in the bundle “default” defines the destination UDP port used to reach the local RET server on the service where the multicast information policy is applied. The RET server port can only be defined in the bundle “default” and applies for all bundles in the policy. If no value is specified, the default is used.

In the bundle “b1” the **local-rt-server** command enables the RET server for all channels in the bundle, and the **rt-buffer-size** *rt-buffer-size* command sets the retransmission buffer for all channels in the bundle to 300 milliseconds.

In the video policy above, the **local-rt-server** commands for the video interface 10.3.3.3 enables the RET server on that interface for all channel types “hd” (High Definition), “sd” (Standard Definition) and “pip” (Picture-in-Picture). The **rt-rate** *rt-burst-percentage* command in the policy indicates that the retransmission rate will be 5% of the nominal rate for all channel types; individual rates can be defined if desired.

For the RET server in a VPLS, these commands within the service instance perform the following tasks to complete the RET server configuration:

- Associate the VPLS with **multicast-info-policy** *multicastinfopolicyname*.
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns an IP address 10.3.3.3 to the video interface.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 192.0.2.1.



Note: SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```

*A:ALA-48config>service>vpls# info
-----
igmp-snooping

```



```

        no shutdown
    exit
    video-interface "vi" create
        video-sap 1
        exit
        address 10.3.3.3/32
        no shutdown
    exit
    multicast-info-policy multicastinfopolicyname
    sap 3/2/13:21 create
        igmp-snooping
            static
                group 192.0.2.1
                starg
            exit
        exit
    exit
    exit
    exit
-----
*A:ALA-48config>service>vpls#

```

The services available on the video interface address 10.3.3.3 are defined in the video policy in which the RET server was enabled.

For the RET server in an IES or VPRN, these commands within the service instance perform the following tasks to complete the RET server configuration:

- Associate the service with **multicast-info-policy** *multicastinfopolicyname*.
- Create the video interface “vi” and assign IP address 10.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on video-interface “vi” for the channel 192.0.2.1.

```

*A:ALA-48config>service>ies# info
-----
        video-interface "vi" create
            video-sap 1
            exit
            address 10.3.3.3/32
            no shutdown
        exit
    multicast-info-policy multicastinfopolicyname
    pim
        interface "vi"
        exit
    exit
    igmp
        interface "vi"
            static
                group 192.0.2.1
                starg
            exit
        exit
    exit
    exit
-----

```

```
*A:ALA-48config>service>ies#
```

The services available on the video interface address 10.3.3.3 are defined in the video policy in which the RET server was enabled.

6.5.1.3 Configuring the FCC Server

This section provides an example configuration for the FCC server. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1.
- A single channel 192.0.2.1 within multicast bundle “b1” with an administrative bandwidth of 8000 kb/s defined in **multicast-info-policy** *multicastinfopolicyname*.
- The FCC mode is burst with a rate 130% of nominal for HD, 200% for SD, and disabled for PIP.
- Local FCC server address is 10.3.3.3 with destination port is UDP 4098.

CLI Syntax:

```
config>isa
video-group video-group-id [create]
    fcc-server
    no shutdown
```

The first step in the configuration is to configure video group 1 enabling the RET server and the ISA-MS hardware.

```
*A:ALA-48config>isa# info
-----
video-group 1 create
    fcc-server
    primary 2/1
    no shutdown
exit
-----
*A:ALA-48config>isa#

*A:ALA-48config>card>mda# info
-----
mda-type isa-ms
-----
*A:ALA-48config>card>mda#
```

The **fcc-server** command in the above output enables the FCC server on the video group.

The channel parameters for 192.0.2.1 are configured in **multicast-info-policy** *multicastinfopolicyname*. The channel configuration includes the administrative bandwidth and the channel's association with video group 1.

```
*A:ALA-48configmcast-mgmtmcast-info-plcy# info
-----
bundle "default" create
    local-fcc-port 4098
exit
bundle "b1" create
    admin-bw 8000
    video
        video-group 1
        fcc-server
        fcc-channel-type hd
    exit
    channel "192.0.2.1" "192.0.2.1" create
    exit
exit
video-policy
    video-interface 10.3.3.3 create
        rt-rate 5
        hd
            fcc-server mode burst
            fcc-burst 30
        exit
        sd
            fcc-server mode burst
            fcc-burst 100
        exit
        pip
            no fcc-server
        exit
    exit
exit
exit
-----
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

The **local-fcc-port** command in the bundle “default” defines the destination UDP port used to reach the FCC server on the service where the multicast information policy is applied. The FCC server port can only be defined in the bundle “default” and applies for all bundles in the policy. If no value is specified, the default is used.

In the bundle “b1”, the **fcc-server** command enables the FCC server for all channels in the bundle, and the **fcc-channel-type hd** command sets the channel type for all channels in the bundle to “hd” (High Definition).

In the video policy context above, the **fcc-server** commands for the video interface 10.3.3.3 enables the FCC server on that interface for all channel types “hd” (High Definition), “sd” (Standard Definition) whereas the **no fcc-server** command disables the FCC for “pip” (Picture-in-Picture) channels on the video interface. The **fcc-burst** command in the policy indicates that the burst rate over the nominal rate for the channel type; HD at 130% (30% over nominal) and SD at 200% (100% over nominal).

For the FCC server in a VPLS, the following commands within the service instance perform the following tasks to complete the FCC server configuration:

- Associate the VPLS with **multicast-info-policy** *multicastinfopolicyname*.
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns an IP address 10.3.3.3 to the video interface.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 192.0.2.1.



Note: SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48configservicevpls# info
-----
    igmp-snooping
        no shutdown
    exit
    video-interface "vi" create
        video-sap 1
        exit
        address 10.3.3.3/32
        no shutdown
    exit
    multicast-info-policy multicastinfopolicyname
    sap 3/2/13:21 create
        igmp-snooping
            static
                group 192.0.2.1
                starg
            exit
        exit
    exit
    exit
-----
*A:ALA-48configservicevpls#
```

The services available on the video interface address 10.3.3.3 are defined in the video policy in which the FCC server was enabled.

For the FCC server in an IES or VPRN, the following commands within the service instance perform the following tasks to complete the FCC server configuration:

- Associate the service with **multicast-info-policy** *multicastinfopolicyname*.
- Create the video interface “vi” and assign IP address 10.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on video-interface “vi” for the channel 192.0.2.1.

```
*A:ALA-49configserviceies# info
-----
        video-interface "vi" create
            video-sap 1
            exit
            address 10.4.4.4/32
            no shutdown
        exit
-----
*A:ALA-49configserviceies#

*A:ALA-48configrouter# info
-----
...
    multicast-info-policy multicastinfopolicyname
    pim
        interface "vi"
        exit
    exit
    igmp
        interface "vi"
        static
            group 192.0.2.1
            starg
        exit
    exit
    exit
-----
*A:ALA-48configrouter#
```

The services available on the video interface address 10.3.3.3 are defined in the video policy in which the FCC server was enabled.

6.5.1.4 Logging and Accounting Collection for Video Statistics

The following output displays a configuration example used in logging and accounting for video.

```
*A:SR-7/Dut-C>config>log# info
-----
        file-id 1
```

```
        location cf3:
    exit
    accounting-policy 1
        shutdown
        record video
        collection-interval 5
        to file 1
    exit
...
-----
*A:SR-7/Dut-C>config>log#
```

Use the following CLI to enable logging and accounting to a service to collect stats for that particular service.

Example:

```
*A:SR-7/Dut-C>config>service>ies# video-interface "vi" accounting-policy 1
*A:SR-7/Dut-C>config>service>ies# info
    video-interface "vi" create
        accounting-policy "1"
    exit
```

Starting stats collection can be enabled by executing a **no shutdown** command on the accounting policy. This starts the recording of stats and the stats will be written in an act-collect directory and a **shutdown** command on the accounting policy will move the recorded file to act directory.

6.6 Configuring ADI Components with CLI

This section provides information to configure ADI using the command line interface.

6.6.1 Configuring ADI in CLI

6.6.1.1 Configuring the RET Client

This section provides an example configuration for the ADI splicer. The configuration example makes the following assumptions:

- A single ISA-MS is configured in slot 2/1 in video group 1.
- The NTP server for the router is 192.168.15.221.
- A single channel main 192.0.2.140 within multicast bundle “b1” is defined in the **multicast-info-policy** *multicastinfopolicyname* context.
- IES service 100 is a Layer 3 service in which ADI will be performed.
- The video interface in IES 100 is 10.100.0.254/8
- The ad server address is 10.200.14.2
- The splicer’s local addresses used to communicate with the ad server are 10.1.1.2 for control traffic and 10.1.1.3 for data traffic.
- For the SCTE 30 communication in the example, the main channel is named 228 with (S,G) = (192.168.9.10,234.4.5.228) and the zone channel is named 228-1 with (S,G) = (10.100.100.1,234.4.5.228).
- Must have an IGMP static entry for the network channel (S,G) on the video-interface to attract the network traffic to the video interface.
- Must have the video-interface enabled in PIM.

6.6.1.2 Configuring a Video Group

The first step in the configuration is to configure a video group (*video-group-id* = 1) and enabling ad insertion and the ISA-MS hardware. The **ad-insert** command enables the ADI splicer on the video group.

```
A:ALA-49>config>isa# info
-----
...
video-group 1 create
```

```

        description "Video Group 1"
        ad-insert
        primary 7/2
        no shutdown
    exit
...
-----
A:ALA-49>config>isa#

```

The following output shows the card and MDA configuration.

```

A:ALA-49>config>card# info
-----
        card-type iom3-xp-c
        mda 1
            shutdown
            mda-type isa-ms
        exit
        mda 2
            mda-type isa-ms
        exit
-----
A:ALA-49>config>card#

```

6.6.1.3 Configuring NTP

NTP is required on the splicer to ensure that time is synchronized between it and the ad server.

```

A:ALA-49>config>system>time# info
-----
        ntp
            no authentication-check
            ntp-server
            server 192.168.15.221
            no shutdown
        exit
...
-----
A:ALA-49>config>system>time#

```

6.6.1.4 Configuring Channel Parameters

The channel parameters for 192.0.2.228 are configured in the **multicast-info-policy** *multicastinfopolicyname* context. For ADI, the channel configuration required is the channel's association with video group 1.

```

*A:ALA-49>config>mcast-mgmt# info
-----
...

```



```
multicast-info-policy "multicastinfopolicyname" create
    bundle "b1" create
        video
            video-group 1
        exit
        channel "192.0.2.228" "192.0.2.228" create
        exit
    exit
    bundle "default" create
    exit
exit
...
-----
*A:ALA-49>config>mcast-mgmt#
```

6.6.1.5 Configuring Service Entities

In addition to the commands needed to configure a service, the following commands within the service instance are used to perform the following ADI configuration steps. This example uses an IES service context.

- Associate IES 100 with **multicast-info-policy** *multicastinfopolicyname*.
- Create the video interface video-100.
- Create a video SAP and associate it with video group 1.
- Assigns an IP address 10.100.0.254 to the video interface and subnet 10.0.0.0/8.
- Name the main channel (S,G) = (192.168.9.10,234.4.5.228) "228" and the zone channel (S,G) = (10.100.100.1,234.4.5.228) "228-1".
- Configure the ad server (address = 10.200.14.2) and create IP addresses within the video interface subnet for SCTE 30 control traffic (10.1.1.2) and data traffic (10.1.1.3).
- The control and data addresses must be in the video interface subnet.

```
*A:ALA-49>config>service>ies# info
-----
...
    video-interface "video-100" create
        video-sap 1
        exit
        address 10.100.0.254/8
        adi
            channel 192.0.2.228 source 192.168.9.10 channel-name "228"
                scte35-action drop
                zone-channel 192.0.2.228 source 10.100.100.1 adi-channel-
name
"228-1"

            exit
            scte30
                ad-server 10.200.14.2
```

```
        local-address control 10.1.1.2 data 10.1.1.3
        exit
    exit
    no shutdown
exit
no shutdown
-----
*A:ALA-49>config>service>ies#
```

The source address (10.100.100.1) for the zone channel (S,G) and the local addresses (10.1.1.2 and 10.1.1.3) used for SCTE 30 communication must all be within the video interface subnet (10.0.0.0/8).

Connections are accepted from multiple ad-servers. This can be used for ad server redundancy.

If the main channel were a (*,G), the source address of 0.0.0.0 would have been specified.

Additional zone channels with distinct names could be configured within the service instance. In a practical configuration, the G for the main channel (192.0.2.228) will be the same for G in the zone channel (S,G) because the STBs will join the (*,G) at the A-server and D-server.

Configuring ADI for a VPRN service instance uses the same commands within the VPRN service context.

6.7 Video Services Command Reference

6.7.1 IP-TV Command Hierarchies

- [Hardware Commands](#)
- [Video Group Commands](#)
- [Video Policy Video Commands](#)
- [Bundle and Channel Commands](#)
- [Service Video Interface Commands](#)

6.7.1.1 Hardware Commands

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide* for hardware command descriptions.

6.7.1.2 Video Group Commands

```

config
  — isa
    — ins-group ins-group-id [create]
    — no ins-group ins-group-id
      — description description-string
      — no description
      — mda mda-id [drain]
      — no mda mda-id
      — port-policy policy-name
      — no port-policy
      — [no] shutdown
    — video-group video-group-id [create]
    — no video-group video-group-id
      — [no] ad-insert
      — [no] analyzer
      — description description-string
      — no description
      — [no] enable-rt-client
      — [no] fcc-server
      — [no] local-rt-server
      — [no] primary mda-id
      — resv-ret resv-ret
      — [no] shutdown
      — [no] stream-selection

```

- **watermark**
 - **bandwidth**
 - **fcc** *percent*
 - **ret** *percent*
 - **total** *percent*
 - **session**
 - **fcc** *percent*
 - **ret** *percent*
 - **total** *percent*

6.7.1.3 Video Policy Video Commands

```

config
— mcast-management
— multicast-info-policy policy-name [create]
— no multicast-info-policy policy-name
— video-policy
— video-interface ip-address [create]
— no video-interface ip-address
— fcc-session-timeout seconds
— no fcc-session-timeout
— hd
— dent-threshold threshold
— no dent-threshold
— fcc-burst burst-percentage
— no fcc-burst
— fcc-server [mode {burst | dent | hybrid}]
— no fcc-server
— [no] local-rt-server
— mc-handover percentage
— no mc-handover
— rt-rate rt-burst-percentage
— no rt-rate
— max-sessions sessions
— no max-sessions
— pip
— dent-threshold threshold
— no dent-threshold
— fcc-burst burst-percentage
— no fcc-burst
— fcc-server [mode {burst | dent | hybrid}]
— no fcc-server
— [no] local-rt-server
— mc-handover percentage
— no mc-handover
— rt-rate rt-burst-percentage
— no rt-rate
— rt-mcast-reply [count count] [interval milliseconds] [hold-time milliseconds]
— no rt-mcast-reply
— ret-session-timeout seconds

```

- **no ret-session-timeout**
- **rt-payload-type** *payload-type*
- **no rt-payload-type**
- **rt-rate** *rt-burst-percentage*
- **no rt-rate**
- **sd**
 - **dent-threshold** *threshold*
 - **no dent-threshold**
 - **fcc-burst** *burst-percentage*
 - **no fcc-burst**
 - **fcc-server** [mode {burst | dent | hybrid}]
 - **no fcc-server**
 - [no] **local-rt-server**
 - **mc-handover** *percentage*
 - **no mc-handover**
 - **rt-rate** *rt-burst-percentage*
 - **no rt-rate**
- **subscriber-bw-limit** *bandwidth*
- **no subscriber-bw-limit**

6.7.1.4 Bundle and Channel Commands

- ```
config
— mcast-management
 — multicast-info-policy policy-name [create]
 — no multicast-info-policy policy-name
 — bundle bundle-name [create]
 — no bundle bundle-name
 — admin-bw kbps
 — no admin-bw
 — bw-activity {use-admin-bw | dynamic [falling-delay seconds]} [black-
 hole-rate kbps]
 — no bw-activity
 — channel ip-address [ip-address] [create]
 — no channel ip-address [ip-address]
 — admin-bw kbps
 — no admin-bw
 — source-override ip-address [create]
 — no source-override ip-address
 — admin-bw kbps
 — no admin-bw
 — video
 — [no] analyzer
 — alarms
 — [no] cc-error
 — non-vid-pid-absent milli-seconds
 — no non-vid-pid-absent
 — pat-repetition [tnc tnc-milli-seconds qos qos-milli-seconds
 poa poa-milli-seconds]
 — no pat-repetition
```

- 
- [no] **pat-syntax**
  - **pcr-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
  - no **pcr-repetition**
  - [no] **pid-pmt-unref**
  - **pmt-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
  - no **pmt-repetition**
  - [no] **pmt-syntax**
  - **report-alarm** severity [tnc | qos | poa]
  - no **report-alarm**
  - [no] **tei-set**
  - [no] **ts-sync-loss**
  - **vid-pid-absent** milli-seconds
  - no **vid-pid-absent**
  - **description** description-string
  - no **description**
  - **fcc-channel-type** {hd | sd | pip}
  - no **fcc-channel-type**
  - **fcc-min-duration** time
  - no **fcc-min-duration**
  - **fcc-server** [disable]
  - no **fcc-server**
  - **local-fcc-port** port
  - no **local-fcc-port**
  - **local-rt-port** port
  - no **local-rt-port**
  - **local-rt-server** [disable]
  - no **local-rt-server**
  - **reorder-audio** time
  - no **reorder-audio**
  - **rt-buffer-size** rt-buffer-size
  - no **rt-buffer-size**
  - **rt-server** disable
  - **rt-server** ip-address port port-num
  - no **rt-server**
  - **video-group** video-group-id
  - no **video-group**
  - **video**
    - [no] **analyzer**
      - **alarms**
        - [no] **cc-error**
        - **non-vid-pid-absent** milli-seconds
        - no **non-vid-pid-absent**
        - **pat-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
        - no **pat-repetition**
        - [no] **pat-syntax**

- **pcr-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
- **no pcr-repetition**
- [no] **pid-pmt-unref**
- **pmt-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
- **no pmt-repetition**
- [no] **pmt-syntax**
- **report-alarm** severity [tnc | qos | poa]
- **no report-alarm**
- [no] **tei-set**
- [no] **ts-sync-loss**
- **vid-pid-absent** milli-seconds
- **no vid-pid-absent**
- **description** description-string
- **no description**
- **fcc-channel-type** {hd | sd | pip}
- **no fcc-channel-type**
- **fcc-min-duration** time
- **no fcc-min-duration**
- **fcc-server** [disable]
- **no fcc-server**
- **local-fcc-port** port
- **no local-fcc-port**
- **local-rt-port** port
- **no local-rt-port**
- **local-rt-server** [disable]
- **no local-rt-server**
- **reorder-audio** time
- **no reorder-audio**
- **rt-buffer-size** rt-buffer-size
- **no rt-buffer-size**
- **rt-server** disable
- **rt-server** ip-address port port-num
- **no rt-server**
- **video-group** video-group-id
- **video-group** disable
- **no video-group**
- **video**
  - [no] **analyzer**
  - **alarms**
    - [no] **cc-error**
    - **non-vid-pid-absent** milli-seconds
    - **no non-vid-pid-absent**
    - **pat-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
    - **no pat-repetition**
    - [no] **pat-syntax**
    - **pcr-repetition** [tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds]
    - **no pcr-repetition**
    - [no] **pid-pmt-unref**

---

```

— pmt-repetition [tnc tnc-milli-seconds qos qos-
 milli-seconds poa poa-milli-seconds]
— no pmt-repetition
— [no] pmt-syntax
— report-alarm severity [tnc | qos | poa]
— no report-alarm
— [no] tei-set
— [no] ts-sync-loss
— vid-pid-absent milli-seconds
— no vid-pid-absent
— [no] description
— fcc-channel-type {hd | sd | pip}
— no fcc-channel-type
— fcc-min-duration time
— no fcc-min-duration
— fcc-server [disable]
— no fcc-server
— local-fcc-port port
— no local-fcc-port
— local-rt-port port
— no local-rt-port
— local-rt-server [disable]
— no local-rt-server
— reorder-audio time
— no reorder-audio
— rt-buffer-size rt-buffer-size
— no rt-buffer-size
— rt-server disable
— rt-server ip-address port port-num
— no rt-server
— source-port port-num
— no source-port
— video-group video-group-id
— video-group disable
— no video-group

```

## 6.7.1.5 Service Video Interface Commands

### 6.7.1.5.1 VPLS Commands

```

config>service>vpls service-id
— multicast-info-policy policy-name
— no multicast-info-policy
— video-interface ip-int-name [create]
— no video-interface ip-int-name
 — [no] address ip-address/mask
 — cpu-protection policy-id
 — no cpu-protection
 — description description-string

```



- **no description**
- **gateway-ip** *ip-address*
- **no gateway-ip**
- **multicast-service** *service-id*
- **no multicast-service**
- **rt-client-src-address** *ip-address*
- **no rt-client-src-address**
- **[no] shutdown**
- **video-sap** *video-group-id*
- **no video-sap**
  - **egress**
    - **filter ip** *ip-filter-id*
    - **no filter**
    - **qos** *policy-id*
    - **no qos**
  - **ingress**
    - **filter ip** *ip-filter-id*
    - **no filter**
    - **qos** *policy-id*
    - **no qos**

#### 6.7.1.5.2 IES Commands

- ```
config>service>ies service-id
— video-interface ip-int-name [create]
— no video-interface ip-int-name
  — [no] address ip-address/mask
  — adi
    — scte30
      — [no] ad-server ip-address
      — local-address control ip-address data ip-address
      — no local-address
    — channel mcast-address source ip-address [channel-name channel-name]
    — no channel mcast-address source ip-address
      — description description-string
      — no description
      — scte35-action {forward | drop}
      — zone-channel mcast-address source ip-address adi-channel-name channel-
        name
      — no zone-channel mcast-address source ip-address
    — cpu-protection policy-id
    — no cpu-protection
    — description description-string
    — no description
    — multicast-service service-id
    — no multicast-service
    — rt-client-src-address ip-address
    — no rt-client-src-address
    — [no] shutdown
    — video-sap video-group-id
    — no video-sap
```

- **egress**
 - **filter ip** *ip-filter-id*
 - **no filter**
 - **qos** *policy-id*
 - **no qos**
- **ingress**
 - **filter ip** *ip-filter-id*
 - **no filter**
 - **qos** *policy-id*
 - **no qos**

6.7.1.5.3 VPRN Commands

VPRN service commands are only applicable to the 7750 SR.

```
config>service>vprn service-id
— video-interface ip-int-name [create]
— no video-interface ip-int-name
  — [no] address ip-address/mask
  — adi
    — scte30
      — [no] ad-server ip-address
      — local-address control ip-address data ip-address
      — no local-address
    — channel mcast-address source ip-address [channel-name channel-name]
    — no channel mcast-address source ip-address
      — description description-string
      — no description
      — scte35-action {forward | drop}
      — zone-channel mcast-address source ip-address adi-channel-name channel-
        name
      — no zone-channel mcast-address source ip-address
    — cpu-protection policy-id
    — no cpu-protection
    — description description-string
    — no description
    — multicast-service service-id
    — no multicast-service
    — rt-client-src-address ip-address
    — no rt-client-src-address
    — [no] shutdown
    — video-sap video-group-id
    — no video-sap
      — egress
        — filter ip ip-filter-id
        — no filter
        — qos policy-id
        — no qos
      — ingress
        — filter ip ip-filter-id
        — no filter
```

- qos *policy-id*
- no qos

6.7.2 Command Descriptions

- [Generic Commands](#)
- [LNS Group Commands](#)
- [Multicast Info Policy Commands](#)
- [Video Policy Commands](#)
- [Bundle and Channel Commands](#)
- [Service Video Interface Commands](#)

6.7.2.1 Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>isa>video-group config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video config>service>ies>video-interface config>service>vpls>video-interface config>service>vprn>video-interface config>service>ies>video-interface>channel config>service>vprn>video-interface>channel
Description	This command creates a text description stored in the configuration file for a configuration context. The description command associates a text string with a configuration context to help identify the context in the configuration file. The no form of this command removes any description string from the context.
Default	No description is associated with the configuration context.
Parameters	<i>description-string</i> — Specifies a text string describing the entity. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	config>isa>video-group config>service>ies>video-interface config>service>vpls>video-interface config>service>vprn>video-interface
Description	This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command. When an entity is disabled, the operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted. Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.
Default	no shutdown

6.7.2.2 LNS Group Commands

Ins-group

Syntax	Ins-group <i>ins-group-id</i> [create] no Ins-group <i>Ins-group-id</i>
Context	config>isa
Description	This command configures the ISA LNS group.
Parameters	<i>Ins-group-id</i> — Specified the LNS group ID. Values 1 to 4 create — Keyword required when first creating the configuration context. Once the context is created, one can navigate into the context without the create keyword.

mda

Syntax	mda <i>mda-id</i> [drain] no mda <i>mda-id</i>

Context	config>isa>Ins-group		
Description	This command configures an ISA LNS group MDA.		
Parameters	<i>mda-id</i> — Specifies the slot and MDA number for the primary video group ISA.		
	Values		
	slot/mda		
	slot	1 to 10 (depending on the chassis model)	
	mda	1 to 2	

port-policy

Syntax	port-policy <i>policy-name</i> no port-policy		
Context	config>isa>Ins-group		
Description	This command enables policies referenced in the config>port-policy context to be created under ports. These are the ports that link the carrier IOM to the ISA, and are hidden within the system (they cannot be created through the CLI). They are created automatically. Use the show port command to view information. Currently only the port scheduler policy is supported. Each Ins-esm port in the Ins-group receives an independent port scheduler instance. The port schedulers are instantiated in the carrier IOM on the Ins-esm ports that carry PPPoE traffic in the downstream direction towards the ISA before the PPPoE traffic is L2TP encapsulated. The no form of the command removes the policy name from the configuration.		
Default	no port-policy		
Parameters	<i>policy-name</i> — specifies the port policy of this LNS group.		

6.7.2.3 Video Group Commands

video-group

Syntax	video-group <i>video-group-id</i> [create] no video-group <i>video-group-id</i>		
Context	config>isa		
Description	This command configures an ISA video group.		

Parameters	<i>video-group-id</i> — Specifies a video group ID.
Values	1 to 4
create	— Keyword required when first creating the configuration context. Once the context is created, one can navigate into the context without the create keyword.

ad-insert

Syntax	[no] ad-insert
Context	config>isa>video-group
Description	This command enables the ad insert server for the group. Ad insertion cannot be enabled if an FCC server or local RT server is enabled. The no form of the command disables the server.
Default	no ad-insert

analyzer

Syntax	[no] analyzer
Context	config>isa>video-group
Description	This command specifies whether or not the video analyzer is enabled for all streams on this video group. The no form of the command disables the analyzer for the group.
Default	no analyzer

enable-rt-client

Syntax	[no] enable-rt-client
Context	config>isa>video-group
Description	By default, the video ISA has both client and server capability for RET (retransmission). The client capability can be disabled to enable higher performance The no form of the command enables higher performance.
Default	enable-rt-client

fcc-server

Syntax	[no] fcc-server
Context	config>isa>video-group
Description	This command enables the FCC server capability for the ISA video group. FCC server cannot be enabled if ad insertion or the local RET server is enabled. FCC server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the FCC server is disabled or if the video group is administratively disabled (shutdown). The no form of the command disables the FCC server.
Default	no fcc-server

local-rt-server

Syntax	[no] local-rt-server
Context	config>isa>video-group
Description	This command enables the local RET server for the group. A local RET server cannot be enabled if an FCC server or ad insertion is enabled. The no form of the command disables the server.
Default	no local-rt-server

primary

Syntax	[no] primary <i>mda-id</i>						
Context	config>isa>video-group						
Description	This command configures the primary video group ISA. Only one primary can be configured per video group when ad insertion is enabled. The maximum number of primaries per video-group for FCC and RD is 4.						
Parameters	<i>mda-id</i> — Specifies the slot and MDA number for the primary video group ISA. <table><tr><td>Values</td><td>slot/mda</td></tr><tr><td>slot</td><td>1 to 10 (depending on the chassis model)</td></tr><tr><td>mda</td><td>1 to 2</td></tr></table>	Values	slot/mda	slot	1 to 10 (depending on the chassis model)	mda	1 to 2
Values	slot/mda						
slot	1 to 10 (depending on the chassis model)						
mda	1 to 2						

resv-ret

Syntax	resv-ret <i>resv-ret</i>
Context	config>isa>video-group
Description	This command provides a mechanism to reserve an explicit amount of egress bandwidth, in Mb/s, for RET for all the ISAs within a video group. If the amount of egress bandwidth is less than the reserved amount, FCC requests are discarded and only RET requests processed. The bandwidth is dynamically adjusted per ISA within the video group if an ISA becomes operational/non-operational within the group.
Default	resv-ret 0

stream-selection

Syntax	[no] stream-selection
Context	config>isa>video-group
Description	This command specifies whether or not stream selection is enabled on this video group. The no form of the command disables stream-selection for the group.
Default	no stream-selection

watermark

Syntax	watermark
Context	config>isa>video-group
Description	This command enables the context to configure watermark parameters.

bandwidth

Syntax	bandwidth
Context	config>isa>video-group>watermark
Description	This command enables the context to configure watermark parameters based on the bandwidth.

session

Syntax	session
Context	config>isa>video-group>watermark
Description	This command enables the context to configure watermark parameters based on the session.

fcc

Syntax	fcc percent
Context	config>isa>video-group>watermark>bandwidth config>isa>video-group>watermark>session
Description	This command sets the watermark to trigger the SNMP trap if the FCC bandwidth or session exceeds the configured percentage. The bandwidth is the available egress bandwidth of the ISA. The SNMP trap is cleared when the consumption is lowered by 10%. For example, if the system resource of the available bandwidth is 10 Gb/s and the watermark is configured to be 90%, the SNMP trap is raised as the bandwidth exceeds 9 Gb/s (90% of 10 Gb/s). The SNMP trap is cleared when the bandwidth drops below 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s). The default value of the watermark is set at 90% of the system resources for both bandwidth and session.
Default	fcc 90
Parameters	<i>percent</i> — Specifies the percentage of the system resources per ISA.
Values	1 to 99

ret

Syntax	ret percent
Context	config>isa>video-group>watermark>bandwidth config>isa>video-group>watermark>session
Description	This command sets the watermark to trigger the SNMP trap if the RET bandwidth or session exceeds the configured percentage. The bandwidth is the available egress bandwidth of the ISA. The SNMP trap is cleared when the consumption is lowered by 10%. For example, if the system resource of the bandwidth available is 10 Gb/s and the watermark is configured to be 90%, the SNMP trap is raised as the bandwidth exceeds 9 Gb/s (90% of 10 Gb/s). The SNMP trap is cleared when the bandwidth drops below 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s). The default value of the watermark is set at 90% of the system resources for both bandwidth and session.
Default	ret 90

Parameters *percent* — Specifies the percentage of the system resources per ISA.
Values 1 to 99

total

Syntax **total** *percent*

Context config>isa>video-group>watermark>bandwidth
 config>isa>video-group>watermark>session

Description This command sets the watermark to trigger the SNMP trap if the combined FCC and RET bandwidth or session exceeds the configured percentage. The bandwidth is the available egress bandwidth of the ISA. The SNMP trap is cleared when the consumption is lowered by 10%. For example, if the system resource of the bandwidth available is 10 Gb/s and the watermark is configured to be 90%, the SNMP trap is raised as the bandwidth exceeds 9 Gb/s (90% of 10 Gb/s). The SNMP trap is cleared when the bandwidth drops below 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s). The default value of the watermark is set at 90% of the system resources for both bandwidth and session.

Default total 90

Parameters *percent* — Specifies the percentage of the system resources per ISA.
Values 1 to 99

6.7.2.4 Multicast Info Policy Commands

multicast-info-policy

Syntax **multicast-info-policy** *policy-name* [create]
 no multicast-info-policy *policy-name*

Context config>mcast-management

Description This command configures a multicast information policy. Multicast information policies are used to manage parameters associated with Layer 2 and Layer 3 multicast records. Multiple features use the configured information within the policy. The multicast ingress path manager uses the policy to decide the inactive and active state behavior for each multicast record using the ingress paths to the switch fabric. The egress multicast CAC function may use the policy information as a basis for allowing or disallowing downstream nodes to join multicast streams. The system's multicast ECMP join decisions are influenced by the channel information contained within the policy.

 Multicast Bundles:

- A multicast information policy consists of one or multiple named bundles. Multicast streams are mapped to a bundle based on matching the destination address of the multicast stream to configured channel ranges defined within the bundles. Each policy has a bundle named 'default' that is used when a destination address does not fall within any of the configured channel ranges.
- Each bundle has a set of default parameters used as the starting point for multicast channels matching the bundle. The default parameters may be overridden by optional exception parameters defined under each channel range. Further optional parameter overrides are possible under explicit source address contexts within each channel range.

Default Multicast Information Policy

- A multicast information policy always exists with the name 'default' and cannot be edited or deleted. The following parameters are contained in the default multicast information policy:

Table 31 **Default Multicast Information Policy Parameters**

Parameter	Description
Policy Description:	Default policy, cannot be edited or deleted.
Bundle:	default
Bundle Description:	Default Bundle, cannot be edited or deleted.
Congestion-Priority-Threshold:	4
ECMP-Optimization-Limit-Threshold:	7
Bundle Defaults:	
Administrative Bandwidth:	0 (undefined)
Preference:	0
CAC-Type:	Optional
Bandwidth Activity:	Dynamic with no black-hole rate
Explicit Ingress SF Path:	None (undefined)
Configured Channel Ranges:	None

- The default multicast information policy is applied to all VPLS and VPRN services and all routing contexts until an explicitly defined multicast information policy has been mapped.

Explicit Multicast Information Policy Associations

- Each VPLS service and each routing context (including VPRN routing contexts) supports an explicit association with an pre-existing multicast information policy. The policy may need to be unique per service or routing context due to the fact that each context has its own multicast address space. The same multicast channels may be and most likely will be used for completely different multicast streams and applications in each forwarding context.

Interaction with Ingress Multicast Path Management

- When ingress multicast path management is enabled on an FP, the system automatically creates a bandwidth manager context that manages the multicast path bandwidth into the switch fabric used by the ingress ports on the FP. As routing or snooping protocols generate L2 or L3 multicast FIB records that will be populated on the line card's forwarding plane, they are processed through the multicast information policy that is associated with the service or routing context associated with the record. The policy will return the following information for the record to be used by the ingress bandwidth manager:
 - The records administrative bandwidth ('0' if undefined)
 - Preference level (0 to 7 with 7 being highest)
 - Bandwidth activity monitoring setting (use admin bw or dynamic monitoring)
If admin bw is indicated, will also return active and inactive thresholds
 - Initial switch fabric multicast path (primary or secondary)
 - Explicit switch fabric multicast path (primary, secondary, or none)

Interaction with Egress Multicast CAC

- The egress multicast CAC feature has its own multicast CAC policy that is applied to egress IP interfaces or egress VPLS interfaces. The policy contains bundles, each with their own sets of channel ranges defined. When a multicast join event occurs on the interface, the system searches the multicast CAC policy to determine how that join event should be processed. The information returned from the CAC lookup provides the bundles allowed bandwidth and the channels administrative bandwidth. Since the allowed bundle bandwidth may change between differing egress interfaces, multiple policies with the same channel information may be needed.

With the addition of the multicast information policy, managing the CAC feature is simplified. The CAC monitor for the egress interface first searches the multicast CAC policy to determine if the multicast join event matches a configured channel range. If a match is found, it simply uses the local policy information. If a match is not found, it then searches the multicast information policy associated with the service or routing context to which the join event is associated. The multicast information policy returns the following information to the interfaces CAC manager:

- Bundle name
- Administrative bandwidth ('0' if undefined)
- Congestion Priority Threshold (high or low)
- CAC Type (mandatory or optional)

The CAC manager evaluates the returned results according to the following rules:

- If the returned administrative bandwidth = '0', all results are ignored
- If the returned bundle name is not found in the local multicast CAC policy, all results are ignored
- The administrative bandwidth is interpreted as channel 'bw'
- A value of 'high' for congestion priority threshold is interpreted as 'class high'
- A value of 'low' for congestion priority threshold is interpreted as 'class low'
- A value of 'mandatory' for CAC type is interpreted as 'type mandatory'
- A value of 'optional' for CAC type is interpreted as 'type optional'
- Bundle bandwidth is always derived from the local multicast CAC policy

Using the multicast information policy to store the CAC information allows a single centralized managed policy for all channel information, allowing the multicast CAC policies to only have bundle defined with the appropriate bundle bandwidth. The multicast CAC policy still may be for channel information in exception cases.

Interaction with Multicast ECMP Optimization

The multicast information policy is used by the multicast ECMP optimization function to derive each channels administrative bandwidth. The ECMP function tallies all bandwidth information for channels joined and attempts to equalize the load between the various paths to the sender. The multicast information policy returns the following information to the ECMP path manager:

1. Administrative bandwidth ('0' if undefined)
2. Preference (0 to 7 with 7 the highest preference value)

Parameters *policy-name* — Identifies the name of the policy to be either created or edited. Each multicast information policy must be uniquely named within the system. Names of up to 32 ASCII characters are supported with the normal character restrictions.

create — The create keyword is required if creating a new multicast information policy when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the multicast information policy name already exists.

multicast-info-policy

Syntax **multicast-info-policy** *policy-name*
no multicast-info-policy

Context config>service>ies
config>service>vpls
config>service>vprn

	config>router
Description	This command overrides the default multicast information policy on a service or routing context. When the policy association is changed, all multicast channels in the service or routing context must be reevaluated. If a multicast information policy is not explicitly associated with the service or routing context, the default multicast information policy is used when ingress multicast path management is enabled. While a multicast information policy is associated with a service or routing context, the policy cannot be deleted from the system. The no form of the command removes an explicit multicast information policy from the service or routing context and restores the default multicast information policy.
Parameters	<i>policy-name</i> — The <i>policy-name</i> parameter is required and specifies an existing multicast information policy that should be associated with the service or routing context. Default default

bundle

Syntax	bundle <i>bundle-name</i> [create] no bundle <i>bundle-name</i>
Context	config>mcast-mgmt>mcast-info-plcy
Description	This command is used to create or edit channel bundles within a multicast information policy. Bundles are used for two main purposes. First, bundles are used by the multicast CAC function to group multicast channels into a common bandwidth context. The CAC function limits the ability for downstream nodes to join multicast channels based on the egress interfaces ability to handle the multicast traffic. Bundling allows multicast channels with common preference or application to be managed into a certain percentage of the available bandwidth. The second function of bundles is to provide a simple provisioning mechanism. Each bundle within a multicast information policy has a set of default channel parameters. If each channel provisioned in to the bundle is able to use the default parameters for the bundle, the provisioning and configuration storage requirements are minimized. Up to 31 explicit bundles may be defined within a multicast information policy (32 including the default bundle). Once a bundle is created, the default channel parameters should be configured and the individual channel ranges should be defined. Within each channel range, override parameters may be defined that override the default channel parameters. Further overrides are supported within the channel range based on explicit source overrides.

A bundle may be deleted at any time (except for the default bundle). When a bundle is deleted, all configuration information within the bundle is removed including multicast channel ranges. Any multicast records using the bundle should be reevaluated. Multicast CAC and ECMP managers should also be updated.

Default Bundle

Each multicast information policy contains a bundle named “default”. The default bundle cannot be deleted. Any multicast channel that fails to match a channel range within an explicit bundle is automatically associated with the default bundle.

The **no** form of the command removes a bundle from the multicast information policy. The default bundle cannot be removed from the policy.

Default	bundle default
Parameters	<i>bundle-name</i> — Specifies bundle expressed as an ASCII string with up to 16 characters and must follow normal naming conventions. If bundle-name already exists, the system will enter the bundle context for editing purposes. If bundle-name does not exist, the system will create the defined bundle in the policy and enter the bundle context for editing purposes. create — The create keyword is required if creating a new multicast information policy bundle when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the bundle name already exists.

admin-bw

Syntax	admin-bw <i>kbps</i> no admin-bw
Context	config>mcast-mgmt>mcast-info-plcy>bundle config>mcast-mgmt>mcast-info-plcy>bundle>channel
Description	This command configures the administrative bandwidth.
Parameters	<i>kbps</i> — Specifies the administrative bandwidth in kb/s. Values 1 to 40000000

bw-activity

Syntax	bw-activity { use-admin-bw dynamic [<i>falling-delay seconds</i>]} [black-hole-rate <i>kbps</i>] no bw-activity
Context	config>mcast-mgmt>mcast-info-plcy>bundle

```
config>mcast-mgmt>mcast-info-plcy>bundle>channel
```

Description

This command defines how the multicast ingress path manager determines the amount of bandwidth required by a multicast channel. The default setting is dynamic which causes the bandwidth manager to adjust the path bandwidth based on the current ingress multicast bandwidth. The alternative setting is use-admin-bw which causes the bandwidth manager to use the configured admin-bw associated with the channel. The use-admin-bw setting is enabled once the channels ingress bandwidth reaches the bandwidth-policy admin-bw-threshold value. The bandwidth manager uses the dynamic method until the threshold has been reached. If the ingress bandwidth falls below the threshold, the bandwidth manager reverts back to the dynamic method.

While operating in dynamic bandwidth mode, the bandwidth manager uses the falling-delay threshold to hold on to the previous highest bandwidth until the delay time has expired. This allows the bandwidth manager ignore momentary drops in channel bandwidth.

The **bw-activity** command in the bundle context defines how the current bandwidth is derived for all channels associated with the bundle unless the channel has an overriding bw-activity defined in the channel context. The channel context may also be overridden by the **bw-activity** command in the source-override context for a specific channel or channel range. The channel and source-override bw-activity settings default to 'null' (undefined) and have no effect unless explicitly set. The default-channel-info bw-activity default value is set to dynamic.

The use-admin-bw setting requires that the channel be configured with an admin-bw value that is not equal to '0' in the same context as the **bw-activity** command using the setting. If use-admin-bw is defined in the default-channel-info context, then the default-channel-info admin-bw setting must not be set to '0'. A similar rule applies for channel and source-override bw-activity and admin-bw settings. Once a context has use-admin-bw configured, the context's admin-bw value cannot be set to '0' and the **no admin-bw** command will fail for that context.

The **bw-activity** command also supports an optional black-hole-rate kilobits-per-second keyword and parameter that defines at which current rate a channel should be placed in the black-hole state. This is intended to provide a protection mechanism against multicast channels that exceed a reasonable rate and cause outages in other channels.

The **no** form of the command reverts to the default parameters.

channel

Syntax **channel** *ip-address* [*ip-address*] [**create**]
 no channel *ip-address* [*ip-address*]

Context config>mcast-mgmt>mcast-info-plcy>bundle

Description	This command defines explicit channels or channel ranges that are associated with the containing bundle. A channel or channel range is defined by their destination IP addresses. A channel may be defined using either IPv4 or IPv6 addresses. If a channel range is being defined, both the start and ending addresses must be the same type. A specific channel may only be defined within a single channel or channel range within the multicast information policy. A defined channel range cannot overlap with an existing channel range. If a channel range is to be shortened, extended, split or moved to another bundle, it must first be removed from its existing bundle. Each specified channel range creates a containing context for any override parameters for the channel range. By default, no override parameters exist. The no form of the command removes the specified multicast channel from the containing bundle.
Parameters	start-channel-ip-address [<i>end-channel-ip-address</i>] — The start-channel-ip-address parameter and optional end-channel-ip-address parameters define the starting and ending destination IP addresses for a channel range. If only the start-channel-ip-address is given, the channel ranges comprises of a single multicast channel. If both the starting and ending address are specified, all addresses within the range including the specified address are part of the channel range. IPv4 or IPv6 addresses may be defined. All specified addresses must be valid multicast destination addresses. The starting IP address must be numerically lower than the ending IP address. Values Any valid IP multicast destination address Default None create — The create keyword is required if creating a new multicast channel range when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified channel range already exists.

source-override

Syntax	source-override <i>ip-address</i> [create] no source-override <i>ip-address</i>
Context	config>mcast-mgmt>mcast-info-plcy>bundle>channel
Description	This command defines a multicast channel parameter override context for a specific multicast sender within the channel range. The specified senders IP address must be of the same type (IPv4 or IPv6) as the containing channel range.

The **no** form of the command removes the specified sender override context from the channel range.

Default none

Parameters *ip-address* — Specifies either an IPv4 or IPv6 address and it must be the same type as the containing channel range.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

create — This keyword is required if creating a new source override when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified source override IP address already exists.

6.7.2.5 Video Policy Commands

video-policy

Syntax **video-policy**

Context config>mcast-mgmt>mcast-info-plcy

Description This command enables the context to configure video interfaces and video services.

video-interface

Syntax **video-interface** *ip-address* [**create**]
no video-interface *ip-address*

Context config>mcast-mgmt>mcast-info-plcy>video-policy

Description This command creates a video interface policy context that correlates to the IP address assigned for a video interface. This interface is created in a subscriber service to which the multicast information policy is assigned. If the specified IP address does not correlate to a video interface IP address, the parameters defined within this context have no effect.

The **no** form of the command deletes the video interface policy context.

- Parameters** *ip-address* — The IP address of a video interface provisioned within the context of a service to which the Multicast Information Policy is assigned. If the IP address does not match the IP address assigned to a video interface, the parameters defined within this context have no effect.
- create** — Mandatory keyword needed when creating a new video interface within the video policy.

fcc-session-timeout

- Syntax** **fcc-session-timeout** *seconds*
no fcc-session-timeout
- Context** config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
- Description** By default, the video ISA will wait for 5 minutes before closing the RTCP session from the subscriber. The RTCP session can be adjusted from 5 second to 5 minutes. The timeout is applicable to both RET and FCC RTCP sessions.
- The **no** form of the command reverts to the default.
- Default** fcc-session-timeout 300
- Parameters** *seconds* — Specifies the FCC session timeout in seconds.
- Values** 5 to 300

hd

- Syntax** **hd**
- Context** config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
- Description** This command configures properties relating to requests received by the video interface for High Definition (HD) channel requests.
- Default** none

dent-threshold

- Syntax** **dent-threshold** *threshold*
no dent-threshold
- Context** config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip

config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description	This command sets the threshold value below which the FCC server will dent/drop unicast data sent to the FCC client during a fast channel change. Within the RTP extension header, the packet priority (PRI) (2 bits) and the fine-grained priority (FPRI) (3 bits) indicate the “importance” of the frame as to how essential it is to the video stream. This parameter is only applicable if the FCC server mode is dent. The no form of the command returns the parameter to the default value.
Default	dent-threshold 16 (only B frames are dropped)
Parameters	<i>threshold</i> — The threshold value is used by the FCC server to compare with the concatenation of the PRI and FPRI to determine whether to send the packet to the FCC client. If the PRI and FPRI expressed as a decimal integer is greater than or equal to the threshold value, the packet will be sent. Values 1 to 31

fcc-burst

Syntax	fcc-burst <i>burst-percentage</i> no fcc-burst				
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd				
Description	This command sets the burst rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client above the received rate to allow the client to catchup to the multicast stream. This parameter is only applicable if the FCC server mode is burst. The no form of the command returns the parameter to the default value.				
Default	fcc-burst 25				
Parameters	<i>burst-percentage</i> — Specifies the percentage of nominal bandwidth used to catch up to the multicast stream. Values <table><tr><td>HD:</td><td>0 to 100</td></tr><tr><td>SD and PIP:</td><td>0 to 600</td></tr></table> Default 25	HD:	0 to 100	SD and PIP:	0 to 600
HD:	0 to 100				
SD and PIP:	0 to 600				

fcc-server

Syntax	fcc-server [mode { burst dent hybrid }] no fcc-server
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd
Description	This command enables the Fast Channel Change (FCC) server and sets the mode to send the FCC unicast stream. The mode indicates how the FCC server will send information to the client. When burst is specified, the FCC server will send the channel at a nominally faster rate than the channel was received based on the applicable fcc-burst setting. When dent is specified, the FCC server will selectively discard frames from the original stream based on the applicable dent-threshold setting. If no mode is specified, burst is the default mode. The no form of the command disables the FCC server at that context and subordinate contexts.
Default	no fcc-server
Parameters	mode burst — Sets the mode of the FCC server to burst when sending the channel to the FCC client. mode dent — Sets the mode of the FCC server to dent when sending the channel to the FCC client. mode hybrid — Combines the burst and dent modes.

local-rt-server

Syntax	[no] local-rt-server
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd
Description	This command enables the local retransmission server function for requests directed to the IP address. The no form of the command disables the retransmission server.
Default	no local-rt-server

mc-handover

Syntax	mc-handover <i>percentage</i>

no mc-handover

Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd				
Description	This command sets the rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client during the handover to the multicast stream. The no form of the command returns the parameter to the default value.				
Default	mc-handover 25				
Parameters	<i>percentage</i> — Specifies the percentage of nominal bandwidth.				
Values	<table><tr><td>HD:</td><td>0 to 100</td></tr><tr><td>SD and PIP:</td><td>0 to 600</td></tr></table>	HD:	0 to 100	SD and PIP:	0 to 600
HD:	0 to 100				
SD and PIP:	0 to 600				
Default	25				

rt-mcast-reply

Syntax	rt-mcast-reply [count <i>count</i>] [interval <i>milliseconds</i>] [hold-time <i>milliseconds</i>] no rt-mcast-reply
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
Description	This command enables the use of multicast retransmission packets by the retransmission server in response to a number of identical retransmission requests. By default, the retransmission server replies to all retransmission requests with a unicast stream directed to the client requesting retransmission. Enabling multicast retransmission on the retransmission server is an optimization where a number of identical retransmission requests received will trigger the retransmission server to service the retransmission request with a single multicast reply stream with packets of Payload Type 33. An example of where multiple clients will request retransmission for identical packets is if there is a packet loss in the Access Network which affects multiple clients. For clients that received the original packets or requested retransmission and had the retransmission serviced in unicast, the multicast retransmission will look like duplicate packets and discard the multicast retransmitted packets. For other clients, the multicast retransmission will look like out-of-sequence multicast packets, so the client must support reception of out of sequence multicast for multicast retransmission for multicast retransmission to be used.

The threshold value for identical retransmission requested received by the retransmission server is configured when enabling multicast retransmission along with a sample interval and a hold time. The sample interval is the elapsed time over which the retransmission requests are counted. The hold time is a quiet period after a multicast retransmission is triggered on the retransmission server where an identical retransmission request will be ignored. After the hold time expires, a new sampling interval is started. Sampling intervals will be restarted until the packets for the multicast request are cleared from the retransmission buffer.

To illustrate the threshold count, sample interval and hold time, suppose the values are 5, 100 ms and 50 ms, respectively. The first retransmission request arrives at time = 0. In one scenario, assume the fifth identical retransmission request arrives at the server at time = 60 ms. In this case, the first four retransmission requests are serviced as unicast and the arrival of the fifth retransmission request triggers a multicast retransmission. All identical retransmission requests received between time = 60 and 110 ms are ignored. At time = 110 ms, a new sampling period is started and retransmission requests are serviced in unicast unless the threshold is passed again in the new sampling period. For a second scenario, assume the fifth identical retransmission request arrives at time = 25 ms. In this scenario, the behavior is the same except the new sampling period starts at time = 75 ms even though this is before the original sampling period was set to expire.

The **no** form of the command disables retransmissions using multicast, so all retransmissions will be sent as unicast.

Default no rt-mcast-reply – Retransmission requests will only be serviced with unicast retransmission replies.

Parameters **count** *count* — Specifies the number of identical retransmission requests received for a packet in a sampling interval after which a reply will be sent as multicast Payload Type 33.

Values 2 to 1024

Default 5

interval *milliseconds* — Specifies the number of milliseconds for a sampling interval.

Values 100 to 8000 ms

Default 100 ms

hold-time *milliseconds* — Specifies the number of milliseconds after a multicast reply is sent that the retransmission server will wait before starting a new sampling period

ret-session-timeout

Syntax **ret-session-timeout** *seconds*
no ret-session-timeout

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description	By default, the video ISA will wait for 5 minutes before closing the RTCP session from the subscriber. The RTCP session can be adjusted from 5 second to 5 minutes. The timeout is applicable to both RET and FCC RTCP sessions. The no form of the command reverts to the default.
Default	ret-session-timeout 300
Parameters	<i>seconds</i> — Specifies the RET session timeout, in seconds. Values 5 to 300

rt-payload-type

Syntax	rt-payload-type <i>payload-type</i> no rt-payload-type
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
Description	This command describes the format to be used by Retransmission (RT) server to send retransmission packets. The RET server interface allows the payload type within the retransmission packets to be configured.
Default	rt-payload-type 99 — Indicates that the frames will be sent in the RFC 4588, <i>RTP Retransmission Payload Format</i> , format.
Parameters	<i>payload-type</i> — Indicates the format expected for received retransmission packets. The value 33 indicates that the frames will be received as originally sent. A value between 96 and 127 indicates the dynamic payload type value (per RFC 3551) to be used for RFC 4588 formatted retransmission packets. Values 33, 96 to 127

rt-rate

Syntax	rt-rate <i>rt-burst-percentage</i> no rt-rate
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip config>mcast-mgmt>mcast-info-plcy>video-policy>video-if config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd
Description	This command sets the rate of nominal bandwidth at which retransmission packets are sent to the retransmission client for requests directed to the IP address. The no form of the command returns the parameter to the default value.
Default	rt-rate 5

Parameters	<i>rt-burst-percentage</i> — Specifies the percentage of nominal bandwidth to send retransmission packets.
Values	1 to 100
Default	5

max-sessions

Syntax	max-sessions <i>sessions</i> no max-sessions
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
Description	This command configures the per-client maximum number of sessions. The no form of the command reverts to the default value.
Default	max-sessions 256
Parameters	<i>sessions</i> — Specifies the per-client maximum number of sessions.
Values	1 to 65536
Default	256

pip

Syntax	pip
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
Description	This command enables the context within a video interface policy to configure properties relating to requests received by the video interface for Picture-in-Picture (PIP) channel requests.
Default	none

sd

Syntax	sd
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
Description	This command enables the context within a video interface policy to configure properties relating to requests received by the video interface for Standard Definition (SD) channel requests.

subscriber-bw-limit

Syntax	subscriber-bw-limit <i>bandwidth</i> no subscriber-bw-limit
Context	config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
Description	This command configures of an egress per-subscriber bandwidth limit for the combined retransmission and Fast Channel Change (FCC) replies for requests received directed to the IP address. If the bandwidth for a request will exceed the bandwidth limit, the request is logged and dropped. The no form of the command disables enforcement of an egress bandwidth limit.
Default	no subscriber-bw-limit
Parameters	<i>bandwidth</i> — The per-subscriber egress bandwidth limit for retransmission and FCC packets in kilobits per second expressed as an integer indicates infinity or no limit.
Values	1 to 4294967295 kb/s

6.7.2.6 Bundle and Channel Commands

video

Syntax	video
Context	config>mcast-mgmt>mcast-info-plcy>bundle config>mcast-mgmt>mcast-info-plcy>bundle>channel config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override
Description	This command enables the context to configure video parameters.

analyzer

Syntax	[no] analyzer
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command enables or disables the analyzer for the group.

alarms

Syntax	alarms
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer
Description	This command enters the context to configure alarms for the analyzer (VQM).

cc-error

Syntax	[no] cc-error
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check the continuity counter. The continuity counter should be incremented per PID; otherwise, it is considered a continuity counter error.
Default	no cc-error

non-vid-pid-absent

Syntax	non-vid-pid-absent <i>milli-seconds</i> no non-vid-pid-absent		
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms		
Description	This command configures the analyzer to check for a PID within the specified interval.		
Default	no non-vid-pid-absent		
Parameters	<i>milli-seconds</i> — Specifies the interval, in milliseconds. <table><tr><td>Values</td><td>100 to 5000</td></tr></table>	Values	100 to 5000
Values	100 to 5000		

pat-repetition

Syntax	pat-repetition [<i>tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds</i>] no pat-repetition

Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for the program association table (PAT). It is expected that the PAT arrives periodically within a certain interval range. It is possible to configure the type of alarm that is raised when the PAT fails to arrive within the specified interval. As the delay increases between two consecutive PATs, the type of alarm raised becomes more critical, from TNC to POA.
Default	no pat-repetition
Parameters	<i>tnc-milli-seconds</i> — Specifies the time, in milliseconds, for which a TNC alarm is raised if the interval between two consecutive PATs is greater than or equal to this configured value. Values 100 to 800 in multiples of 100 only Default 100 <i>qos-milli-seconds</i> — Specifies the time, in milliseconds, for which a QoS alarm is raised if the interval between two consecutive PATs is greater than or equal to this configured value. Values 200 to 900 in multiples of 100 only and higher than the <i>tnc-milli-seconds</i> value Default 200 <i>poa-milli-seconds</i> — Specifies the time, in milliseconds, for which a POA alarm is raised if the interval between two consecutive PATs is greater than or equal to this configured value. Values 300 to 1000 in multiples of 100 only and higher than the <i>qos-milli-seconds</i> value Default 500

pat-syntax

Syntax	[no] pat-syntax
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for PAT syntax errors.
Default	no pat-syntax

pcr-repetition

Syntax	pcr-repetition [<i>tnc tnc-milli-seconds qos qos-milli-seconds poa poa-milli-seconds</i>] no pcr-repetition
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for the program clock reference (PCR). It is expected that the PCR arrives periodically within a certain interval range. It is possible to configure the type of alarm that is raised when the PCR fails to arrive within the specified interval. As the delay increases between two consecutive PCRs, the type of alarm raised becomes more critical, from TNC to POA.
Default	no pcr-repetition
Parameters	<i>tnc-milli-seconds</i> — Specifies the time, in milliseconds, for which a TNC alarm is raised if the interval between two consecutive PCRs is greater than or equal to this configured value. Values 100 to 800 in multiples of 100 only Default 100 <i>qos-milli-seconds</i> — Specifies the time, in milliseconds, for which a QoS alarm is raised if the interval between two consecutive PCRs is greater than or equal to this configured value. Values 200 to 900 in multiples of 100 only and higher than the <i>tnc-milli-seconds</i> value Default 200 <i>poa-milli-seconds</i> — Specifies the time, in milliseconds, for which a POA alarm is raised if the interval between two consecutive PCRs is greater than or equal to this configured value. Values 300 to 1000 in multiples of 100 only and higher than the <i>qos-milli-seconds</i> value Default 500

pid-pmt-unref

Syntax	[no] pat-syntax
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms

```
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-
override>video>analyzer>alarms
```

Description This command configures the analyzer to check for unreferenced PIDs that have not been referred in the PMT.

Default no pid-pmt-unref

pmt-repetition

Syntax **pcr-repetition** [**tnc** *tnc-milli-seconds* **qos** *qos-milli-seconds* **poa** *poa-milli-seconds*]
no pcr-repetition

Context config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-
override>video>analyzer>alarms

Description This command configures the analyzer to check for the program map table (PMT). It is expected that the PMT arrives periodically within a certain interval range. It is possible to configure the type of alarm that is raised when the PMT fails to arrive within the specified interval. As the delay increases between two consecutive PMTs, the type of alarm raised becomes more critical, from TNC to POA.

Default no pmt-repetition

Parameters *tnc-milli-seconds* — Specifies the time, in milliseconds, for which a TNC alarm is raised if the interval between two consecutive PMTs is greater than or equal to this configured value.

Values 100 to 4800 in multiples of 100 only

Default 400

qos-milli-seconds — Specifies the time, in milliseconds, for which a QoS alarm is raised if the interval between two consecutive PMTs is greater than or equal to this configured value.

Values 200 to 4900 in multiples of 100 only and higher than the *tnc-milli-seconds* value

Default 800

poa-milli-seconds — Specifies the time, in milliseconds, for which a POA alarm is raised if the interval between two consecutive PMTs is greater than or equal to this configured value.

Values 300 to 5000 in multiples of 100 only and higher than the *qos-milli-seconds* value

Default 2000

pmt-syntax

Syntax	[no] pat-syntax
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for PMT syntax errors.
Default	no pmt-syntax

report-alarm

Syntax	report-alarm severity {tnc qos poa} no report-alarm
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the type of alarm to monitor and raise through SNMP. The severity of alarms increases from TNC, to QoS, and then to POA. For example, if QoS alarms are configured, the analyzer only raises alarms and events related to QoS. The analyzer may raise alarms for POA events if they occur, but alarms for TNC are not sent.
Default	no report-alarm
Parameters	severity — Keyword to configure the type of alarm. tnc — Specifies to monitor and raise alarms for TNC events. qos — Specifies to monitor and raise alarms for QoS events. poa — Specifies to monitor and raise alarms for POA events.

tei-set

Syntax	[no] tei-set
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for TEI set errors.
Default	no tei-set

ts-sync-loss

Syntax	[no] ts-sync-loss
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for synchronization loss errors.
Default	no ts-sync-loss

vid-pid-absent

Syntax	vid-pid-absent <i>milli-seconds</i> no vid-pid-absent
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms
Description	This command configures the analyzer to check for a VID PID within the specified time interval.
Default	no vid-pid-absent
Parameters	<i>milli-seconds</i> — Specifies the time, in milliseconds, for which to check for a VID PID. Values 100 to 5000

fcc-channel-type

Syntax	fcc-channel-type { hd sd pip } no fcc-channel-type
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command configures the channel type for the bundle/channel. The channel type is used in the video policy to set various Fast Channel Change (FCC) parameters including the type of FCC and various FCC rates. The no form of the command returns the parameter to the default value.
Default	no fcc-channel

- Parameters**
- hd** — The channel type is High-Definition (HD) (Default).
 - sd** — The channel type is Standard Definition (SD).
 - pip** — The channel type is Picture in Picture (PIP).

fcc-min-duration

- Syntax** **fcc-min-duration** *time*
no fcc-min-duration
- Context** config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
- Description** This command configures the minimum time duration, in milliseconds, of the Fast Channel Change (FCC) burst. The value of this object determines the starting point of the FCC burst. If the current Group of Pictures (GOP) has less than the minimum duration worth of data, FCC burst begins from the previous GOP.
- The **no** form of the command reverts to the default value.
- Default** fcc-min-duration 300
- Parameters** *time* — Specifies the FCC burst minimum duration, in milliseconds.
- Values** 300 to 8000

fcc-server

- Syntax** **fcc-server** [**disable**]
no fcc-server
- Context** config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
- Description** This command enables Fast Channel Change (FCC) for a multicast bundle or channel. Additional parameters such as **fcc-channel-type** should also be configured to match the characteristics of the bundle/channel.
- The **no** form of the command disables removes the FCC configuration for the bundle/channel context and implies the setting is inherited from a higher context or the default policy.
- Default** no fcc
- Parameters** **disable** — Explicitly disables the FCC server within the policy. For the default bundle within the default multicast information policy, the **no** form of the command and the **disable** keyword have the same meaning and imply that the server is disabled.

local-fcc-port

Syntax	local-fcc-port <i>port</i> no local-fcc-port
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command configures the local port on which Fast Channel Change (FCC) requests are received. The value of this object can only be set for the default bundle and will be used by all bundles and channels. The local-fcc-port <i>port</i> value is the only configuration parameter in the bundle “default” context. The no form of the command removes the port from the video configuration.
Parameters	<i>port</i> — Specifies a local port for FCC requests. Values 1024 to 5999, 6251 to 65535

local-rt-port

Syntax	local-rt-port <i>port</i> no local-rt-port
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command configures the local port on which retransmission (RET) requests are received. The value of this object can only be set for the default bundle and will be used by all channels. The local-rt-port <i>port</i> value is the only configuration parameter in the bundle “default” context. The no form of the command removes the port from the video configuration.
Parameters	<i>port</i> — Specifies a local port for RT requests. Values 1024 to 5999, 6251 to 65535

local-rt-server

Syntax	local-rt-server [disable] no local-rt-server

Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command enables the local retransmission server capability on the ISA video group. RET server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the RET server is disabled or if the video group is administratively disabled (shutdown). The no form of the command returns the parameter to the default value where the RET server is disabled on the video group.
Default	no local-rt-server
Parameters	disable — Specifies to disable the RET server.

reorder-audio

Syntax	reorder-audio <i>time</i> no reorder-audio
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
Description	This command configures the time, in milliseconds, by which the audio packets are reordered in the ad stream. Configuring this parameter depends on what is configured on the A Server and the GOP sizes of the network stream. Typically, this configuration should match the A Server configuration. The no form of the command removes the time value from the configuration.
Default	no reorder-audio
Parameters	<i>time</i> — Specifies the audio reorder time, in milliseconds.
	Values 100 to 1000

rt-buffer-size

Syntax	rt-buffer-size <i>rt-buffer-size</i> no rt-buffer-size
Context	config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command configures the retransmission buffer for channels within the bundle or channel range.

The **no** form of the command returns the parameter to the default value.

Default	300
Parameters	<i>rt-buffer-size</i> — Specifies the buffer size, in milliseconds, to store channel packets.
Values	300 to 8000

rt-server

Syntax	rt-server disable rt-server <i>ip-address</i> port <i>port-num</i> no rt-server
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command enables and configures the upstream retransmission server configuration parameters. The no form of the command removes the upstream retransmission server configuration and implies the configuration is inherited from a higher context or from the default policy.
Default	no rt-server – The upstream retransmission server settings are inherited.
Parameters	disable — This keyword explicitly disables the upstream retransmission server within the policy. For the default bundle within the default Multicast Information Policy, the no form of the command and the disable keyword have the same meaning and imply the server is disabled. <i>ip-address</i> — The IP address of the upstream retransmission server. port <i>num</i> — The UDP port to use to send RET requests to the upstream RET server. Values 1024 to 5999, 6251 to 65535

source-port

Syntax	source-port <i>port-num</i> no source-port
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video
Description	This command configures the source port for upstream RET requests. The source-port <i>port-num</i> value is the only configuration parameter in the bundle “default” context. The no form of the command removes the value from the configuration.

Parameters	<i>port-num</i> — Specifies the source port in the received RTP multicast stream.
Values	1024 to 65535

video-group

Syntax	video-group <i>video-group-id</i> video-group disable no video-group
Context	config>mcast-mgmt>mcast-info-plcy>bundle>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>video config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video
Description	This command assigns a video group ID to the channel.
Parameters	<i>video-group-id</i> — specifies the identifier for this video group. The video group must have been configured in the config>isa context.
Values	1 to 4
	disable — Explicitly disables the video group within the policy.

6.7.2.7 Service Video Interface Commands

video-interface

Syntax	video-interface <i>ip-int-name</i> [create] no video-interface <i>ip-int-name</i>
Context	config>service>ies config>service>vpls config>service>vprn
Description	This command creates a video interface within the service. The video interface and associated IP addresses are the addresses to which clients within the service will send requests. The video interface must be associated with an ISA group using the video-sap command and have IP addresses for it to be functional. The no form of the command deletes the video interface. The video interface must be administratively shut down before issuing the no video-interface command.
Default	none

- Parameters** *ip-int-name* — Specifies the name of the video interface, up to 32 characters. An interface name cannot be in the form of an IP address. If the string contains special characters (#, \$, spaces, and so on), the entire string must be enclosed within double quotes.
- create** — This keyword is mandatory when creating a video interface.

address

- Syntax** **[no] address** *ip-address/mask*
- Context** config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface
- Description** This command assigns an IP address to the video interface within the service. Video interface IP addresses are used by video service clients to direct requests for video server services. Up to 16 IP address/subnets can be defined. The addresses defined must all be distinct and cannot be contained within a previously defined address. In the VPLS context, only one IP address can be defined for a video interface.
- The **no** form of the command deletes the IP address/subnet from the video interface.
- Default** none
- Parameters** *ip-address* — Specifies the IP address/subnet of the video interface in dotted decimal notation.
- mask* — Specifies the subnet mask length for the IP address expressed as an integer.

adi

- Syntax** **adi**
- Context** config>service>ies>video-interface
config>service>vprn>video-interface
- Description** This command enables the context to configure ad insertion (ADI) for the video interface.

channel

- Syntax** **channel** *mcast-address* **source** *ip-address* [**channel-name** *channel-name*]
no channel *mcast-address* **source** *ip-address*
- Context** config>service>ies>video-interface
config>service>vprn>video-interface
- Description** This command configures channel parameters for ad insertion.

- Parameters** *mcast-address* — Specifies the multicast address.
- source** *ip-address* — Specifies the source IP address.
- channel-name** *channel-name* — Specifies the channel name up to 32 characters in length.

cpu-protection

- Syntax** **cpu-protection** *policy-id*
 no cpu-protection
- Context** config>service>vpls>video-if
 config>service>ies>video-if
 config>service>vprn>video-if
- Description** This command assigns an existing CPU protection policy to the associated service video interface. The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-protection-policy-id* context. The number of RTCP messages per client will be limited to the number as configured under the policy.
- Default** none
- Parameters** *policy-id* — Specifies a CPU protection policy.
- Values** 1 to 255

scte35-action

- Syntax** **scte35-action** {**forward** | **drop**}
- Context** config>service>ies>video-interface>channel
 config>service>vprn>video-interface>channel
- Description** This command specifies whether the Society of Cable Telecommunications Engineers 35 (SCTE 35) cue avails in the stream need to be forwarded or not. When specified to forward, SCTE 35 messages will be forwarded downstream. When specified to drop, SCTE 35 messages will not be forwarded downstream. They will be still be processed for local splicing decisions.
- Parameters** **forward** — Forwards SCTE 35 messages downstream.
- drop** — Drops SCTE 35 messages.

zone-channel

- Syntax** **zone-channel** *mcast-address* **source** *ip-address* **adi-channel-name** *channel-name*
 no zone-channel *mcast-address* **source** *ip-address*

Context	config>service>ies>video-interface>channel config>service>vprn>video-interface>channel
Description	This command configures zone-channel parameters or ad insertion. The channel configuration along with the zone-channel configuration associates a network channel to a zone-channel and builds the store and forward relationship.
Parameters	<i>mcast-address</i> — Specifies the IP multicast group address for which this entry contains information. source <i>ip-address</i> — Specifies the type of address to be used for a source address/ adi-channel-name <i>channel-name</i> — Specifies the name for this zone channel.

scte30

Syntax	scte30
Context	config>service>ies>video-interface>adi config>service>vprn>video-interface>adi
Description	This command enables the context to configure SCTE 30 parameters.

ad-server

Syntax	[no] ad-server <i>ip-address</i>
Context	config>service>ies>video-interface>adi>scte30 config>service>vprn>video-interface>adi>scte30
Description	This command configures the ad server address. A TCP session will be accepted for SCTE 30 messaging only for IP addresses that appear in this configuration. The no form of the command removes the address from the ad server configuration.
Parameters	<i>ip-address</i> — Specifies the IP address of the ad server.

local-address

Syntax	local-address control <i>ip-address data ip-address</i> no local-address
Context	config>service>ies>video-interface>adi>scte30 config>service>vprn>video-interface>adi>scte30

Description	SCTE 30 requires a TCP session per zone-channel between the ad server and splicer for control communication and it requires UDP sessions on which the video ad stream is sent. This command specifies the splicer's control IP address to which the ad-servers should setup TCP connections and the data IP address to which the video ad streams should be sent. The no form of the command removes the address information from the local address configuration.
Parameters	control ip-address — Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad control streams. This address should be in the same subnet as the ip address assigned to the video interface. The values of control ip-address and the data ip-address specify the local IP address to which ad servers send SCTE 30 ad data streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error. data ip-address — Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad data streams. This address should be in the same subnet as the ip address assigned to the video interface. The values of the control ip-address and the data ip-address specify the local IP address to which ad servers send SCTE 30 ad control streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

multicast-service

Syntax	multicast-service <i>service-id</i> no multicast-service
Context	config>service>ies>video-interface config>service>vpls>video-interface config>service>vprn>video-interface
Description	This command adds a multicast service association to the video interface. This parameter is not required on the video interface when the service carries both unicast and multicast traffic. When multicast and unicast are carried in separate service instances, the operator can set this parameter on the unicast video interface to form an association with the multicast service when replies need to be sent in the multicast service instance. When multicast and unicast are carried in separate services when a downstream device (such as a DSLAM) can perform a service cross connect between the services and performs multicast replication. The no form of the command removes the multicast service association.
Default	none

Parameters	<i>service-id</i> — The service ID of the associated multicast service.
Values	
	<i>service-id:</i> 1 to 2147483647
	<i>svc-name:</i> 64 characters maximum

rt-client-src-address

Syntax	rt-client-src-address <i>ip-address</i> no rt-client-src-address
Context	config>service>ies>video-interface config>service>vpls>video-interface config>service>vprn>video-interface
Description	This command assigns the IP address for the retransmission client on the video interface within the service. The RET client IP address is the originating address used for communication with upstream RET servers. If no RET client address is assigned, the RT client is operationally down as the RET client configuration is incomplete. For a VPLS service, the RET client address cannot be the same as an existing address for the video interface, but it must be an address within a video interface subnet. For IES and VPRN, the RET client address can be the same as an existing address for the video interface or an address within a video interface subnet. The no form of the command deletes the RT client address from the video interface.
Default	none
Parameters	<i>ip-address</i> — Specifies the IP address for the retransmission client on the video interface within the service.

video-sap

Syntax	video-sap <i>video-group-id</i> no video-sap
Context	config>service>ies>video-interface config>service>vpls>video-interface config>service>vprn>video-interface
Description	This command configures a service video interface association with a video group. The no form of the command removes the video group association.
Default	none

Parameters	<i>video-group-id</i> — Specifies the video group ID number.
Values	1 to 4

egress

Syntax	egress
Context	config>service>ies>video-interface>video-sap config>service>vpls>video-interface>video-sap config>service>vprn>video-interface>video-sap
Description	This command enables the context to configure egress parameters for the service's video SAP.

ingress

Syntax	ingress
Context	config>service>ies>video-interface>video-sap config>service>vpls>video-interface>video-sap config>service>vprn>video-interface>video-sap
Description	This command enables the context to configure in parameters for the service's video SAP.

filter

Syntax	filter ip <i>ip-filter-id</i> no filter
Context	config>service>ies>video-interface>video-sap>egress config>service>vpls>video-interface>video-sap>egress config>service>vprn>video-interface>video-sap>egress config>service>ies>video-interface>video-sap>ingress config>service>vpls>video-interface>video-sap>ingress config>service>vprn>video-interface>video-sap>ingress
Description	This command associates an existing IP filter policy with an ingress or egress video SAP. Filter policies control the forwarding and dropping of packets based on the matching criteria. Filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets. The no form of this command removes any configured filter ID association with the SAP. The filter ID itself is not removed from the system.

Parameters **ip** *ip-filter-id* — Specifies the ID for the IP filter policy.

Values 1 to 65535

qos

Syntax **qos** *policy-id*
no qos

Context config>service>ies>video-interface>video-sap>egress
config>service>vpls>video-interface>video-sap>egress
config>service>vprn>video-interface>video-sap>egress
config>service>ies>video-interface>video-sap>ingress
config>service>vpls>video-interface>video-sap>ingress
config>service>vprn>video-interface>video-sap>ingress

Description This command associates an existing egress or ingress QoS policy to a video interface. If the policy-id does not exist, an error will be returned. Attempts to associate a QoS policy of the wrong type returns an error. Only one QoS policy can be associated with a video interface at one time in the ingress and egress contexts. Attempts to associate a second QoS policy of a given type will return an error.

The **no** form of the command removes the QoS policy association from the video interface, and the QoS policy reverts to the default.

Default default QoS policy

Parameters *policy-id* — The sap-egress or sap-ingress policy ID to associate with the video interface on ingress or egress. The policy ID must already exist.

Values 1 to 65535

gateway-ip

Syntax **gateway-ip** *ip-address*
no gateway-ip

Context config>service>vpls>video-interface

Description This command assigns a gateway IP address for the video interface within the VPLS service. Because VPLS is a Layer 2 service and the video interface is modeled like a host within the service, the video interface needs a gateway IP to send requests to devices outside of the VPLS subnet.

The **no** form of the command deletes the gateway IP address from the VPLS video interface.

Default none

Parameters *ip-address* — Specifies the gateway IP address of the VPLS video interface.

6.8 Show, Clear, and Debug Command Reference

6.8.1 Command Hierarchies

- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)

6.8.1.1 Show Commands

```
show
  — isa
    — video-group [video-group-id]

show
  — video
    — adi
      — channel [service service-id] [interface ip-int-name] [address mcast-address]
        [source ip-address] [detail]
      — session [service service-id] [interface ip-int-name] [address mcast-address]
        [source ip-address]
      — splice-status [service service-id] [interface ip-int-name] [address mcast-
        address] [source ip-address] [start-time start-time [interval time-interval]]
    — channel [service service-id] [interface ip-int-name] [address mcast-address] [source
      ip-address] [summary | detail] [pid | config | [analyzer [interval time-interval]]]
    — interface [service service-id] [interface ip-int-name] [stats {rt-server | fcc-server}]
    — interface [service service-id] [interface ip-int-name] summary
    — rtp-session [service service-id] [source ip-address] [detail [stats {rt-server | fcc-
      server}]]
    — rtp-session [service service-id] summary
```

6.8.1.2 Clear Commands

```
clear
  — video
    — id service-id
      — session all
      — session client srcAddr
    — statistics
      — id service-id
        — adi-session
        — channel all [rt-client] [rt-server] [fcc-server] [ad-insert]
```

- **channel** *grp-address* [**source** *srcAddr*] [**rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]
- **interface** *ip-int-name* [**address** *ip-address*] [**rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]
- **session** **all** [**rt-server**] [**fcc-server**]
- **session** **client** *srcAddr* [**rt-server**] [**fcc-server**]
- **isa** *video-group-id* [*mda-id*]

6.8.1.3 Debug Commands

- ```
debug
 — [no] service
 — id service-id
 — [no] video-interface video-ip-int-name
 — adi [zone-channel-name]
 — no adi
 — adi-packet [zone-channel-name] [type {type-name [type-name] | all}]
 — no adi-packet
 — fcc-server [client client-ip [source-port src-port]]
 — no fcc-server
 — packet-rx [client client-ip [source-port src-port]] [fcc-join] [fcc-leave]
 [ret-nack]
 — no packet-rx
 — packet-tx [group grp-addr [source srcAddr]] [ret-nack]
 — no packet-tx
 — rt-client [group group-addr]
 — no rt-client
 — rt-server [client client-ip [source-port src-port]]
 — no rt-server
 — sg [group grp-addr [source src-addr]]
 — no sg
```

## 6.8.2 Command Descriptions

- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)

## 6.8.2.1 Show Commands

### video-group

|                    |                                                              |
|--------------------|--------------------------------------------------------------|
| <b>Syntax</b>      | <b>video-group</b> [ <i>video-group-id</i> ]                 |
| <b>Context</b>     | show>isa                                                     |
| <b>Description</b> | This command displays ISA IPSec group information            |
| <b>Parameters</b>  | <i>ipsec-aa-group-id</i> — Specifies the ISA video group ID. |
| <b>Output</b>      | The following is an example output for this command.         |

#### Sample Output

```
A:SR-7/Dut-C# show isa video-group
=====
ISA Video Group
=====
Video Group Id : 1 Admin State : Up
Oper State : Up RT Server State : Enabled
FCC Server State : Disabled ADI State : Disabled
RT Resv Bandwidth(Mbps): 0 ADI State : Disabled

MDA : 2/1 Channels : 2
Admin State : Up Oper State : Up
Used Cache (bytes) : 586622 Available Cache (bytes): 1869186816
Mem alloc failures : 0 Dropped pkts (denting) : 0
Failed Chnl Allocs : 0 Egress Bandwidth excee*: 0
Bandwidth in use(kbps) : 0 Peak Bandwidth(kbps) : 200
Egress stream resets : 0 Ingress stream resets : 53
Ad stream resets : 0 Ad stream aborts : 0
SSRC collisions : 0 Received data packets : 4521
Received data octets : 6284714 Rx data packet errors : 0
Transmitted data packets: 1183 Transmitted data octets: 1646212
Tx data packet errors : 0 Tx lost data packets : 47
Active RTCP sessions : 1 Requested RTP Packets : 968
RTCP Parse Errors : 0 RTCP Config Errors : 0
RTCP IPC Errors : 0 RTCP SG Errors : 0
RTCP Subscriber Errors : 0 RTCP Interface Errors : 0
Total RET BW (Kbps) : 0 Max. RET BW (Kbps) : 100
Total FCC BW (Kbps) : 0 Drop Count for FCC : 0
Mcast RET Req for RTCP : 0 Mcast RET Req for RUDDP : 0
Mcast RET Created : 0 Mcast RET Req Quenched : 0
HighPkt pool limit hit : 0

Pkts Lost (2-10) : 24 Pkts Lost (11-20) : 48
Pkts Lost (21-30) : 0 Pkts Lost (31-40) : 0
Pkts Lost (>40) : 0

Video-groups : 1
=====
* indicates that the corresponding row element may have been truncated.
A:SR-7/Dut-C#
```

---

## adi

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>adi</b> [ <b>service</b> <i>service-id</i> ] [ <b>interface</b> <i>ip-int-name</i> ] [ <b>address</b> <i>mcast-address</i> ] [ <b>source</b> <i>ip-address</i> ] [ <b>detail</b> ]                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | show>video                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | This command displays ad insertion channel information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <b>service</b> <i>service-id</i> — Displays information pertaining to the specified service ID.<br><b>Values</b> 1 — 2147483648<br>svc-name — a string up to 64 characters in length.<br><b>interface</b> <i>ip-int-name</i> — Displays information pertaining to the specified interface.<br><b>address</b> <i>mcast-address</i> — Displays information pertaining to the specified multicast channel address.<br><b>source</b> <i>ip-address</i> — Displays information pertaining to the source IP address.<br><b>detail</b> — The output displays detailed information. |

## channel

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>channel</b> [ <b>service</b> <i>service-id</i> ] [ <b>interface</b> <i>ip-int-name</i> ] [ <b>address</b> <i>mcast-address</i> ] [ <b>source</b> <i>ip-address</i> ] [ <b>detail</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | show>video>adi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | This command displays video channel information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>service</b> <i>service-id</i> — Displays video channel information pertaining to the specified service ID.<br><b>Values</b> service-id: 1 to 2148278381<br>svc-name: A string up to 64 characters<br>router-name: Base, management, vpls-management<br><b>Default</b> Base<br><b>interface</b> <i>ip-int-name</i> — Displays video channel information pertaining to the specified interface.<br><b>address</b> <i>mcast-address</i> — Displays video channel information pertaining to the specified multicast channel address.<br><b>source</b> <i>ip-address</i> — Displays video channel information pertaining to the source IP address.<br><b>detail</b> — The output displays detailed video channel information. |



---

session

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>session</b> [ <b>service</b> <i>service-id</i> ] [ <b>interface</b> <i>ip-int-name</i> ] [ <b>address</b> <i>mcast-address</i> ] [ <b>source</b> <i>ip-address</i> ]                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | show>video>adi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command displays ADI video session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <b>service</b> <i>service-id</i> — Displays video session information pertaining to the specified service ID.<br><b>Values</b> 1 to 2147483648<br>svc-name — a string up to 64 characters in length.<br><b>interface</b> <i>ip-int-name</i> — Displays session information for the specified interface.<br><b>address</b> <i>mcast-address</i> — Displays session information for the specified multicast address.<br><b>source</b> <i>ip-address</i> — Displays session information for the specified IP address. |
| <b>Output</b>      | The following is an example output for this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Sample Output**

```
*B:IPTV-SR7# show video adi session
=====
Adi Session
=====
Service Id : 100 Interface Name : video-100
Group Address : 192.0.2.241 Source Address : 10.100.100.1
Ad Server Addr : 10.200.14.2 Up Time : 0d 13:30:02
Init Requests : 1 Succ/Unsucc Resp : 1/0
Alive Requests : 0 Succ/Unsucc Resp : 0/0
Cue Requests : 0 Succ/Unsucc Resp : 0/0
Abort Requests : 0 Succ/Unsucc Resp : 0/0
Splice Requests : 910 Succ/Unsucc Resp : 906/4
Successful splice-in complete responses : 902
Successful splice-out complete responses : 894
Unsuccessful splice-out complete responses : 11
Invalid SCTE30 R*: 0

Number of adi sessions : 1
=====
*B:IPTV-SR7#
```

## splice-status

|                |                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>splice-status</b> [ <b>service</b> <i>service-id</i> ] [ <b>interface</b> <i>ip-int-name</i> ][ <b>address</b> <i>mcast-address</i> ] [ <b>source</b> <i>ip-address</i> ] [ <b>start-time</b> <i>start-time</i> [ <b>interval</b> <i>time-interval</i> ]] |
| <b>Context</b> | show>video>adi                                                                                                                                                                                                                                               |

- Description** This command displays ADI slice information.
- Parameters**
- service** *service-id* — Displays splice status information pertaining to the specified service ID.
  - Values** 1 to 2148278317
  - svc-name** — a string up to 64 characters.
  - interface** *ip-int-name* — Displays splice status information for the specified interface.
  - address** *mcast-address* — Displays splice status information for the specified multicast address.
  - source** *ip-address* — Displays splice status information for the specified IP address.
  - start-time** *start-time* — Enter the start time.
  - Values** 1 to 4294967295 minutes earlier
  - interval** *time-interval* — Enter the interval time.
  - Values** 1 to 4294967295 minutes
- Output** The following is an example output for this command.

**Sample Output**

```
*B:IPTV-SR7# show video adi splice-status
=====
Adi Splice Status
=====
Service Id : 100 Interface Name : video-100
Group Address : 192.0.2.241 Source Address : 10.100.100.1
Start Time : 07/17/2009 10:19:14 Ad Server Addr : 10.200.14.2
Status : Complete Rate : 8936 kbps
Duration Req : 30 sec Duration Played : 29 sec
Session Id : 1 Prior Session Id : 4294967295
SpliceIn SeqNum : 378 SpliceOut SeqNum : 29727
Abort Reason : None Black Frames : 0
First black frame PTS : 1530
Max Ad Stream PTS : 0
Min Network Stream PTS : 0

Service Id : 100 Interface Name : video-100
Group Address : 192.0.2.241 Source Address : 10.100.100.1
Start Time : 07/17/2009 10:19:44 Ad Server Addr : 10.200.14.2
Status : Complete Rate : 0 kbps
Duration Req : 30 sec Duration Played : 0 sec
Session Id : 2 Prior Session Id : 1
SpliceIn SeqNum : 29727 SpliceOut SeqNum : 0
Abort Reason : Session incomplete Black Frames : 0
First black frame PTS : 1530
Max Ad Stream PTS : 0
Min Network Stream PTS : 0

*B:IPTV-SR7#
```

---

channel

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>channel</b> [ <b>service</b> <i>service-id</i> ] [ <b>interface</b> <i>ip-int-name</i> ] [ <b>address</b> <i>mcast-address</i> ] [ <b>source</b> <i>ip-address</i> ] [ <b>summary</b>   <b>detail</b> ] [ <b>pid</b>   <b>config</b>   [ <b>analyzer</b> [ <b>interval</b> <i>time-interval</i> ]]]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | show>video                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command displays video channel information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><b>service</b> <i>service-id</i> — Displays video channel information pertaining to the specified service ID.</p> <p><b>Values</b>      <i>service-id</i>: 1 to 214748364<br/>                 <i>svc-name</i>: A string up to 64 characters<br/>                 <i>router-name</i>: Base, management, vpls-management</p> <p><b>Default</b>      Base</p> <p><b>interface</b> <i>ip-int-name</i> — Displays video channel information pertaining to the specified interface.</p> <p><b>address</b> <i>mcast-address</i> — Displays video channel information pertaining to the specified multicast channel address.</p> <p><b>source</b> <i>ip-address</i> — Displays video channel information pertaining to the source IP address.</p> <p><b>summary</b> — The output displays summarized video channel information.</p> <p><b>detail</b> — The output displays detailed video channel information.</p> |
| <b>Output</b>      | The following is an example output for this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Sample Output

```
*A:SR-12/Dut-C# show video channel analyzer
=====
Video channel analyzer summary
=====
 Channel number : 1

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
MDI Delay Factor : 7 MDI Loss Rate : 0
Good Secs : 54

 Channel number : 2

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
MDI Delay Factor : 6 MDI Loss Rate : 0
Good Secs : 54

 Channel number : 3

Service Id : 300 Interface Name : video-300
```

```
Group Address : 192.0.2.7 Source Address : 10.20.13.3
MDI Delay Factor : 7 MDI Loss Rate : 0
Good Secs : 54

Number of channels : 3
=====
*A:SR-12/Dut-C#

*A:SR-12/Dut-
C# show video channel analyzer address 192.0.2.6 source 10.20.13.2 interface "video-
300" detail
=====
Video channel analyzer detail
=====
Channel number : 1

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
MDI Delay Factor : 8 MDI Loss Rate : 0
Good Secs : 80
=====
GOP Stats
=====
Min Max Avg

GOP Length 40 78 48
Frames/Sec 39 55 53
=====
Frame Stats
=====
I-Frame P-Frame B-Frame

Good 19 986 0
Bad 0 0 0
=====
Error Stats
=====
POA Events QoS Events TNC Events

PAT Rep 0 0 0
PMT Rep 0 0 0
PCR Rep 0 0 0
PAT Syntax Err - - 0
PMT Syntax Err - - 0
Sync Byte Err - 0 -
Sync Loss 0 - -
Unref PID - - 0
Traffic Loss 0 - -

Overall 0 0 0
=====
Reoccurring events only increment counter once every second

Number of channels : 1
=====
*A:SR-12/Dut-C#

*A:SR-12/Dut-C# show video channel pid
```

```
=====
Video Channel PID
=====
Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 0 PID Type : pat
MPEG Stream Type : 0 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 0

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 2 PID Type : audio
MPEG Stream Type : 4 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 126336

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 32 PID Type : video
MPEG Stream Type : 27 Is PCR PID : Yes
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 1952192

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 33 PID Type : pmt
MPEG Stream Type : 0 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 0

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 308 PID Type : audio
MPEG Stream Type : 4 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 126336

Number of pids for this channel: 5

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
PID : 0 PID Type : pat
MPEG Stream Type : 0 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 0

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
PID : 2 PID Type : audio
MPEG Stream Type : 4 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 126336

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
PID : 32 PID Type : video
MPEG Stream Type : 27 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
```

```
Absent Err Secs : 0 PID Bitrate : 1949184

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
PID : 33 PID Type : pmt
MPEG Stream Type : 0 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 0

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
PID : 308 PID Type : audio
MPEG Stream Type : 4 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 136864
=====
*A:SR-12/Dut-C#

*A:SR-12/Dut-C# show video channel pid interface "video-
300" source 10.20.13.3 address 192.0.2.5
=====
Video Channel PID
=====
No Matching Entries
=====

*A:SR-12/Dut-C# show video channel config
=====
Video channel config
=====
Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
Analyzer State : Enabled Cc Error : Disabled
PAT Rep Err : Enabled TNC PAT Rep : 200
QOS PAT Rep : 400 POA PAT Rep : 600
PAT Syntax : Enabled PCR Rep Err : Enabled
TNC PCR Rep : 200 QOS PCR Rep : 400
POA PCR Rep : 600 Vid PID Absent : 1000
PID PMT Unref : Enabled PMT Rep Err Secs : Enabled
TNC PMT Rep : 400 QOS PMT Rep : 800
POA PMT Rep : 2000 PMT Syntax : Enabled
SCTE35 Err Secs : Disabled TEI Err Secs : Disabled
TS Sync Loss : Enabled Non-Vid Pid Abse*: 1000
Alarm Sev : tnc

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
Analyzer State : Enabled Cc Error : Disabled
PAT Rep Err : Enabled TNC PAT Rep : 200
QOS PAT Rep : 400 POA PAT Rep : 600
PAT Syntax : Enabled PCR Rep Err : Enabled
TNC PCR Rep : 200 QOS PCR Rep : 400
POA PCR Rep : 600 Vid PID Absent : 1000
PID PMT Unref : Enabled PMT Rep Err Secs : Enabled
TNC PMT Rep : 400 QOS PMT Rep : 800
POA PMT Rep : 2000 PMT Syntax : Enabled
SCTE35 Err Secs : Disabled TEI Err Secs : Disabled
TS Sync Loss : Enabled Non-Vid Pid Abse*: 1000
```

```

Alarm Sev : tnc

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.7 Source Address : 10.20.13.3
Analyzer State : Enabled Cc Error : Disabled
PAT Rep Err : Enabled TNC PAT Rep : 200
QOS PAT Rep : 400 POA PAT Rep : 600
PAT Syntax : Enabled PCR Rep Err : Enabled
TNC PCR Rep : 200 QOS PCR Rep : 400
POA PCR Rep : 600 Vid PID Absent : 1000
PID PMT Unref : Enabled PMT Rep Err Secs : Enabled
TNC PMT Rep : 400 QOS PMT Rep : 800
POA PMT Rep : 2000 PMT Syntax : Enabled
SCTE35 Err Secs : Disabled TEI Err Secs : Disabled
TS Sync Loss : Enabled Non-Vid Pid Abse*: 1000
Alarm Sev : tnc

Number of channels : 3
=====
* indicates that the corresponding row element may have been truncated.
*A:SR-12/Dut-C#

*A:SR-12/Dut-C# show video channel config interface "video-300"
=====
Video channel config
=====
Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.3
Analyzer State : Enabled Cc Error : Disabled
PAT Rep Err : Enabled TNC PAT Rep : 200
QOS PAT Rep : 400 POA PAT Rep : 600
PAT Syntax : Enabled PCR Rep Err : Enabled
TNC PCR Rep : 200 QOS PCR Rep : 400
POA PCR Rep : 600 Vid PID Absent : 1000
PID PMT Unref : Enabled PMT Rep Err Secs : Enabled
TNC PMT Rep : 400 QOS PMT Rep : 800
POA PMT Rep : 2000 PMT Syntax : Enabled
SCTE35 Err Secs : Disabled TEI Err Secs : Disabled
TS Sync Loss : Enabled Non-Vid Pid Abse*: 1000
Alarm Sev : tnc

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 192.168.2.1
Analyzer State : Enabled Cc Error : Disabled
PAT Rep Err : Enabled TNC PAT Rep : 200
QOS PAT Rep : 400 POA PAT Rep : 600
PAT Syntax : Enabled PCR Rep Err : Enabled
TNC PCR Rep : 200 QOS PCR Rep : 400
POA PCR Rep : 600 Vid PID Absent : 1000
PID PMT Unref : Enabled PMT Rep Err Secs : Enabled
TNC PMT Rep : 400 QOS PMT Rep : 800
POA PMT Rep : 2000 PMT Syntax : Enabled
SCTE35 Err Secs : Disabled TEI Err Secs : Disabled
TS Sync Loss : Enabled Non-Vid Pid Abse*: 1000
Alarm Sev : tnc

```

```
Service Id : 300
Group Address : 192.0.2.7
Analyzer State : Enabled
PAT Rep Err : Enabled
TNC PAT Rep : 400
QOS PAT Rep : 400
PAT Syntax : Enabled
TNC PCR Rep : 200
POA PCR Rep : 600
PID PMT Unref : Enabled
TNC PMT Rep : 400
POA PMT Rep : 2000
SCTE35 Err Secs : Disabled
TS Sync Loss : Enabled
Alarm Sev : tnc

Interface Name : video-300
Source Address : 10.20.13.3
Cc Error : Disabled
TNC PAT Rep : 200
POA PAT Rep : 600
PCR Rep Err : Enabled
QOS PCR Rep : 400
Vid PID Absent : 1000
PMT Rep Err Secs : Enabled
QOS PMT Rep : 800
PMT Syntax : Enabled
TEI Err Secs : Disabled
Non-Vid Pid Abse*: 1000
```

```

Number of channels : 3
```

```
=====
* indicates that the corresponding row element may have been truncated.
```

```
*A:SR-12/Dut-C#
```

```
*A:SR-12/Dut-C# show video channel pid
```

```
=====
Video Channel PID
```

```
=====
Service Id : 300
Group Address : 192.0.2.6
PID : 0
MPEG Stream Type : 0
Cc Err Secs : 0
Absent Err Secs : 16

Interface Name : video-300
Source Address : 10.20.13.2
PID Type : pat
Is PCR PID : No
TEI Err Secs : 0
PID Bitrate : 0
```

```
Service Id : 300
Group Address : 192.0.2.6
PID : 2
MPEG Stream Type : 4
Cc Err Secs : 0
Absent Err Secs : 0

Interface Name : video-300
Source Address : 10.20.13.2
PID Type : audio
Is PCR PID : No
TEI Err Secs : 0
PID Bitrate : 126336
```

```
Service Id : 300
Group Address : 192.0.2.6
PID : 32
MPEG Stream Type : 27
Cc Err Secs : 0
Absent Err Secs : 0

Interface Name : video-300
Source Address : 10.20.13.2
PID Type : video
Is PCR PID : Yes
TEI Err Secs : 0
PID Bitrate : 1941664
```

```
Service Id : 300
Group Address : 192.0.2.6
PID : 33
MPEG Stream Type : 0
Cc Err Secs : 0
Absent Err Secs : 16

Interface Name : video-300
Source Address : 10.20.13.2
PID Type : pmt
Is PCR PID : No
TEI Err Secs : 0
PID Bitrate : 0
```

```
=====
*A:SR-12/Dut-C#
```

```
*A:SR-12/Dut-C# show video channel pid interface "video-
300" source 10.20.13.2 address 192.0.2.6
```



```
Video Channel PID
=====
Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 0 PID Type : pat
MPEG Stream Type : 0 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 16 PID Bitrate : 0

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 2 PID Type : audio
MPEG Stream Type : 4 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 136864

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 32 PID Type : video
MPEG Stream Type : 27 Is PCR PID : Yes
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 1931136

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 33 PID Type : pmt
MPEG Stream Type : 0 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 16 PID Bitrate : 0

Service Id : 300 Interface Name : video-300
Group Address : 192.0.2.6 Source Address : 10.20.13.2
PID : 308 PID Type : audio
MPEG Stream Type : 4 Is PCR PID : No
Cc Err Secs : 0 TEI Err Secs : 0
Absent Err Secs : 0 PID Bitrate : 136864

Number of pids for this channel: 5

Number of channels : 1
=====
*A:SR-12/Dut-C#
```

## interface

|                    |                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>interface</b> [service <i>service-id</i> ] [interface <i>ip-int-name</i> ] [stats {rt-server   fcc-server}]<br><b>interface</b> [service <i>service-id</i> ] [interface <i>ip-int-name</i> ] <b>summary</b> |
| <b>Context</b>     | show>video                                                                                                                                                                                                     |
| <b>Description</b> | This command displays video interface information.                                                                                                                                                             |
| <b>Parameters</b>  | <b>service</b> <i>service-id</i> — Displays video interface information pertaining to the specified service ID.                                                                                                |
| <b>Values</b>      | 1 to 2148278317                                                                                                                                                                                                |

**svc-name** — a string up to 64 characters.

**interface ip-int-name** — Displays video interface information pertaining to the specified interface.

**stats** — Displays video interface statistics.

**Values**     **rt-server** — Displays video interface statistics for the RET server.

**fcc-server** — Displays video interface statistics for the FCC server.

**Output**     The following is an example output for this command.

### Sample Output

```
*A:Dut-C# show video interface
=====
Video interface
=====
Service Id : 1
Name : vi
Admin/Oper State : Up/Up If Index : 0
Video Group Id : 1 Sap Id : lag-201:5
Sessions : 2000 Mcast Protocol : PIM

Address : 10.3.3.3/32
Tx Failed Pkts : 0
SCTE30 TCP sess : 0 SCTE30 INIT sess : 0
SD RT Svr State : Enabled
SD RT Requests : 0 SD Failed Req : 0
SD RTP Pkts Req : 0 SD RT Replies : 0
Tx SD Bytes : 0 Tx SD Packets : 0
HD RT Svr State : Enabled
HD RT Requests : 0 HD Failed Req : 0
HD RTP Pkts Req : 0 HD RT Replies : 0
Tx HD Bytes : 0 Tx HD Packets : 0
PIP RT Svr State : Enabled
PIP RT Requests : 0 PIP Failed Req : 0
PIP RTP Pkts Req : 0 PIP RT Replies : 0
Tx PIP Bytes : 0 Tx PIP Packets : 0
SD FCC Svr State : Enabled
SD FCC Requests : 0 SD FCC Svr Mode : Burst
Tx SD Bytes : 0 SD Failed Req : 0
SD FCC Replies : 0 Tx SD Packets : 0
HD FCC Svr State : Enabled
HD FCC Requests : 448820 HD FCC Svr Mode : Burst
Tx HD Bytes : 17150845788 HD Failed Req : 0
HD FCC Replies : 448820 Tx HD Packets : 293148098
PIP FCCSvr State : Enabled
PIP FCC Requests : 0 PIP FCC Svr Mode : Burst
Tx PIP Bytes : 0 PIP Failed Req : 0
PIP FCC Replies : 0 Tx PIP Pkts : 0

Interfaces : 1
=====
*A:Dut-C#
```

---

rtp-session

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>rtp-session</b> [ <b>service</b> <i>service-id</i> ] [ <b>source</b> <i>ip-address</i> ] [ <b>detail</b> [ <b>stats</b> { <b>rt-server</b>   <b>fcc-server</b> }]]<br><b>rtp-session</b> [ <b>service</b> <i>service-id</i> ] <b>summary</b>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | show>video                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command displays video session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <b>service</b> <i>service-id</i> — Displays video session information pertaining to the specified service ID.<br><b>Values</b> 1 to 2148278317<br>svc-name — a string up to 64 characters.<br><b>source</b> <i>ip-address</i> — Displays session information for the specified IP address.<br><b>detail</b> — The output displays detailed video session information.<br><b>stats</b> — Displays video session statistics.<br><b>Values</b> <b>rt-server</b> — Displays video session statistics for the RT server.<br><b>fcc-server</b> — Displays video session statistics for the FCC server.<br><b>summary</b> — The output displays summarized video session information. |
| <b>Output</b>      | The following is an example output for this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Sample Output**

```
*A:Dut-C# show video rtp-session
=====
Video RTP session
=====
Service Id Source address SSRC Id (hex) RT reqs FCC reqs
Interface Source Port Time to expire RT replies FCC replies

1 10.0.103.103 1 0 226
vi 1000 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1001 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1002 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1003 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1004 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1005 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1006 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1007 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1008 0d 00:03:24 0 225
1 10.0.103.103 1 0 226
vi 1009 0d 00:03:24 0 225
```

```

Number of RTP sessions : 10
=====
*A:Dut-C#

*A:Dut-C# show video rtp-session summary
=====
Video RTP session summary
=====
Num Sessions : 2000
Rx RT Requests : 0
Tx RT Replies : 0
Rx FCC Requests : 371068
Tx FCC Replies : 368259
Tx RT Packets : 0
Tx RT Octets : 0
Tx FCC Packets : 243011904
Tx FCC Octets : 14152149376

Interfaces : 1
=====
*A:Dut-C#

*A:Dut-C# show video rtp-session detail
=====
Video RTP session detail
=====
Service Id : 1
Interface : vi
Source Address : 10.0.103.103
Source Port : 1000
Destination Addr : 10.3.3.3
CName : ixiaPort
Up Time : 0d 00:07:08
SSRC Id (hex) : 1
Time to Expire : 0d 00:04:59
Num RT Requests : 0
RT Packets Sent : 0
RT Failed Pkts : 0
Num RT Replies : 0
RT Octets Sent : 0
Req RTP Packets : 0
Num FCC Requests : 212
FCC Packets Sent : 138582
FCC Failed Pkts : 1
Num FCC Replies : 211
FCC Octets Sent : 8145140

*A:Dut-C#
```

6.8.2.2 Clear Commands

id

|             |                                                                               |
|-------------|-------------------------------------------------------------------------------|
| Syntax      | id service-id                                                                 |
| Context     | clear>video                                                                   |
| Description | This command clears video information pertaining to the specified service ID. |

---

**Parameters**    **service** *service-id* — Specifies the service ID to clear.

**Values**        1 to 2148278317  
                                      *svc-name* — a string up to 64 characters.

## session

**Syntax**        **session all**  
                  **session client** *srcAddr*

**Context**        clear>video>id

**Description**    This command clears session information.

**Parameters**    **all** — Clears all sessions.  
                  **client** *srcAddr* — Clears information for the client source address.

## statistics

**Syntax**        **statistics**

**Context**        clear>video

**Description**    This command clears video related statistics.

## id

**Syntax**        **id** *service-id*

**Context**        clear>video>statistics

**Description**    This command clears video statistics for a particular service.

**Parameters**    **service** *service-id* — Specifies the service ID to clear statistics.

**Values**        1 to 2148278317  
                                      *svc-name* — a string up to 64 characters.

## adi-session

**Syntax**        **adi-session**

**Context**        clear>video>statistics>id

**Description**    This command clears video statistics for an ADI session.

## channel

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>channel all</b> [rt-client] [rt-server] [fcc-server] [ad-insert]<br><b>channel</b> <i>grp-address</i> [source <i>srcAddr</i> ] [rt-client] [rt-server] [fcc-server] [ad-insert]                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | clear>video>statistics>id                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | This command clears video statistics for a particular channel.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>all</b> — Clears statistics for all channels.<br><b>rt-client</b> — Clears all RET client related statistics.<br><b>rt-server</b> — Clears all RET server related statistics.<br><b>fcc-server</b> — Clears all FCC server related statistics.<br><b>ad-insert</b> — Clears all ad insert related statistics.<br><i>grp-address</i> — Clears statistics for the specified channel group address.<br><b>source</b> <i>srcAddr</i> — Clears statistics for the specified source address. |

## interface

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>interface</b> <i>ip-int-name</i> [address <i>ip-address</i> ] [rt-client] [rt-server] [fcc-server] [ad-insert]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | clear>video>statistics>id                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command clears video statistics for a particular channel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <i>ip-int-name</i> — Clears statistics for the specified interface.<br><b>address</b> <i>ip-address</i> — Clears statistics for the specified IP address.<br><b>rt-client</b> — Clears all RET client related statistics.<br><b>rt-server</b> — Clears all RET server related statistics.<br><b>fcc-server</b> — Clears all FCC server related statistics.<br><b>ad-insert</b> — Clears all ad insert related statistics.<br><i>grp-address</i> — Clears statistics for the specified channel group address.<br><b>source</b> <i>srcAddr</i> — Clears statistics for the specified source address. |

## session

|                |                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>session all</b> [rt-server] [fcc-server]<br><b>session client</b> <i>srcAddr</i> [rt-server] [fcc-server] |
| <b>Context</b> | clear>video>statistics>id                                                                                    |

---

|                    |                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command clears video statistics for a particular channel.                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <p><b>all</b> — Clears statistics for all sessions.</p> <p><b>rt-server</b> — Clears all RET server related statistics.</p> <p><b>fcc-server</b> — Clears all FCC server related statistics.</p> <p><b>client</b> <i>srcAddr</i> — Clears statistics for the specified source address.</p> |

## isa

|                    |                                                                                                                                                                                                                                                                                                                                                                                                           |         |          |       |                                          |      |        |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|----------|-------|------------------------------------------|------|--------|
| <b>Syntax</b>      | <b>isa</b> <i>video-group-id</i> [ <i>mda-id</i> ]                                                                                                                                                                                                                                                                                                                                                        |         |          |       |                                          |      |        |
| <b>Context</b>     | clear>video>statistics                                                                                                                                                                                                                                                                                                                                                                                    |         |          |       |                                          |      |        |
| <b>Description</b> | .This command clears statistics for a particular ISA video group.                                                                                                                                                                                                                                                                                                                                         |         |          |       |                                          |      |        |
| <b>Parameters</b>  | <p><i>video-group-id</i> — statistics for a particular ISA video group a video group ID.</p> <p><b>Values</b> 1 to 4</p> <p><i>mda-id</i> — Specifies the card/slot identifying a provisioned ISA.</p> <p><b>Values</b></p> <table> <tr> <td>mda-id:</td><td>slot/mda</td></tr> <tr> <td>slot:</td><td>1 to 10 (depending on the chassis model)</td></tr> <tr> <td>mda:</td><td>1 to 2</td></tr> </table> | mda-id: | slot/mda | slot: | 1 to 10 (depending on the chassis model) | mda: | 1 to 2 |
| mda-id:            | slot/mda                                                                                                                                                                                                                                                                                                                                                                                                  |         |          |       |                                          |      |        |
| slot:              | 1 to 10 (depending on the chassis model)                                                                                                                                                                                                                                                                                                                                                                  |         |          |       |                                          |      |        |
| mda:               | 1 to 2                                                                                                                                                                                                                                                                                                                                                                                                    |         |          |       |                                          |      |        |

### 6.8.2.3 Debug Commands

## video-interface

|                    |                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] video-interface</b> <i>video-ip-int-name</i>                                                                                         |
| <b>Context</b>     | debug>service>id                                                                                                                             |
| <b>Description</b> | <p>This command enables debugging for video interfaces.</p> <p>The <b>no</b> form of the command disables the video interface debugging.</p> |
| <b>Parameters</b>  | <i>video-ip-int-name</i> — Specifies the video interface name.                                                                               |

## adi

|               |                                         |
|---------------|-----------------------------------------|
| <b>Syntax</b> | <b>adi</b> [ <i>zone-channel-name</i> ] |
|---------------|-----------------------------------------|

**no adi**

|                    |                                                                            |
|--------------------|----------------------------------------------------------------------------|
| <b>Context</b>     | debug>service>id>video-interface                                           |
| <b>Description</b> | This command enables debugging for the ad insert server.                   |
| <b>Parameters</b>  | <i>zone-channel-name</i> — Specifies the channel name up to 32 characters. |

adi-packet

|                    |                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>adi-packet</b> [ <i>zone-channel-name</i> ] [ <b>type</b> { <i>type-name</i> [ <i>type-name</i> ]   <b>all</b> }]<br><b>no adi-packet</b>                                                      |
| <b>Context</b>     | debug>service>id>video-interface                                                                                                                                                                  |
| <b>Description</b> | This command enables debugging for ADI packets exchanged between the splicer and the ad-server over scte30 sessions.                                                                              |
| <b>Parameters</b>  | <i>zone-channel-name</i> — Specifies the channel name up to 32 characters.<br><b>type</b> <i>type-name</i> — Specifies the ADI packet type.<br><b>Values</b> alive, abort, init, splice, cue, all |
| <b>Output</b>      | The following is an example output for this command.                                                                                                                                              |

**Sample Output**

```
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-
1 type init
A:IPTV-SR7# show debug
debug
 service id 100
 video-interface video-100
 adi-packet 240-1 type init
 exit
 exit
exit
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-
1 type alive
A:IPTV-SR7# show debug
debug
 service id 100
 video-interface video-100
 adi-packet 240-1 type alive
 exit
 exit
exit
```

fcc-server

|               |                                                                                            |
|---------------|--------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>fcc-server</b> [ <i>client</i> <i>client-ip</i> [ <i>source-port</i> <i>src-port</i> ]] |
|---------------|--------------------------------------------------------------------------------------------|



### no fcc-server

|                    |                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | debug>service>id>video-interface                                                                                                                             |
| <b>Description</b> | This command enables debugging the FCC server.                                                                                                               |
| <b>Parameters</b>  | <p><b>client</b> <i>client-ip</i> — Specifies the client IP address.</p> <p><b>source-port</b> <i>src-port</i> — Specifies the source port's IP address.</p> |

## packet-rx

|                    |                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>packet-rx</b> [ <b>client</b> <i>client-ip</i> [ <b>source-port</b> <i>src-port</i> ]] [ <b>fcc-join</b> ] [ <b>fcc-leave</b> ] [ <b>ret-nack</b> ]<br><b>no packet-rx</b>                                                                                                                                                                     |
| <b>Context</b>     | debug>service>id>video-interface                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | This command enables debugging of received RTCP messages. The options for this command allow the user to filter only certain types of messages to appear in the debug traces.                                                                                                                                                                     |
| <b>Parameters</b>  | <p><b>client</b> <i>client-ip</i> — Specifies the client IP address.</p> <p><b>source-port</b> <i>src-port</i> — Specifies the source port.</p> <p><b>fcc-join</b> — Enables debugging for FCC joins.</p> <p><b>fcc-leave</b> — Enables debugging for FCC leaves.</p> <p><b>ret-nack</b> — Enables debugging for retransmission nack packets.</p> |

## packet-tx

|                    |                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>packet-tx</b> [ <b>group</b> <i>grp-addr</i> [ <b>source</b> <i>srcAddr</i> ]] [ <b>ret-nack</b> ]<br><b>no packet-tx</b>                               |
| <b>Context</b>     | debug>service>id>video-interface                                                                                                                           |
| <b>Description</b> | This command enables debugging transmitted RTCP packets.                                                                                                   |
| <b>Parameters</b>  | <p><b>client</b> <i>client-ip</i> — Specifies the client IP address.</p> <p><b>source</b> <i>src-srcAddr</i> — Specifies the source port's IP address.</p> |

## rt-client

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>rt-client</b> [ <b>group</b> <i>group-addr</i> ]<br><b>no rt-client</b> |
| <b>Context</b> | debug>service>id>video-interface                                           |

|             |                                                                         |
|-------------|-------------------------------------------------------------------------|
| Description | This command enables debugging the RET client.                          |
| Parameters  | <b>group</b> <i>group-addr</i> — Specifies the multicast group address. |

rt-server

|             |                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>rt-server</b> [ <b>client</b> <i>client-ip</i> [ <b>source-port</b> <i>src-port</i> ]]<br><b>no rt-server</b>                                               |
| Context     | debug>service>id>video-interface                                                                                                                               |
| Description | This command enables debugging for the RET server.                                                                                                             |
| Parameters  | <b>client</b> <i>client-ip</i> — Specifies the client IP address.<br><b>source</b> <i>src-srcAddr</i> — Specifies the source port.<br><b>Values</b> 1 to 65535 |

sg

|             |                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>sg</b> [ <b>group</b> <i>grp-addr</i> [ <b>source</b> <i>src-addr</i> ]]<br><b>no sg</b>                                              |
| Context     | debug>service>id>video-interface                                                                                                         |
| Description | This command enables channel debugging.                                                                                                  |
| Parameters  | <b>group</b> <i>grp-addr</i> — Specifies the multicast channel address.<br><b>source</b> <i>src-addr</i> — Specifies the source address. |

## 7 Network Address Translation

### 7.1 Terminology

**BNG Subscriber** — A broader term than the ESM Subscriber, independent of the platform on which the subscriber is instantiated. It includes ESM subscribers on 7750 SR as well as subscribers instantiated on third party BNGs. Some of the NAT functions, such as Subscriber Aware Large Scale NAT44 utilizing standard RADIUS attribute work with subscribers independently of the platform on which they are instantiated.

**Deterministic NAT** — A mode of operation where mappings between the NAT subscriber and the outside IP address and port-range are allocated at the time of configuration. Each subscriber is permanently mapped to an outside IP and a dedicated port block. This dedicated port block is referred to as deterministic port block. Logging is not needed as the reverse mapping can be obtained using a known formula. The subscriber's ports can be expanded by allocating a dynamic port block in case that all ports in deterministic port block are exhausted. In such case logging for the dynamic port block allocation/de-allocation is required.

**Enhanced Subscriber Management (ESM) subscriber** — A host or a collection of hosts instantiated in 7750 SR Broadband Network Gateway (BNG). The ESM subscriber represents a household or a business entity for which various services with committed Service Level Agreements (SLA) can be delivered. NAT function is not part of basic ESM functionality.

**L2-Aware NAT** — In the context of 7750 SR platform combines Enhanced Subscriber Management (ESM) subscriber-id and inside IP address to perform translation into a unique outside IP address and outside port. This is in contrast with classical NAT technique where only inside IP is considered for address translations. Since the subscriber-id alone is sufficient to make the address translation unique, L2-Aware NAT allows many ESM subscribers to share the same inside IP address. The scalability, performance and reliability requirements are the same as in LSN.

**Large Scale NAT (LSN)** — Refers to a collection of network address translation techniques used in service provider network implemented on a highly scalable, high performance hardware that facilitates various intra and inter-node redundancy mechanisms. The purpose of LSN semantics is to make delineation between high scale and high performance NAT functions found in service provider networks and enterprise NAT that is usually serving much smaller customer base at smaller speeds. The following NAT techniques can be grouped under the LSN name:

- Large Scale NAT44 or Carrier Grade NAT (CGN)

- DS-Lite
- NAT64

Each distinct NAT technique is referred to by its corresponding name (Large Scale NAT44 [or CGN], DS-Lite and NAT64) with the understanding that in the context of 7750 SR platform, they are all part of LSN (and not enterprise based NAT).

Large Scale NAT44 term can be interchangeably used with the term Carrier Grade NAT (CGN) which in its name implies high reliability, high scale and high performance. These are again typical requirements found in service provider (carrier) network.

L2-Aware NAT term refers to a separate category of NAT defined outside of LSN.

NAT RADIUS accounting — Reporting (or logging) of address translation related events (port-block allocation/de-allocation) via RADIUS accounting facility. NAT RADIUS accounting is facilitated via regular RADIUS accounting messages (start/interim-update/stop) as defined in RFC 2866, *RADIUS Accounting*, with NAT specific VSAs.

NAT RADIUS accounting — Can be interchangeably used with the term NAT RADIUS logging.

NAT Subscriber — in NAT terminology a NAT subscriber is an inside entity whose true identity is hidden from the outside. There are a few types of NAT implementation in 7750 SR and subscribers for each implementation are defined as follows:

- Large Scale NAT44 (or CGN) — The subscriber is an inside IPv4 address.
- L2-Aware NAT — The subscriber is an ESM subscriber which can spawn multiple IPv4 inside addresses.
- DS-Lite — The subscriber in DS-lite can be identified by the CPE's IPv6 address (B4 element) or an IPv6 prefix. The selection of address or prefix as the representation of a DS-Lite subscriber is configuration dependent.
- NAT64 — The subscriber is an IPv6 prefix.

Non-deterministic NAT — A mode of operation where all outside IP address and port block allocations are made dynamically at the time of subscriber instantiation. Logging in such case is required.

Port block — A collection of ports that is assigned to a subscriber. A deterministic LSN subscriber can have only one deterministic port block that can be extended by multiple dynamic port blocks. Non-deterministic LSN subscriber can be assigned only dynamic port blocks. All port blocks for a LSN subscriber must be allocated from a single outside IP address.

Port-range — A collection of ports that can spawn multiple port blocks of the same type. For example, deterministic port-range includes all ports that are reserved for deterministic consumption. Similarly dynamic port-range is a total collection of ports that can be allocated in the form of dynamic port blocks. Other types of port-ranges are well-known ports and static port forwards.

## 7.2 Network Address Translation (NAT) Overview

The 7750 SR supports Network Address (and port) Translation (NAPT) to provide continuity of legacy IPv4 services during the migration to native IPv6. By equipping the multi-service ISA (MS ISA) in an IOM3-XP, the 7750 SR can operate in two different modes, known as:

- Large Scale NAT, and;
- Layer 2-Aware NAT

These two modes both perform source address and port translation as commonly deployed for shared Internet access. The 7750 SR with NAT is used to provide consumer broadband or business Internet customers access to IPv4 Internet resources with a shared pool of IPv4 addresses, such as may occur around the forecast IPv4 exhaustion. During this time it, is expected that native IPv6 services will still be growing and a significant amount of Internet content will remain IPv4.

### 7.2.1 Principles of NAT

Network Address Translation devices modify the IP headers of packets between a host and server, changing some or all of the source address, destination address, source port (TCP/UDP), destination port (TCP/UDP), or ICMP query ID (for ping). The 7750 SR in both NAT modes performs Source Network Address and Port Translation (S-NAPT). S-NAPT devices are commonly deployed in residential gateways and enterprise firewalls to allow multiple hosts to share one or more public IPv4 addresses to access the Internet. The common terms of inside and outside in the context of NAT refer to devices inside the NAT (that is behind or masqueraded by the NAT) and outside the NAT, on the public Internet.

TCP/UDP connections use ports for multiplexing, with 65536 ports available for every IP address. Whenever many hosts are trying to share a single public IP address there is a chance of port collision where two different hosts may use the same source port for a connection. The resultant collision is avoided in S-NAPT devices by translating the source port and tracking this in a stateful manner. All S-NAPT devices are stateful in nature and must monitor connection establishment and traffic to maintain translation mappings. The 7750 SR NAT implementation does not use the well-known port range (1 to 1023).

In most circumstances, S-NAPT requires the inside host to establish a connection to the public Internet host or server before a mapping and translation will occur. With the initial outbound IP packet, the S-NAPT knows the inside IP, inside port, remote IP, remote port and protocol. With this information the S-NAPT device can select an IP and port combination (referred to as outside IP and outside port) from its pool of addresses and create a unique mapping for this flow of data.

Any traffic returned from the server will use the outside IP and outside port in the destination IP/port fields – matching the unique NAT mapping. The mapping then provides the inside IP and inside port for translation.

The requirement to create a mapping with inside port and IP, outside port and IP and protocol will generally prevent new connections to be established from the outside to the inside as may occur when an inside host wishes to be a server.

## 7.2.2 Application Compatibility

Applications which operate as servers (such as HTTP, SMTP, and so on) or peer-to-peer applications can have difficulty when operating behind an S-NAPT because traffic from the Internet cannot reach the NAT without a mapping in place.

Different methods can be employed to overcome this, including:

- Port Forwarding;
- STUN support; and,
- Application Layer Gateways (ALG)

The 7750 SR supports all three methods following the best-practice RFC for TCP (RFC 5382, *NAT Behavioral Requirements for TCP*) and UDP (RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*). Port Forwarding is supported on the 7750 SR to allow servers which operate on well-known ports <1024 (such as HTTP and SMTP) to request the appropriate outside port for permanent allocation.

STUN is facilitated by the support of Endpoint-Independent Filtering and Endpoint-Independent Mapping (RFC 4787) in the NAT device, allowing STUN-capable applications to detect the NAT and allow inbound P2P connections for that specific application. Many new SIP clients and IM chat applications are STUN capable.

Application Layer Gateways (ALG) allows the NAT to monitor the application running over TCP or UDP and make appropriate changes in the NAT translations to suit. The 7750 SR has an FTP ALG enabled following the recommendation of the IETF BEHAVE RFC for NAT (RFC 5382).

---

Even with these three mechanisms some applications will still experience difficulty operating behind a NAT. As an industry-wide issue, forums like UPnP the IETF, operator and vendor communities are seeking technical alternatives for application developers to traverse NAT (including STUN support). In many cases the alternative of an IPv6-capable application will give better long-term support without the cost or complexity associated with NAT.



## 7.3 Large Scale NAT

Large Scale NAT represents the most common deployment of S-NAPT in carrier networks today, it is already employed by mobile operators around the world for handset access to the Internet.

A Large Scale NAT is typically deployed in a central network location with two interfaces, the inside towards the customers, and the outside towards the Internet. A Large Scale NAT functions as an IP router and is located between two routed network segments (the ISP network and the Internet).

Traffic can be sent to the Large Scale NAT function on the 7750 SR using IP filters (ACL) applied to SAPs or by installing static routes with a next-hop of the NAT application. These two methods allow for increased flexibility in deploying the Large Scale NAT, especially those environments where IP MPLS VPN are being used in which case the NAT function can be deployed on a single PE and perform NAT for any number of other PE by simply exporting the default route.

The 7750 SR NAT implementation supports NAT in the base routing instance and VPRN, and through NAT traffic may originate in one VPRN (the inside) and leave through another VPRN or the base routing instance (the outside). This technique can be employed to provide customers of IP MPLS VPN with Internet access by introducing a default static route in the customer VPRN, and NATing it into the Internet routing instance.

As Large Scale NAT is deployed between two routed segments, the IP addresses allocated to hosts on the inside must be unique to each host within the VPRN. While RFC1918 private addresses have typically been used for this in enterprise or mobile environments, challenges can occur in fixed residential environments where a subscriber has existing S-NAPT in their residential gateway. In these cases the RFC 1918 private address in the home network may conflict with the address space assigned to the residential gateway WAN interface. Some of these issues are documented in *draft-shirasaki-nat444-isp-shared-addr-02*. Should a conflict occur, many residential gateways will fail to forward IP traffic.

### 7.3.1 Port Range Blocks

The S-NAPT service on the 7750 SR BNG incorporates a port range block feature to address scalability of a NAT mapping solution. With a single BNG capable of hundreds of thousands of NAT mappings every second, logging each mapping as it is created and destroyed logs for later retrieval (as may be required by law enforcement) could quickly overwhelm the fastest of databases and messaging protocols. Port range blocks address the issue of logging and customer location

functions by allocating a block of contiguous outside ports to a single subscriber. Rather than log each NAT mapping, a single log entry is created when the first mapping is created for a subscriber and a final log entry when the last mapping is destroyed. This can reduce the number of log entries by 5000x or more. An added benefit is that as the range is allocated on the first mapping, external applications or customer location functions may be populated with this data to make real-time subscriber identification, rather than having to query the NAT as to the subscriber identity in real-time and possibly delay applications.

Port range blocks are configurable as part of outside pool configuration, allowing the operator to specify the number of ports allocated to each subscriber when a mapping is created. Once a range is allocated to the subscriber, these ports are used for all outbound dynamic mappings and are assigned in a random manner to minimize the predictability of port allocations (*draft-ietf-tsvwg-port-randomization-05*).

Port range blocks also serve another useful function in a Large Scale NAT environment, and that is to manage the fair allocation of the shared IP resources among different subscribers.

When a subscriber exhausts all ports in their block, further mappings will be prohibited. As with any enforcement system, some exceptions are allowed and the NAT application can be configured for reserved ports to allow high-priority applications access to outside port resources while exhausted by low priority applications.

### 7.3.1.1 Reserved Ports and Priority Sessions

Reserved ports allows an operator to configure a small number of ports to be reserved for designated applications should a port range block be exhausted. Such a scenario may occur when a subscriber is unwittingly subjected to a virus or engaged in extreme cases of P2P file transfers. In these situations, rather than block all new mappings indiscriminately the 7750 SR NAT application allows operators to nominate a number of reserved ports and then assign a 7750 SR forwarding class as containing high priority traffic for the NAT application. Whenever traffic reaches the NAT application which matches a priority session forwarding class, reserved ports will be consumed to improve the chances of success. Priority sessions could be used by the operator for services such as DNS, web portal, e-mail, VoIP, and so on, to permit these applications even when a subscriber exhausted their ports.

## 7.3.1.2 Preventing Port Block Starvation

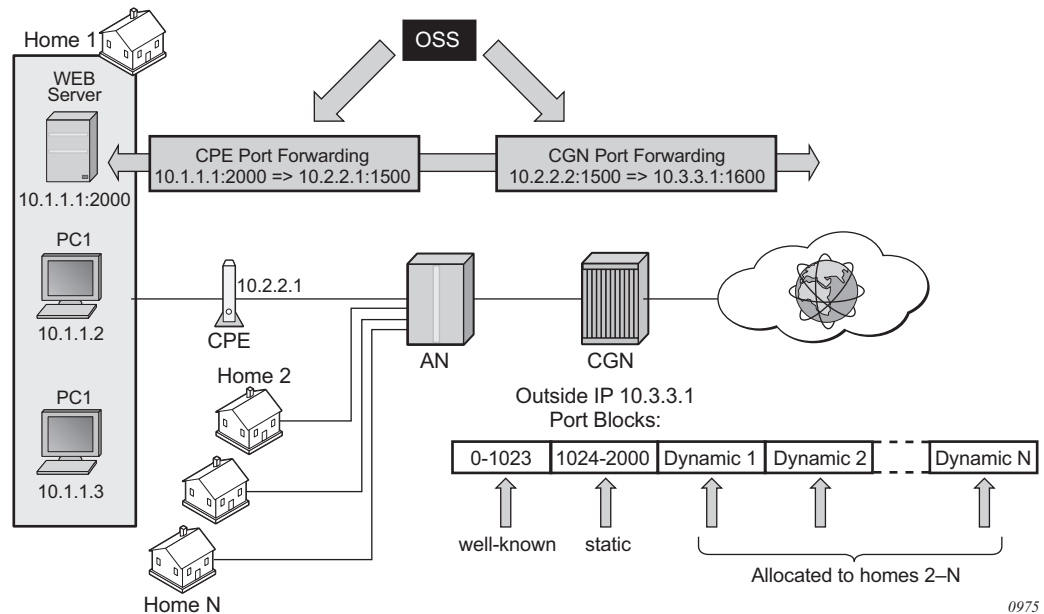
### 7.3.1.2.1 Dynamic Port Block Starvation in LSN

The outside IP address is always shared for the subscriber with a port forward (static or via PCP) and the dynamically allocated port block, insofar as the port from the port forward is in the range >1023. This behavior can lead to starvation of dynamic port blocks for the subscriber. An example for this scenario is shown in [Figure 55](#).

- A static port forward for the WEB server in Home 1 is allocated in the CPE and the CGN. At the time of static port forward creation, no other dynamic port blocks for Home 1 exist (PCs are powered off).
- Assume that the outside IP address for the newly created static port forward in the CGN is 10.3.3.1.
- Over time dynamic port blocks are allocated for a number of other homes that share the same outside IP address, 10.3.3.1. Eventually those dynamic port block allocations will exhaust all dynamic port block range for the address 10.3.3.1.
- Once the dynamic port blocks are exhausted for outside IP address 10.3.3.1, a new outside IP address (for example, 10.3.3.2) will be allocated for additional homes.

Eventually the PCs in Home 1 come to life and they try to connect to the Internet. Due to the dynamic port block exhaustion for the IP address 10.3.3.1 (that is mandated by static port forward – Web Server), the dynamic port block allocation will fail and consequently the PCs will not be able to access the Internet. There will be no additional attempt within CGN to allocate another outside IP address. In the CGN there is no distinction between the PCs in Home 1 and the Web Server when it comes to source IP address. They both share the same source IP address 10.2.2.1 on the CPE.

- The solution for this is to reserve a port block (or blocks) during the static port forward creation for the given subscriber.

**Figure 55 Dynamic Port Block Starvation in LSN**

0975

### 7.3.1.2.2 Dynamic Port Block Reservation

To prevent starvation of dynamic port blocks for the subscribers that utilize port forwards, a dynamic port block (or blocks) will be reserved during the lifetime of the port forward. Those reserved dynamic port blocks will be associated with the same subscriber that created the port forward. However, a log would not be generated until the dynamic port block is actually used and mapping within that block are created.

At the time of the port forward creation, the dynamic port block will be reserved in the following fashion:

- If the dynamic port block for the subscriber does not exist, then a dynamic port block for the subscriber will be reserved. No log for the reserved dynamic port block is generated until the dynamic port block starts being utilized (mapping created due to the traffic flow).
- If the corresponding dynamic port block already exists, then it will be reserved even after the last mapping within the last port block had expired.

The reserved dynamic port block (even without any mapping) will continue to be associated with the subscriber as long as the port forward for the subscriber is present. The log (syslog or RADIUS) will be generated only when there is not active mapping within the dynamic port block and all port forwards for the subscriber are deleted.

Additional considerations with dynamic port block reservation:

- The port block reservation should be triggered only by the first port forward for the subscriber. The subsequent port forwards will not trigger additional dynamic port block reservation.
- Only a single dynamic port block for the subscriber is reserved (that is, no multiple port-block reservations for the subscriber are possible).
- This feature is enabled with the configuration command **port-forwarding-dyn-block-reservation** under the **configure>service>vprn>nat>outside>pool** and the **configure>router>nat>outside>pool** CLI hierarchy. This command can be enabled only if the maximum number of configured port blocks per outside IP is greater or equal then the maximum configured number of subscribers per outside IP address. This will guarantee that all subscribers (up to the maximum number per outside IP address) configured with port forwards will be able to reserve a dynamic port block.
- In case that the port-reservation is enabled while the outside pool is operational and subscribers traffic is already present, the following two cases will have to be considered:
  - The configured number of subscribers per outside IP is less or equal than the configured number of port blocks per outside IP address (this is permitted) but all dynamic port blocks per outside IP address are occupied at the moment when port reservation is enabled. This will leave existing subscribers with port forwards that do not have any dynamic port blocks allocated (orphaned subscribers), unable to reserve dynamic port blocks. In this case the orphaned subscribers will have to wait until dynamic port blocks allocated to the subscribers without port forwards are freed.
  - The configured number of subscribers per outside IP is greater than the configured number of port blocks per outside IP address. In addition, all dynamic port blocks per outside IP address are allocated. Before the port reservation is even enabled, the subscriber-limit per outside IP address will have to be lowered (by configuration) so that it is equal or less than the configured number of port blocks per outside IP address. This action will cause random deletion of subscribers that do not have any port forwards. Such subscribers will be deleted until the number of subscriber falls below the newly configured subscriber limit. Subscribers with static port forwards will not be deleted, regardless of the configured subscriber-limit number. Once the number of subscriber is within the newly configured subscriber-limit, the port-reservation can take place under the condition that the dynamic port blocks are available. If certain subscribers with port forwards have more than one dynamic port block allocated, the orphaned subscribers will have to wait for those additional dynamic port blocks to expire and consequently be released.
- This feature is supported on the following applications: CGN, DS-Lite and NAT64.

## 7.3.2 Timeouts

Creating a NAT mapping is only one half of the problem – removing a NAT mapping at the appropriate time maximizes the shared port resource. Having ports mapped when an application is no longer active reduces solution scale and may impact the customer experience should they exhaust their port range block. The NAT application provides timeout configuration for TCP, UDP and ICMP.

TCP state is tracked for all TCP connections, supporting both three-way handshake and simultaneous TCP SYN connections. Separate and configurable timeouts exist for TCP SYN, TCP transition (between SYN and Open), established and time-wait state. Time-wait assassination is supported and enabled by default to quickly remove TCP mappings in the TIME WAIT state.

UDP does not have the concept of connection state and is subject to a simple inactivity timer. Company-sponsored research into applications and NAT behavior suggested some applications, like the Bittorrent Distributed Hash Protocol (DHT) can make a large number of outbound UDP connections that are unsuccessful. Rather than wait the default five (5) minutes to time these out, the 7750 SR NAT application supports an udp-initial timeout which defaults to 15 seconds. When the first outbound UDP packet is sent, the 15 second time starts – it is only after subsequent packets (inbound or outbound) that the default UDP timer will become active, greatly reducing the number of UDP mappings.

## 7.3.3 Watermarks

It is possible to define watermarks to monitor the actual usage of sessions and/or ports.

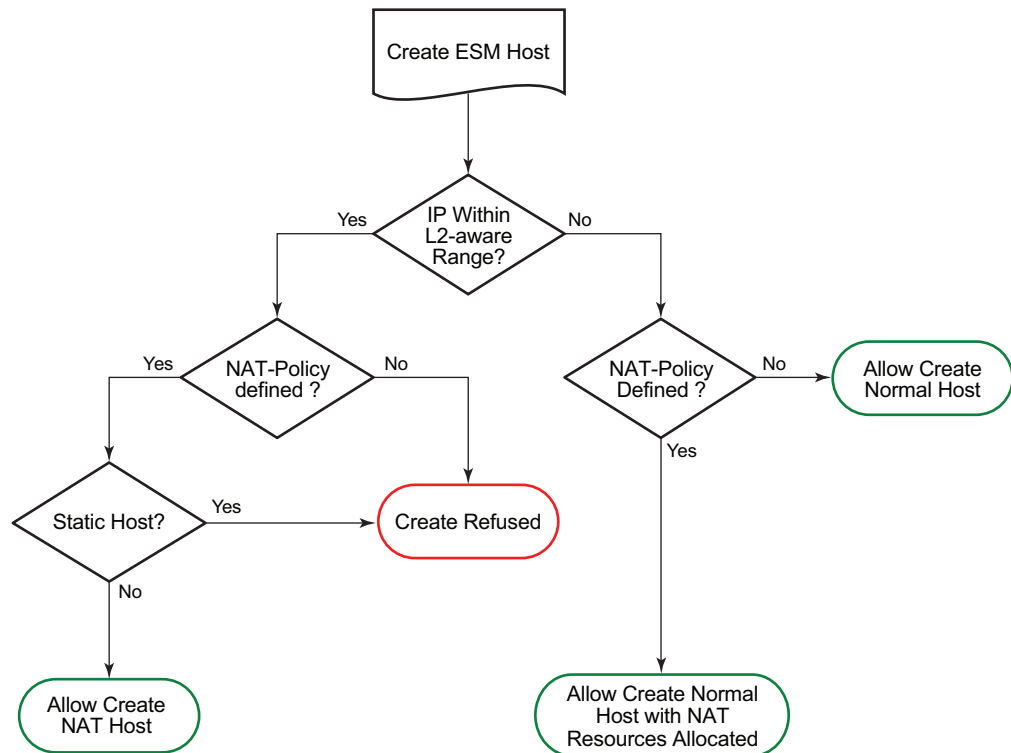
For each watermark, a high and a low value has to be set. Once the high value is reached, a notification will be send. As soon as the usage drops below the low watermark, another notification will be send.

Watermarks can be defined on nat-group, pool and policy level.

- **Nat-group:** Watermarks can be placed to monitor the total number of sessions on an MDA.
- **Pool:** Watermarks can be placed to monitor the total number of blocks in use in a pool.
- **Policy:** In the policy it is possible to define watermarks on session and port usage. In both cases, it is the usage per subscriber (for L2-Aware nat) or per host (for large-scale nat) that will be monitored.

## 7.4 L2-Aware NAT

**Figure 56** L2-Aware Tree



OSSG711

NAT is supported on DHCP, PPPoE and L2TP, there is not support for static and ARP hosts.

In an effort to address issues of conflicting address space raised in *draft-shirasaki-nat444-isp-shared-addr-02*, an enhancement to Large Scale NAT was co-developed to give every broadband subscriber their own NAT mapping table, yet still share a common outside pool of IPs.

Layer-2 Aware (or subscriber aware) NAT is combined with Enhanced Subscriber Management on the 7750 SR BNG to overcome the issues of colliding address space between home networks and the inside routed network between the customer and Large Scale NAT.

---

Layer-2 Aware NAT permits every broadband subscriber to be allocated the exact same IPv4 address on their residential gateway WAN link and then proceeds to translate this into a public IP through the NAT application. In doing so, L2-Aware NAT avoids the issues of colliding address space raised in draft-shirasaki without any change to the customer gateway or CPE.

Layer-2-Aware NAT is supported on any of the ESM access technologies, including PPPoE, IPoE (DHCP) and L2TP LNS. For IPoE both n:1 (VLAN per service) and 1:1 (VLAN per subscriber) models are supported. A subscriber device operating with L2-Aware NAT needs no modification or enhancement – existing address mechanisms (DHCP or PPP/PCP) are identical to a public IP service, the 7750 SR BNG simply translates all IPv4 traffic into a pool of IPv4 addresses, allowing many L2-Aware NAT subscribers to share the same IPv4 address.

More information on L2-Aware NAT can be found in draft-miles-behave-l2nat-00.



## 7.5 One-to-One (1:1) NAT

In 1:1 NAT, each source IP address is translated in 1:1 fashion to a corresponding outside IP address. However, the source ports are passed transparently without translation.

The mapping between the inside IP addresses and outside IP addresses in 1:1 NAT supports two modes:

- Dynamic - the operator can specify the outside IP addresses in the pool, but the exact mapping between the inside IP address and the configured outside IP addresses is performed dynamically by the system in a semi-random fashion.
- Static – the mappings between IP addresses are configurable and they can be explicitly set.

The dynamic version of 1:1 NAT is protocol dependent. Only TCP/UDP/ICMP protocols are allowed to traverse such NAT. All other protocols are discarded, with the exception of PPTP with ALG. In this case, only GRE traffic associated with PPTP is allowed through dynamic 1:1 NAT.

The static version of 1:1 NAT is protocol agnostic. This means that all IP based protocols are allowed to traverse static 1:1 NAT.

The following points are applicable to 1:1 NAT:

- Even though source ports are not being translated, the state maintenance for TCP and UDP traffic is still performed.
- Traffic can be initiated from outside towards any statically mapped IPv4 address.
- 1:1 NAT can be supported simultaneously with NAPT (classic non 1:1 NAT) within the same inside routing context. This is accomplished by configuring two separate NAT pools, one for 1:1 NAT and the other for non 1:1 NAPT.

### 7.5.1 Static 1:1 NAT

In static 1:1 NAT, inside IP addresses are statically mapped to the outside IP addresses. This way, devices on the outside can predictably initiate traffic to the devices on the inside.

Static configuration is based on the CLI concepts used in deterministic NAT. For example:

```
config
router
```

```

nat
 inside
 deterministic
 prefix 10.0.0.0/24 subscriber-type classic-lsn-sub nat-policy 'one-
to-one'
 map start 10.0.0.10 end 10.0.0.10 to 1.2.3.4
 map start 10.0.0.15 end 10.0.0.15 to 1.2.3.20
 map start 10.0.0.100 end 10.0.0.100 to 1.2.3.30

```

Static mappings are configured according to the map statements. The map statement can be configured manually by the operator or automatically by the system. IP addresses from the automatically generated map statements are sequentially mapped into available outside IP address in the pool:

- The first inside IP address is mapped to the first available outside IP address from the pool
- The second inside IP address is mapped to the second available outside IP address from the pool

The following mappings apply to the example above:

```

Static mappings
10.0.0.0 - 1.2.3.0
10.0.0.1 - 1.2.3.1
10.0.0.2 - 1.2.3.2
10.0.0.3 - 1.2.3.3
10.0.0.4 - 1.2.3.5
10.0.0.5 - 1.2.3.6
:
10.0.0.9 - 1.2.3.10
10.0.0.10 - 1.2.3.4
10.0.0.11 - 1.2.3.11
10.0.0.12 - 1.2.3.12
:
10.0.0.14 - 1.2.3.14
10.0.0.15 - 1.2.3.20
10.0.0.16 - 1.2.3.15
:
10.0.0.19 - 1.2.3.18
10.0.0.20 - 1.2.3.19
10.0.0.21 - 1.2.3.21
:
10.0.0.28 - 1.2.3.28
10.0.0.29 - 1.2.3.29
10.0.0.30 - 1.2.3.31
:
10.0.0.99 - 1.2.3.100
10.0.0.100 - 1.2.3.30
10.0.0.101 - 1.2.3.101
:
10.0.0.255 - 1.2.3.255

```

### 7.5.1.1 Protocol Agnostic Behavior

Although static 1:1 NAT is protocol agnostic, the state maintenance for TCP and UDP traffic is still required in order to support ALGs. Therefore, the existing scaling limits related to the number of supported flows still apply.

Protocol agnostic behavior in 1:1 NAT is a property of a NAT pool:

```
config
 router / service vprn
 nat
 outside
 pool "one-to-one" nat-group 1 type large-
scale applications agnostic create
 address-range 192.168.0.0 192.168.255.255 create
```

The application **agnostic** command is a pool create-time parameter. This command automatically pre-sets the following pool parameters:

```
mode one-to-one
port-forwarding-range 0
port-reservation blocks 1
subscriber-limit 1
deterministic port-reservation 65536.
```

Once pre-set, these parameters cannot be changed while the pool is operating in protocol agnostic mode.

The **deterministic port-reservation 65536** command configures the pool to operate in static (or deterministic) mode.

### 7.5.1.2 Modification of Parameters in Static 1:1 NAT

Parameters in the static 1:1 NAT can be changed according to the following rules:

- The deterministic pool must be in a **no shutdown** state when a **prefix** or a **map** command in deterministic NAT is added or removed.
- All configured prefixes referencing the pool via the NAT policy must be deleted (un-configured) before the pool can be shut down.
- Map statements can be modified only when prefix is shutdown state. All existing map statements must be removed before the new ones are created.

### 7.5.1.3 Load Distribution over ISAs in Static 1:1 NAT

For best traffic distribution over ISAs, the value of the **classic-lsn-max-subscriber-limit** *max* parameter should be set to 1.

```
config
 router / service vprn X
 nat
 inside
 deterministic
 classic-lsn-max-subscriber-limit <num>
```

This means that traffic is load balanced over ISAs based on inside IP addresses. In static 1:1 NAT this is certainly possible since the subscriber-limit parameter at the pool level is preset to a fixed value of 1.

However, if 1:1 static NAT is simultaneously used with regular (many-to-one) deterministic NAT where the subscriber-limit parameter can be set to a value greater than 1, then the classic-lsn-max-subscriber-limit parameter will also have to be set to a value that is greater than 1. The consequence of this is that the traffic will be load balanced based on the consecutive blocks of IP addresses (subnets) rather than individual IP addresses. See [Deterministic NAT](#) for information about Deterministic NAT behavior.

### 7.5.1.4 NAT-Policy Selection

The traffic match criteria used in the selection of specific NAT policies in static 1:1 NAT (the deterministic part of the configuration) must not overlap with traffic match criteria that is used in the selection of a specific NAT policy used in filters or in destination-prefix statement (these are used for traffic diversion to NAT). Otherwise, traffic will be dropped in ISA.

A specific NAT policy in this context refers to a non-default NAT policy, or a NAT policy that is directly referenced in a filter, in a **destination-prefix** command or in a **deterministic prefix** command.

The following example is used to clarify this point.

- Traffic is diverted to NAT using specific **nat-policy** *pol-2*:

```
service vprn 10
 nat
 inside
 destination-prefix 192.168.0.0/16 nat-policy pol-2
 deterministic
 prefix 10.10.10.0/24 subscriber-type classic-lsn-sub nat-policy pol-1
```

- The deterministic (source) prefix 10.10.10.0/30 is configured to be mapped to **nat-policy** pol-1 specifically which points to protocol agnostic 1:1 nat pool.

```
service vprn 10
 nat
 inside
 destination-prefix 192.168.0.0/16 nat-policy pol-2
 deterministic
 prefix 10.10.10.0/30 subscriber-type classic-lsn-sub nat-policy pol-1
```

- Packet received in the ISA has srcIP 10.10.10.1 and destIP 192.168.10.10.
- If no NAT mapping for this traffic exists in the ISA, a NAT policy (and with this, the NAT pool) must be determined in order to create the mapping. Traffic is diverted to NAT using **nat-policy** pol-2, while the deterministic mapping suggests that **nat-policy pol-1** should be used (this is a different pool from the one referenced in **nat-policy pol-2**). Due to the specific NAT policy conflict, traffic will be dropped in the ISA.

In order to successfully pass traffic between two subnets through NAT while simultaneously using static 1:1 NAT and regular LSN44, a default (**non-specific**) NAT policy can be used for regular LSN44.

For example:

```
service vprn 10
 nat
 inside
 destination-prefix 192.168.0.0/16
 nat-policy pol-2
 deterministic
 prefix 10.10.10.0/30 subscriber-type classic-lsn-sub nat-
policy pol-1
```

In this case, the four hosts from the prefix 10.10.10.0/30 are mapped in 1:1 fashion to 4 IP addresses from the pool referenced in the specific nat-policy pol-1, while all other hosts from the 10.10.10.0/24 network are mapped to the NAT pool referenced by the default nat-policy pol-2. In way, a NAT policy conflict is avoided.

In summary, a specific NAT policy (in filter, **destination-prefix** command or in deterministic **prefix** command) will always take precedence over a default NAT policy. However, traffic that matches classification criteria (in filter, **destination-prefix** command or a deterministic **prefix** command) that leads to multiple specific nat-policies, will be dropped.

---

### 7.5.1.5 Mapping Timeout

Static 1:1 NAT mappings are explicitly configured, and therefore, their lifetime is tied to the configuration.

### 7.5.1.6 Logging

The logging mechanism for static mapping is the same as in Deterministic NAT. Configuration changes are logged via syslog and enhanced with reverse querying on the system.

### 7.5.1.7 Restrictions

Static 1:1 NAT is supported only for LSN44 (there is no support for DS-Lite/NAT64 or L2-Aware NAT).

## 7.5.2 ICMP

In 1:1 NAT, certain ICMP messages contain an additional IP header embedded in the ICMP header. For example, when the ICMP message is sent to the source due to the inability to deliver datagram to its destination, the ICMP generating node includes the original IP header of the packet plus 64bits of the original datagram. This information helps the source node to match the ICMP message to the process associated with this message.

When these messages are received in the downstream direction (on the outside), 1:1 NAT recognizes them and changes the destination IP address not only in the outside header but also in the ICMP header. In other words, a lookup in the downstream direction is performed in the ISA to determine if the packet is ICMP with a specific type. Depending on the outcome, the destination IP address in the ICMP header is changed (reverted to the original source IP address).

Messages carrying the original IP header within ICMP header are:

- Destination Unreachable Messages (Type 3)
- Time Exceeded Message (Type 11)
- Parameter Problem Message (Type 12)
- Source Quench Message (Type 4)

## 7.6 Deterministic NAT

### 7.6.1 Overview

In deterministic NAT the subscriber is deterministically mapped into an outside IP address and a port block. The algorithm that performs this deterministic mapping is revertive, which means that a NAT subscriber can be uniformly derived from the outside IP address and the outside port (and the routing instance). Thus, logging in deterministic NAT is not needed.

The deterministic [subscriber <-> outside-ip, deterministic-port-block] mapping can be automatically extended by a dynamic port-block in case that deterministic port block becomes exhausted of ports. By extending the original deterministic port block of the NAT subscriber by a dynamic port block yields a satisfactory compromise between a deterministic NAT and a non-deterministic NAT. There will be no logging as long as the translations are in the domain of the deterministic NAT. Once the dynamic port block is allocated for port extension, logging will be automatically activated.

NAT subscribers in deterministic NAT are not assigned outside IP address and deterministic port-block on a first come first serve basis. Instead, deterministic mappings will be pre-created at the time of configuration regardless of whether the NAT subscriber is active or not. In other words we can say that overbooking of the outside address pool is not supported in deterministic NAT. Consequently, all configured deterministic subscribers (for example, inside IP addresses in LSN44 or IPv6 address/prefix in DS-Lite) will be guaranteed access to NAT resources.

### 7.6.2 Supported Deterministic NAT Types

The routers support Deterministic LSN44 and Deterministic DS-Lite. The basic deterministic NAT principle is applied equally to both NAT flavors. The difference between the two stem from the difference in interpretation of the subscriber – in LSN44 a subscriber is an IPv4 address, whereas in DS-Lite the subscriber is an IPv6 address or prefix (configuration dependent).

With the exception of **classic-lsn-max-subscriber-limit** and **dslite-max-subscriber-limit** commands in the inside routing context, the deterministic NAT configuration blocks are for the most part common to LSN44 and DS-Lite.

Deterministic DS-Lite section at the end of this section will focus on the features specific to DS-Lite.

### 7.6.3 Number of Subscribers per Outside IP and per Pool

The outside pools in deterministic NAT can contain an arbitrary number of address ranges, where each address range can contain an arbitrary number of IP addresses (up to the ISA maximum).

The maximum number of NAT subscribers that can be mapped to a single outside IP address is configurable using a **subscriber-limit** command under the pool hierarchy. For Deterministic NAT, this number is restricted to the power of 2 ( $2^n$ ). The consequence of this is that the number of NAT subscribers must be configuration-wise organized in ranges with the boundary that must be power of 2.

For example, in LSN44 where the NAT subscriber is an IP address, the deterministic subscribers would be configured with prefixes (for example, 10.10.10.0/24 – 256 subscribers) rather than an IP address range that would contain an arbitrary number of addresses (e.g. 10.10.10.10 – 10.10.10.50).

On the other hand, in DS-Lite the deterministic subscribers are for the most part already determined by the prefix with the **subscriber-prefix-length** command under the DS-Lite configuration node.

The number of subscribers per outside IP (the **subscriber-limit** command [ $2^n$ ]) multiplied by the number of IP addresses over all address-range in an outside pool will determine the maximum number of subscribers that a deterministic pool can support.

### 7.6.4 Referencing a Pool

In deterministic NAT, the outside pool can be shared amongst subscribers from multiple routing instances. Also, NAT subscribers from a single routing instance can be selectively mapped to different outside pools.

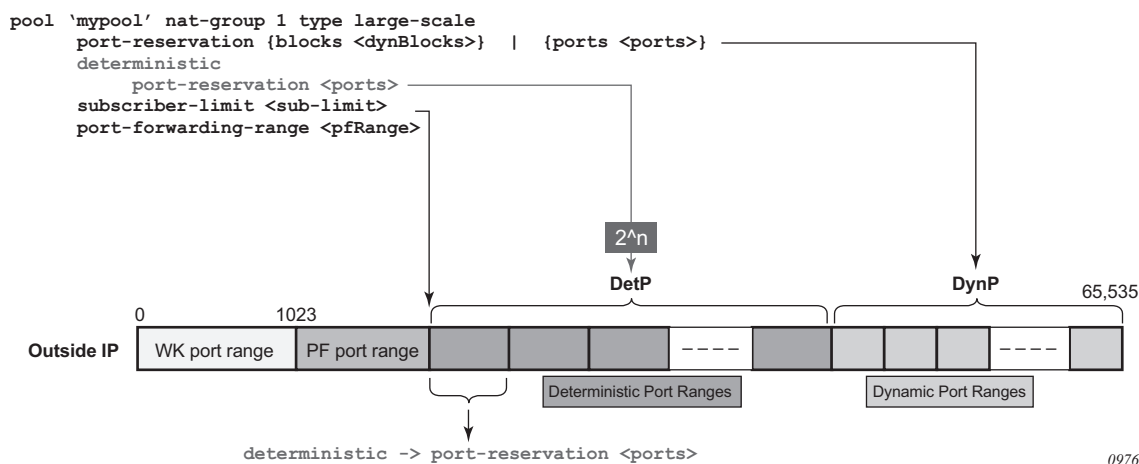
### 7.6.5 Outside Pool Configuration

The number of deterministic mappings that a single outside IP address can sustain is determined through the configuration of the outside pool.

The port allocation per an outside IP is shown in [Figure 57](#).



**Figure 57 Outside Pool Configuration**



The well-known ports are predetermined and are in the range 0 — 1023.

The upper limit of the port range for static port forwards (wildcard range) is determined by the existing **port-forwarding-range** command.

The range of ports allocated for deterministic mappings (DetP) is determined by multiplying the number of subscribers per outside IP (**subscriber-limit** command) with the number of ports per deterministic block (**deterministic>port-reservation** command). The number of subscribers per outside IP in deterministic NAT must be power of 2 ( $2^n$ ).

The remaining ports, extending from the end of the deterministic port range to the end of the total port range (65,535) are used for dynamic port allocation. The size of each dynamic port block is determined with the existing **port-reservation** command.

The **deterministic>port-reservation** command enables deterministic mode of operation for the pool.

Examples:

The follow show three examples with deterministic Large Scale NAT44 where the requirements are:

- 300, 500 or 700 (three separate examples) ports in each deterministic port block.
- A subscriber (an inside IPv4 address in LSN44) can extend its deterministic ports by a minimum of one dynamic port-block and by a maximum of four dynamic port blocks.
- Each dynamic port-block contains 100 ports.

- Oversubscription of dynamic port blocks is 4:1. This means that 1/4th of inside IP addresses may be starved out of dynamic port blocks in worst case scenario.
- The wildcard (static) port range is 3000 ports.

In the first case, the ideal case will be examined where an arbitrary number of subscribers per outside IP address is allocated according to our requirements outlined above. Then the limitation of the number of subscribers being power of 2 will be factored in.

**Table 32** Contiguous Number of Subscribers

| Well-Known Ports* | Static Port Range* | Number of Ports in Deterministic Block* | Number of Deterministic Blocks | Number of Ports in Dynamic Block* | Number of Dynamic Blocks | Number of Inside IP Addresses per Outside IP Address* | Block Limit per Inside IP Address* | Wasted Ports |
|-------------------|--------------------|-----------------------------------------|--------------------------------|-----------------------------------|--------------------------|-------------------------------------------------------|------------------------------------|--------------|
| 0-1023            | 1024-4023          | 300                                     | 153                            | 100                               | 153                      | 153                                                   | 5                                  | 312          |
| 0-1023            | 1024-4023          | 500                                     | 102                            | 100                               | 102                      | 102                                                   | 5                                  | 312          |
| 0-1023            | 1024-4023          | 700                                     | 76                             | 100                               | 76                       | 76                                                    | 5                                  | 712          |

The example in [Table 32](#) shows how port ranges would be carved out in ideal scenario.

\* — Signifies the fixed parameters (requirements).

The other values are calculated according to the fixed requirements.

**port-block-limit** includes the deterministic port block plus all dynamic port-blocks.

Next, a more realistic example with the number of subscribers being equal to 2^n are considered. The ratio between the deterministic ports and the dynamic ports per port-block just like in the example above: 3/1, 5/1 and 7/1 are preserved. In this case, the number of ports per port-block is dictated by the number of subscribers per outside IP address.

**Table 33** Preserving Det/Dyn Port Ratio with 2^n Subscribers

| Well-Known Ports* | Static Port Range* | Number of Ports in Deterministic Block* | Number of Deterministic Blocks | Number of Ports in Dynamic Block* | Number of Dynamic Blocks | Number of Inside IP Addresses per Outside IP Address* | Block Limit per Inside IP Address* | Wasted Ports |
|-------------------|--------------------|-----------------------------------------|--------------------------------|-----------------------------------|--------------------------|-------------------------------------------------------|------------------------------------|--------------|
| 0-1023            | 1024-4023          | 180                                     | 256                            | 60                                | 256                      | 256                                                   | 5                                  | 72           |
| 0-1023            | 1024-4023          | 400                                     | 128                            | 80                                | 128                      | 128                                                   | 5                                  | 72           |
| 0-1023            | 1024-4023          | 840                                     | 64                             | 120                               | 64                       | 64                                                    | 5                                  | 72           |

\* — Signifies the fixed parameters (requirements).

The final example is similar as [Table 32](#) with the difference that the number of deterministic port blocks fixed are kept, as in the original example (300, 500 and 700).

**Table 34** Fixed Number of Deterministic Ports with 2<sup>n</sup> Subscribers

| Well-Known Ports | Static Port Range | Number of Ports in Deterministic Block | Number of Deterministic Blocks | Number of Ports in Dynamic Block | Number of Dynamic Blocks | Number of Inside IP Addresses per Outside IP Address | Block Limit per Inside IP Address | Wasted Ports |
|------------------|-------------------|----------------------------------------|--------------------------------|----------------------------------|--------------------------|------------------------------------------------------|-----------------------------------|--------------|
| 0-1023           | 1024-4023         | 300                                    | 128                            | 180                              | 128                      | 128                                                  | 5                                 | 72           |
| 0-1023           | 1024-4023         | 500                                    | 64                             | 461                              | 64                       | 64                                                   | 5                                 | 8            |
| 0-1023           | 1024-4023         | 700                                    | 64                             | 261                              | 64                       | 64                                                   | 5                                 | 8            |

The three examples from above should give us a perspective on the size of deterministic and dynamic port blocks in relation to the number of subscribers (2<sup>n</sup>) per outside IP address. Operators should run a similar dimensioning exercise before they start configuring their deterministic NAT.

The CLI for the highlighted case in the [Table 32](#) is displayed:

```
configure
 service
 vprn
 nat
 outside
 pool mypool
 port-reservation ports 180
 deterministic
 port-reservation 300
 subscriber-limit 128
 port-forwarding-range 4023
```

Where:

128 subs \* 300ports = 38,400 deterministic port range

128 subs \* 180ports = 23,040 dynamic port range

Det+dyn available ports = 65,536 – 4024 = 61,512

Det+dyn usable pots = 128\*300 + 128 \*180 = 61,440 ports

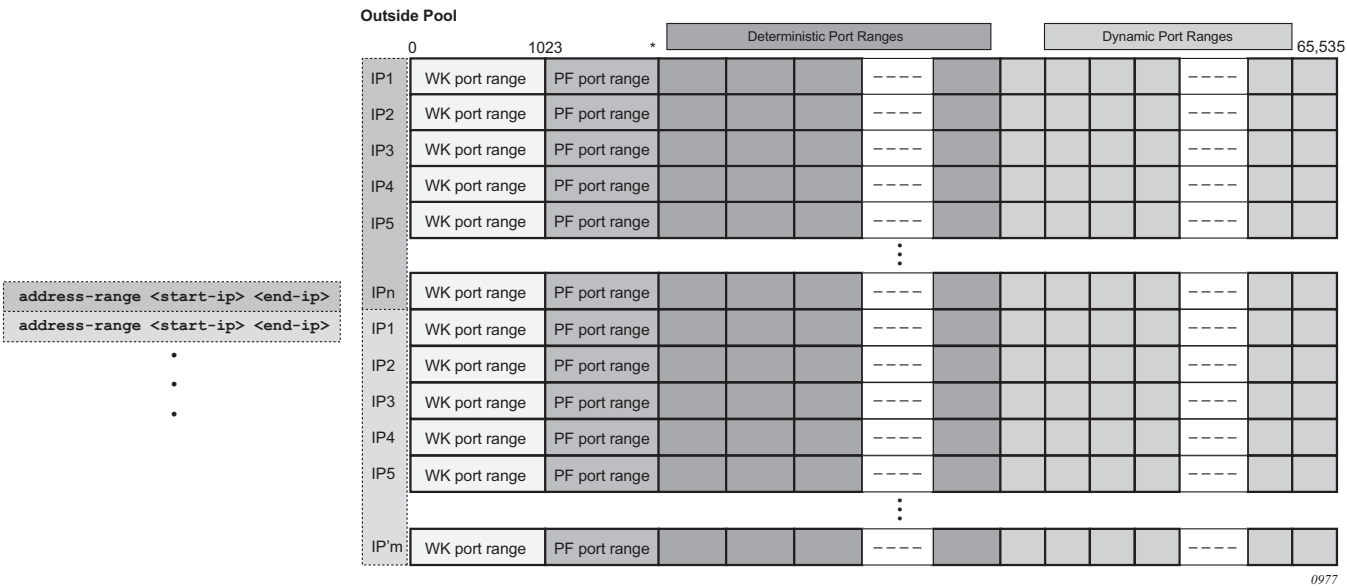
72 ports per outside-ip are wasted.

```
configure
service
nat
 nat-policy mypolicy
 block-limit 5 ? 1 deterministic port block + 4 dynamic port blocks
```

This configuration will allow 128 subscribers (inside IP addresses in LSN44) for each outside address (compression ratio is 128:1) with each subscriber being assigned up to 1020 ports (300 deterministic and 720 dynamic ports over 4 dynamic port blocks).

The outside IP addresses in the pool and their corresponding port ranges are organized as shown in [Figure 58](#).

Figure 58 Outside Address Ranges



Assuming that the above graph depicts an outside deterministic pool, the number of subscribers that can be accommodated by this deterministic pool is represented by purple squares (number of IP addresses in an outside pool \* subscriber-limit). The number of subscribers across all configured prefixes on the inside that are mapped to the same deterministic pool must be less than the outside pool can accommodate. In other words, an outside address pool in deterministic NAT cannot be oversubscribed.

The following is a CLI representation of a deterministic pool definition including the outside IP ranges:

```
pool 'mypool' nat-group 1 type large-scale
 port-reservation {blocks <dynBlocks>} | {ports <ports>}
 deterministic
 port-reservation <ports>
 subscriber-limit <sub-limit>
 port-forwarding-range <pfRange>
 address-range <start-ip-address> <end-ip-address>
 address-range <start-ip-address> <end-ip-address>
```

## 7.6.6 Mapping Rules and the map Command in Deterministic LSN44

The common building block on the inside in the deterministic LSN44 configuration is a IPv4 prefix. The NAT subscribers (inside IPv4 addresses) from the configured prefix will be deterministically mapped to the outside IP addresses and corresponding deterministic port-blocks. Any inside prefix in any routing instance can be mapped to any pool in any routing instance (including the one in which the inside prefix is defined).

The mapping between the inside prefix and the deterministic pool is achieved through a NAT policy that can be referenced per each individual inside IPv4 prefix. IPv4 addresses from the prefixes on the inside will be distributed over the IP addresses defined in the outside pool referenced by the NAT policy.

The mapping itself is represented by the **map** command under the prefix hierarchy:

```
router/service vprn
 nat
 inside
 deterministic
 prefix <ip-prefix/length> subscriber-type <nat-sub-type> nat-
policy <nat-policy-name>
 map start <inside-ip-address> end <inside-ip-address> to <outside-ip-
address>
```

The purpose of the map statement is to split the number of subscribers within the configured prefix over available sequences of outside IP addresses. The key parameter that governs mappings between the inside IPv4 addresses and outside IPv4 addresses in deterministic LSN44 is defined by the **outside>pool>subscriber-limit** command. This parameter must be power of 2 and it limits the maximum number of NAT subscribers that can be mapped to the same outside IP address.

The follow are rules governing the configuration of the map statement:

- Step 1.** If the number of subscribers per configured prefix is greater than the subscriber-limit per outside IP parameter ( $2^n$ ), then the lowest  $n$  bits of the **map start** *inside-ip-address* must be set to 0.
- Step 2.** If the number of subscribers per configured prefix is equal or less than the subscriber-limit per outside IP parameter ( $2^n$ ), then only one **map** command for this prefix is allowed. In this case there is no restriction on the lower  $n$  bits of the **map start** *inside-ip-address*. The range of the inside IP addresses in such map statement represents the prefix itself.
- Step 3.** The *outside-ip-address* in the map statements must be unique amongst all map statements referencing the same pool. In other words, two map statements cannot reference the same *outside-ip-address* in the pool.

In case that the number of subscribers (IP addresses in LSN44) in the **map** statement is larger than the subscriber-limit per outside IP, then the subscribers must be split over a block of consecutive outside IP addresses where the *outside-ip-address* in the map statement represent only the first outside IP address in that block.

The number of subscribers (range of inside IP addresses in LSN44) in the map statement does not have to be a power of 2. Rather it has to be a multiple of a power of two  $m * 2^n$ , where  $m$  is the number of consecutive outside IP addresses to which the subscribers are mapped and the  $2^n$  is the subscriber-limit per outside IP.

An example of the map statement is given below:

```
router
nat
 outside
 pool 'my-det-pool' nat-group 1 type large-scale
 subscriber-limit 128
 deterministic
 port-reservation 400
 address-range 192.168.0.0 192.168.0.10

service vprn 10
nat
 inside
 deterministic
 prefix 10.0.0.0/24 subscriber-type classic-lsn-sub nat-policy det
 map start 10.0.0.0 end 10.0.0.255 to 192.168.0.1
```

In this case, the configured 10.0.0.0/24 prefix is represented by the range of IP addresses in the map statement (10.0.0.0-10.0.0.255). Since the range of 256 IP addresses in the map statement cannot be mapped into a single outside IP address (subscriber-limit=128), this range must be further implicitly split within the system and mapped into multiple outside IP addresses. The implicit split will create two IP address ranges, each with 128 IP addresses (10.0.0.0/25 and 10.0.0.128/25) so that

addresses from each IP range are mapped to one outside IP address. The hosts from the range 10.0.0.0-10.0.0.127 will be mapped to the first IP address in the pool (128.251.0.1) as explicitly stated in the map statement (to statement). The hosts from the second range, 10.0.0.128-10.0.0.255 will be implicitly mapped to the next consecutive IP address (128.251.0.2).

Alternatively, the **map** statement can be configured as:

```
service vprn 10
nat
 inside
 deterministic
 prefix 10.0.0.0/24 subscriber-type classic-lsn-sub nat-policy det
 map start 10.0.0.0 end 10.0.0.127 to 192.168.0.1
 map start 10.0.0.128 end 10.0.0.255 to 192.168.0.5
```

In this case the IP address range in the map statement is split into two non-consecutive outside IP addresses. This gives the operator more freedom in configuring the mappings.

However, the following configuration is not supported:

```
service vprn 10
nat
 inside
 deterministic
 prefix 10.0.0.0/24 subscriber-type classic-lsn-sub nat-policy det
 map start 10.0.0.0 end 10.0.0.63 to 192.168.0.1
 map start 10.0.0.64 end 10.0.0.127 to 192.168.0.3
 map start 10.0.0.128 end 10.0.0.255 to 192.168.0.5
```

Considering that the subscriber-limit = 128 ( $2^n$ ; where  $n=7$ ), the lower  $n$  bits of the start address in the second map statement (map start 10.0.0.64 end 10.0.0.127 to 192.168.0.3) are not 0. This is in violation of the rule #1 that governs the provisioning of the map statement.

Assuming that we use the same pool with 128 subscribers per outside IP address, the following scenario is also not supported (configured prefix in this example is different than in previous example):

```
service vprn 10
nat
 inside
 deterministic

prefix 10.0.0.0/26 subscriber-type classic-lsn-sub nat-policy det
 map start 10.0.0.0 end 10.0.0.63 to 192.168.0.1

prefix 10.0.1.0/26 subscriber-type classic-lsn-sub nat-policy det
 map start 10.0.1.0 end 10.0.1.63 to 192.168.0.1
```



Although the lower  $n$  bits in both map statements are 0, both statements are referencing the same outside IP (192.168.0.1). This is violating rule #2 that governs the provisioning of the map statement. Each of the prefixes in this case will have to be mapped to a different outside IP address, which will lead to underutilization of outside IP addresses (half of the deterministic port-blocks in each of the two outside IP addresses will not be utilized).

In conclusion, considering that the number of subscribers per outside IP (subscriber-limit) must be  $2^n$ , the inside IP addresses from the configured prefix will be split on the  $2^n$  boundary so that every deterministic port-block of an outside IP is utilized. In case that the originally configured prefix contains less subscribers (IP addresses in LSN44) than an outside IP address can accommodate ( $2^n$ ), all subscribers from such configured prefix will be mapped to a single outside IP. Since the outside IP cannot be shared with NAT subscribers from other prefixes, some of the deterministic port-blocks for this particular outside IP address are not utilized.

Each configured prefix can evaluate into multiple **map** commands. The number of **map** commands will depend on the length of the configured prefix, the **subscriber-limit** command and fragmentation of outside address-range within the pool with which the prefix is associated.

## 7.6.7 Hashing Considerations in Deterministic LSN44

Support for multiple MS-ISAs in the nat-group calls for traffic hashing on the inside in the ingress direction. This will ensure fair load balancing of the traffic amongst multiple MS-ISAs. While hashing in non-deterministic LSN44 can be performed per source IP address, hashing in deterministic LSN44 is based on subnets instead of individual IP addresses. The length of the hashing subnet is common for all configured prefixes within an inside routing instance. In case that a prefixes from an inside routing instances is referencing multiple pools, the common hashing prefix length will be chosen according to the pool with the highest number of subscribers per outside IP address. This will ensure that subscribers mapped to the same outside IP address will be always hashed to the same MS-ISA.

In general, load distribution based on hashing is dependent on the sample. Large and more diverse sample will ensure better load balancing. Therefore the efficiency of load distribution between the MS-ISAs is dependent on the number and diversity of subnets that hashing algorithm is taking into consideration within the inside routing context.

A simple rule for good load balancing is to configure a large number of subscribers relative to the largest  $t$  subscriber-limit parameter in any given pool that is referenced from this inside routing instance.

Figure 59 Deterministic LSN44 Configuration Example

|                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>VRPN 1 nat   inside     prefix 10.10.10.0/24 nat-policy &lt;pool-1&gt;     prefix 10.20.20.0/23 nat-policy &lt;pool-1&gt;     max-subscriber-limit-in-deterministic-pools 64</pre>                                    | <pre>VRPN 3 nat   outside     pool 'pool-1' nat-group 1 type large-scale       port-reservation blocks 100       deterministic-port-reservation ports 500       subscriber-limit 54       port-forwarding-range 5000       address-range 10.0.1.0 10.0.1.100       address-range 10.0.2.0 10.0.2.200      pool 'pool-2' nat-group 1 type large-scale       port-reservation blocks 500       deterministic-port-reservation ports 200       subscriber-limit 256       port-forwarding-range 5000       address-range 10.0.3.0 10.0.3.100       address-range 10.0.4.0 10.0.4.200</pre>                                                                                                                                                                                                                                                                                                       |
| <pre>VRPN 2 nat   inside     prefix 10.10.10.0/24 nat-policy &lt;pool-1&gt;     prefix 10.20.20.0/23 nat-policy &lt;pool-1&gt;     max-subscriber-limit-in-deterministic-pools 256</pre>                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>VRPN 1<br/>768 subscribers -&gt; to pool-1<br/>Source prefixes will be divided into 12/26 prefixes that will be load balanced over ISAs.<br/>Load balancing: low to medium</p>                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>VRPN 2<br/>256 subscribers -&gt; to pool-1<br/>65536 subscribers -&gt; to pool-2<br/>Source prefixes will be internally divided into 257/24 prefixes that will be load balanced over ISAs.<br/>Load balancing: good</p> | <p>Pool-1:<br/>Subscribers per outside IP: 64 (config: 2^n: n=6)<br/>Total subscribers per pool: 19326 (302 outside_IPs * 64 subs)<br/><br/>Ports per deterministic block = 500 (config)<br/>Deterministic port range: 5001-37000<br/><br/>Dynamic port range: 37001-65535<br/>Dynamic port blocks: 100 (config)<br/>Ports per dynamic block: 285<br/>Ports wasted per outside IP: 35<br/>Unutilized IPs according to the mappings: 18304</p> <p>Pool-2:<br/>Subscribers per outside IP: 256 (config: 2^n: n=8)<br/>Total subscribers per pool: 77312 (302 outside_IPs * 256 subs)<br/><br/>Ports per deterministic block = 200 (config)<br/>Deterministic port range: 5001-51200<br/><br/>Dynamic port range: 51201-65535<br/>Dynamic port blocks: 500 (config)<br/>Ports per dynamic block: 28<br/>Ports wasted per outside IP: 334<br/>Unutilized IPs according to the mappings: 11776</p> |

0979

The configuration example shown [Figure 59](#) depicts a case in which prefixes from multiple routing instances are mapped to the same outside pool and at the same time the prefixes from a single inside routing instance are mapped to different pools (we do not support the latter with non-deterministic NAT).



**Note:** In this example is the inside prefix 10.10.10.0/24 that is present in VRPN 1 and VRPN 2. In both VRPNs, this prefix is mapped to the same pool - pool-1 with the subscriber-limit of 64. Four outside IP addresses per prefix per VRPN (eight in total) are allocated to accommodate the mappings for all hosts in prefix 10.10.10.0/24. But the hashing prefix length in VRPN1 is based on the subscriber-limit 64 (VRPN1 references only pool-1) while the hashing prefix length in VRPN2 is based on the subscriber-limit 256 in pool-2 (VRPN2 references both pools, pool-1 and pool-2 and we must select the larger subscriber-limit). The consequence of this is that the traffic from subnet 10.10.10.0/24 in VRPN 1 can be load balanced over 4 MS-ISA (hashing prefix length is 26) while traffic from the subnet 10.10.10.0/24 in VRPN 2 is always sent to the same MS-ISA (hashing prefix length is 24).

### **7.6.7.1 Distribution of Outside IP Addresses Across MS-ISAs in an MS-ISA NA Group**

Distribution of outside IP addresses across the MS-ISAs is dependent on the ingress hashing algorithm. Since traffic from the same subscriber is always pre-hashed to the same MS-ISA, the corresponding outside IP address also must reside on the same ISA. CPM runs the hashing algorithm in advance to determine on which MS-ISA the traffic from particular inside subnet will land and then the corresponding outside IP address (according to deterministic NAT mapping algorithm) will be configured in that particular MS-ISA.

### **7.6.8 Sharing of Deterministic NAT Pools**

Sharing of the deterministic pools between LSN44 and DS-Lite is supported.

### **7.6.9 Simultaneous support of dynamic and deterministic NAT**

Simultaneous support for deterministic and non-deterministic NAT inside of the same routing instance is supported. However, an outside pool can be only deterministic (although expandable by dynamic ports blocks) or non-deterministic at any given time.

Ingress hashing for all NATed traffic within the VRF will in this case be performed based on the subnets driven by the classic-lsn-max-subscriber-limit parameter.

### **7.6.10 Selecting Traffic for NAT**

Deterministic NAT does not change the way how traffic is selected for the NAT function but instead only defines a predictable way for translating subscribers into outside IP addresses and port-blocks.

Traffic is still diverted to NAT using the existing methods:

- routing based – traffic is forwarded to the NAT function if it matches a configured destination prefix that is part of the routing table. In this case inside and outside routing context must be separated.

- filter based – traffic is forwarded to the NAT function based on any criteria that can be defined inside an IP filter. In this case the inside and outside routing context can be the same.

## 7.6.11 Inverse Mappings

The inverse mapping can be performed with a MIB locally on the node or externally via a script sourced in the router. In both cases, the input parameters are <outside routing instance, outside IP, outside port. The output from the mapping is the subscriber and the inside routing context in which the subscriber resides.

### 7.6.11.1 MIB approach

Reverse mapping information can be obtained using the following command:

```
tools dump nat deterministic-mapping outside-ip <ipv4-address> router <router-
instance> outside-port <[1..65535]>
<ipv4-address> : a.b.c.d
<router-instance> : <router-name> | <service-id>
 router-name - "Base"
 service-id - [1..2147483647]
```

Example:

```
tools dump nat deterministic-mapping outside-ip 10.0.0.2 router "Base" outside-
port 2333
```

Output:

```
Inside router 10 ip 10.0.5.171 -- outside router Base ip 10.0.0.2 port 2333 at Mon Jan
7 10:02:02 PST 2013
```

### 7.6.11.2 Off-line Approach to Obtain Deterministic Mappings

Instead of querying the system directly, there is an option where a Python script can be generated on router and exported to an external node. This Python script contains mapping logic for the configured deterministic NAT in the router. The script can be then queried off-line to obtain mappings in either direction. The external node must have installed Python scripting language with the following modules: getopt, math, os, socket and sys.

The purpose of such off-line approach is to provide fast queries without accessing the router. Exporting the Python script for reverse querying is a manual operation that needs to be repeated every time there is configuration change in deterministic NAT.

The script is exported outside of the box to a remote location (assuming that writing permissions on the external node are correctly set). The remote location is specified with the following command:

```
config service nat deterministic-script location <remote-url>
<remote-url> - [{ftp:// | tftp://}<login>:<pswd>@<remote-locn>/] [<file-path>]
180 chars max
```

The status of the script is shown using the following command:

```
show service nat deterministic-script
=====
Deterministic NAT script data
=====
Location : ftp://10.10.10.10/pub/det-nat-script/det-nat.py
Save needed : yes
Last save result : none
Last save time : N/A
=====
```

Once the script location is specified, the script can be exported to that location with the following command:

```
admin nat save-deterministic-script
```

This needs to be repeated manually every time the configuration affecting deterministic NAT changes.

Once the script is exported (saved), the status of the script is changed as well:

```
show service nat deterministic-script
=====
Deterministic NAT script data
=====
Location : ftp://10.10.10.10/pub/det-nat-script/det-nat.py
Save needed : no
Last save result : success
Last save time : 2013/01/07 10:33:43
=====
```

The script itself can be run to obtain mapping in forward or backward direction:

```
user@external-server:/home/ftp/pub/det-nat-script$./det-nat.py
Usage: det-nat-.py {{DIRECTION PARAMS}} | -h[elp] }
where DIRECTION := { -f[orward] | -b[ackward] }
where PARAMS := { -s[ervice] -a[ddress] -p[ort] }
```

The following displays an example in which source addresses are mapped in the following manner:

```
Router 10, Source-ip: 10.0.5.0-10.0.5.127 to router base, outside-ip 10.0.0.1
Router 10 Source-ip: 10.0.5.128-10.0.5.255 to router base outside-ip 10.0.0.2
```

The forward query for this example will be performed as:

```
user@external-server:/home/ftp/pub/det-nat-script$./det-nat.py -f -s 10 -a 10.0.5.10
```

Output:

```
subscriber has public ip address 10.0.0.1 from service 0 and is using ports [1324 -
1353]
```

The reverse query for this example will be performed as:

```
user@external-server:/home/ftp/pub/det-nat-script$./det-nat.py -b -s 0 -
a 10.0.0.1 -p 3020
```

Output:

```
subscriber has private ip address 10.0.5.66 from service 10
```

## 7.6.12 Logging

Every configuration change concerning the deterministic pool will be logged and the script (if configured for export) will be automatically updated (although not exported). This is needed to keep current track of deterministic mappings. In addition, every time a deterministic port-block is extended by a dynamic block, the dynamic block will be logged just as it is today in non-deterministic NAT. The same logic is followed when the dynamic block is de-allocated.

All static port forwards (including PCP) are also logged.

PCP allocates static port forwards from the wildcard-port range.

## 7.6.13 Deterministic DS-Lite

A subscriber in non-deterministic DS-Lite is defined as v6 prefix, with the prefix length being configured under the DS-Lite NAT node:

```
config>service>vprn>nat>inside>dslite#
subscriber-prefix-length [32..64 | 128] (default is 128)
```

All incoming IPv6 traffic with source IPv6 addresses falling under a unique v6 prefix that is configured with **subscriber-prefix-length** command will be considered as a single subscriber. As a result, all source IPv4 addresses carried within that IPv6 prefix will be mapped to the same outside IPv4 address.

The concept of deterministic DS-Lite is very similar to deterministic LSN44. The DS-lite subscribers (IPv6 addresses/prefixes) are deterministically mapped to outside IPv4 addresses and corresponding deterministic port-blocks.

Although the subscriber in DS-Lite is considered to be either a B4 element (IPv6 address) or the aggregation of B4 elements (IPv6 prefix determined by the **subscriber-prefix-length** command), only the IPv4 source addresses and ports carried inside of the IPv6 tunnel are actually translated.

The prefix statement for deterministic DS-lite remains under the same deterministic CLI node as for the deterministic LSN44. However, the prefix statement parameters for deterministic DS-Lite differ from the one for deterministic LSN44 in the following fashion:

- DS-Lite prefix will be a v6 prefix (instead of v4). The DS-lite subscriber whose traffic is mapped to a particular outside IPv4 address and the deterministic port block is deduced from the prefix statement and the subscriber-prefix-length statement.
- Subscriber-type is set to dslite-lsn-sub.

```
config>service>vprn>nat>inside>deterministic#
 prefix <v6-prefix/length> subscriber-type dslite-lsn-sub nat-policy <policy-
name>
```

#### Example:

```
config>service>vprn>nat>inside>deterministic#
 prefix 2001:db8::/56 subscriber-type dslite-lsn-sub nat-policy det-policy

config>service>vprn>nat>inside>dslite#
 subscriber-prefix-length 60
```

In this case, 16 v6 prefixes (from 2001:db8::/60 to 2001:db8:00:F0::/60) are considered DS-Lite subscribers. The source IPv4 addresses/ports inside of the IPv6 tunnels is mapped into respective deterministic port blocks within an outside IPv4 address according to the map statement.

The map statement contains minor modifications as well. It maps DS-Lite subscribers (IPv6 address or prefix) to corresponding outside IPv4 addresses. Continuing on the previous example:

```
map start 2001:db8::/60 end 2001:db8:00:F0::/60 to 192.168.1.1
```

The prefix length (/60) in this case must be the same as configured subscriber-prefix-length. If we assume that the subscriber-limit in the corresponding pool is set to 8 and outside IP address range is 192.168.1.1 to 192.168.1.10, then the actual mapping is the following:

```
2001:db8::/60 to 2001:db8:00:70::/60 to 192.168.1.1
2001:db8:00:80::/60 to 2001:db8:00:F0::/60 to 192.168.1.2
```

### 7.6.13.1 Hashing Considerations in DS-Lite

The ingress hashing and load distribution between the ISAs in Deterministic DS-Lite is governed by the highest number of configured subscribers per outside IP address in any pool referenced within the given inside routing context.

This limit is configured under:

```
configure
router/service vprn
 nat
 inside
 deterministic
 dslite-max-subscriber-limit <1,2,4,8...32768>
```

While ingress hashing in non-deterministic DS-Lite is governed by the **subscriber-prefix-length** command, in deterministic DS-Lite the ingress hashing is governed by the combination of **dslite-max-subscriber-limit** and **subscriber-prefix-length** commands. This is to ensure that all DS-Lite subscribers that are mapped to a single outside IP address are always sent to the same MS-ISA (on which that outside IPv4 address resides). In essence, as soon as deterministic DS-Lite is enabled, the ingress hashing is performed on an aggregated set of  $n = \log_2(\text{dslite-max-subscriber-limit})$  contiguous subscribers.  $n$  is the number of bits used to represent the largest number of subscribers within an inside routing context, that is mapped to the same outside IP address in any pool referenced from this inside routing context (referenced through the NAT policy).

Once the deterministic DS-lite is enabled (a **prefix** command under the deterministic CLI node is configured), the ingress hashing influenced by the **dslite-max-subscriber-limit** will be in effect for both flavors of DS-Lite (deterministic and non-deterministic) within the inside routing context assuming that both flavors are configured simultaneously.

With introduction of deterministic DS-lite, the configuration of the subscriber-prefix-length must adhere to the following rule:



- The configured value for the subscriber-prefix-length minus the number of bits representing the dslite-max-subscriber-limit value, must be in the range [32..64,128]. Or:

```
subscriber-prefix-length - n = [32..64,128]
where n = log2(dslite-max-subscriber-limit)
[or dslite-max-subscriber-limit = 2^n]
```

This can be clarified by the two following examples:

- dslite-max-subscriber-limit = 64 —  $n=6$  [ $\log_2(64) = 6$ ].

This means that 64 DS-Lite subscribers will be mapped to the same outside IP address. Consequently the prefix length of those subscribers must be reduced by 6 bits for hashing purposes (so that chunks of 64 subscribers are always hashed to the same ISA).

According to our rule, the prefix of those subscribers (subscriber-prefix-length) can be only in the range of [38..64], and no longer in the range [32..64, 128].

- dslite-max-subscriber-limit = 1 >  $n=0$  [ $\log_2(1) = 0$ ]

This means that each DS-lite subscriber will be mapped to its own outside IPv4 address. Consequently there is no need for the aggregation of the subscribers for hashing purposes, since each DS-lite subscriber is mapped to an entire outside IPv4 address (with all ports). Since the subscriber prefix length are not contracted in this case, the prefix length can be configured in the range [32..64, 128].

In other words the largest configured prefix length for the deterministic DS-lite subscriber will be  $32+n$ , where  $n = \log_2(\text{dslite-max-subscriber-limit})$ . The subscriber prefix length can extend up to 64 bits. Beyond 64 bits for the subscriber prefix length, there is only one value allowed: 128. In the case  $n$  must be 0, which means that the mapping between B4 elements (or IPv6 address) and the IPv4 outside addresses is in 1:1 ratio (no sharing of outside IPv4 addresses).

The dependency between the subscriber definition in DS-Lite (based on the subscriber-prefix-length) and the subscriber hashing mechanism on ingress (based on the dslite-max-subscriber-limit value), will influence the order in which deterministic DS-lite is configured.

### 7.6.13.2 Order of Configuration Steps in Deterministic DS-Lite

Configure deterministic DS-Lite in the following order.

- Step 1.** Configure DS-lite subscriber-prefix-length
- Step 2.** Configure dslite-max-subscriber-limit

- Step 3.** Configure deterministic prefix (using a NAT policy)
- Step 4.** Optionally configure map statements under the prefix
- Step 5.** Configure DS-lite AFTR endpoints
- Step 6.** Enable (no shutdown) DS-lite node

Modifying the `dslite-max-subscriber-limit` requires that all `nat`-policies be removed from the inside routing context.

To migrate a non-deterministic DS-Lite configuration to a deterministic DS-Lite configuration, the non-deterministic DS-Lite configuration must be first removed from the system. The following steps should be followed:

- Step 1.** Shutdown DS-lite node
- Step 2.** Remove DS-lite AFTR endpoints
- Step 3.** Remove global NAT policy
- Step 4.** Configure/modify DS-lite subscriber-prefix-length
- Step 5.** Configure `dslite-max-subscriber-limit`
- Step 6.** Reconfigure global NAT policy
- Step 7.** Configure deterministic prefix
- Step 8.** Optionally configure one or more manual map statements under the prefix
- Step 9.** Reconfigure DS-lite AFTR endpoints
- Step 10.** Enable (no shutdown) DS-lite node
- Step 11.** Configuration Restrictions in Deterministic NAT

#### NAT Pool

- To modify **nat pool** parameters, the **nat pool** must be in a shutdown state.
- Shutting down the **nat pool** by configuration (**shutdown** command) is not allowed in case that any NAT policy referencing this pool is active. In other words, all configured prefixes referencing the pool via the NAT policy must be deleted system-wide before the pool can be shut down. Once the pool is enabled again, all prefixes referencing this pool (with the NAT policy) will have to be recreated. For a large number of prefixes, this can be performed with an offline configuration file executed using the **exec** command.

#### NAT Policy

- All NAT policies (deterministic and non-deterministic) in the same inside routing-instance must point to the same `nat-group`.
- A NAT policy (be it a global or in a deterministic prefix) must be configured before one can configure an AFTR endpoint.

## NA Group

- The active-mda-limit in a nat-group cannot be modified as long as a deterministic prefix using that NAT group exists in the configuration (even if that prefix is shutdown). In other words, all deterministic prefixes referencing (with the NAT policy) any pool in that nat-group, must be removed.

## Deterministic Mappings (prefix and map statements)

- Non-deterministic policy must be removed before adding deterministic mappings.
- Modifying, adding or deleting prefix and map statements in deterministic DS-Lite require that the corresponding nat pool is enabled (in **no-shutdown** state).
- Removing an existing prefix statement requires that the prefix node is in a shutdown state.

```
config>service>vprn>nat>inside>deterministic# info

 classic-lsn-max-subscriber-limit 128
prefix 10.0.5.0/24 subscriber-type classic-lsn-sub nat-policy "det"
 map start 10.0.5.0 end 10.0.5.127 to 192.168.0.7
 map start 10.0.5.128 end 10.0.5.255 to 192.168.0.2
 shutdown

config>service>vprn>nat>inside>deterministic# info

 dslite-max-subscriber-limit 128
 prefix 2001:db8:0:1/64 subscriber-type dslite-lsn-sub nat-policy "det"
map start 2001:db8::/64 end 2001:db8::FF:0:0:0/64 to 10.0.0.5
 shutdown

config>service>vprn>nat>inside>ds-lite#
 subscriber-prefix-length 64
 no shutdown
```

Similarly, the map statements can be added or removed only if the prefix node is in a shutdown state.

- There are a few rules governing the configuration of the map statement:
  - If the number of subscribers per configured prefix is greater than the subscriber-limit per outside IP parameter ( $2^n$ ), then the lowest n bits of the map start <inside-ip-address> must be set to 0.
  - If the number of subscribers per configured prefix is equal or less than the subscriber-limit per outside IP parameter ( $2^n$ ), then only one **map** command for this prefix is allowed. In this case there is no restriction on the lower n bits of the map start <inside-ip-address>. The range of the inside IP addresses in such map statement represents the prefix itself.

The *outside-ip-address* in the map statements must be unique amongst all map statements referencing the same pool. In other words, two map statements cannot reference the same <outside-ip-address> in a pool.

#### Configuration Parameters

- The subscriber-limit in deterministic nat pool must be a power of 2.
- The nat inside classic-lsn-max-subscriber-limit must be power of 2 and at least as large as the largest subscriber-limit in any deterministic nat pool referenced by this routing instance. In order to change this parameter, all nat-policies in that inside routing instance must be removed.
- The nat inside ds-lite-max-subscriber-limit must be power of 2 and at least as large as the largest subscriber-limit in any deterministic nat pool referenced by this routing instance. In order to change this parameter, all nat-policies in that inside routing instance must be removed.
- In DS-lite, the [subscriber-prefix-length - log2(dslite-max-subscriber-limit)] value must fall within [32 ..64, 128].
- In Ds-Lite, the subscriber-prefix-length can be only modified if the DS-lite CLI node is in shutdown state and there are no deterministic DS-lite prefixes configured.

#### Miscellaneous

- Deterministic NAT is not supported in combination with 1:1 NAT. Therefore the nat pool cannot be in mode 1:1 when used as deterministic pool. Even if each subscriber is mapped to its own unique outside IP (sub-limit=1, det-port-reservation ports (65535-1023), NAPT (port translation) function is still performed.
- Wildcard port forwards (including PCP) will map to the wildcard port ranges and not the deterministic port range. Consequently logs will be generated for static port forwards using PCP.

## 7.7 Destination Based NAT (DNAT)

Destination NAT (DNAT) in SR OS is supported for LSN44 and L2-Aware NAT. DNAT can be used for traffic steering where the destination IP address of the packet is rewritten. In this fashion traffic can be redirected to an appliance or set of servers that are in control of the operator, without the need for a separate transport service (for example, PBR plus LSP). Applications utilizing traffic steering via DNAT normally require some form of inline traffic processing, such as inline content filtering (parental control, antivirus/spam, firewalling), video caching, and so on.

Once the destination IP address of the packet is translated, traffic is naturally routed based on the destination IP address lookup. DNAT will translate the destination IP address in the packet while leaving the original destination port untranslated.

Similar to source based NAT (Source Network Address and Port Translation (SNAPT)), the SR OS will maintain state of DNAT translations so that the source IP address in the return (downstream) packet is translated back to the original address.

Traffic selection for DNAT processing in MS-ISA is performed via a NAT classifier.

### 7.7.1 Combination of SNAPT and DNAT

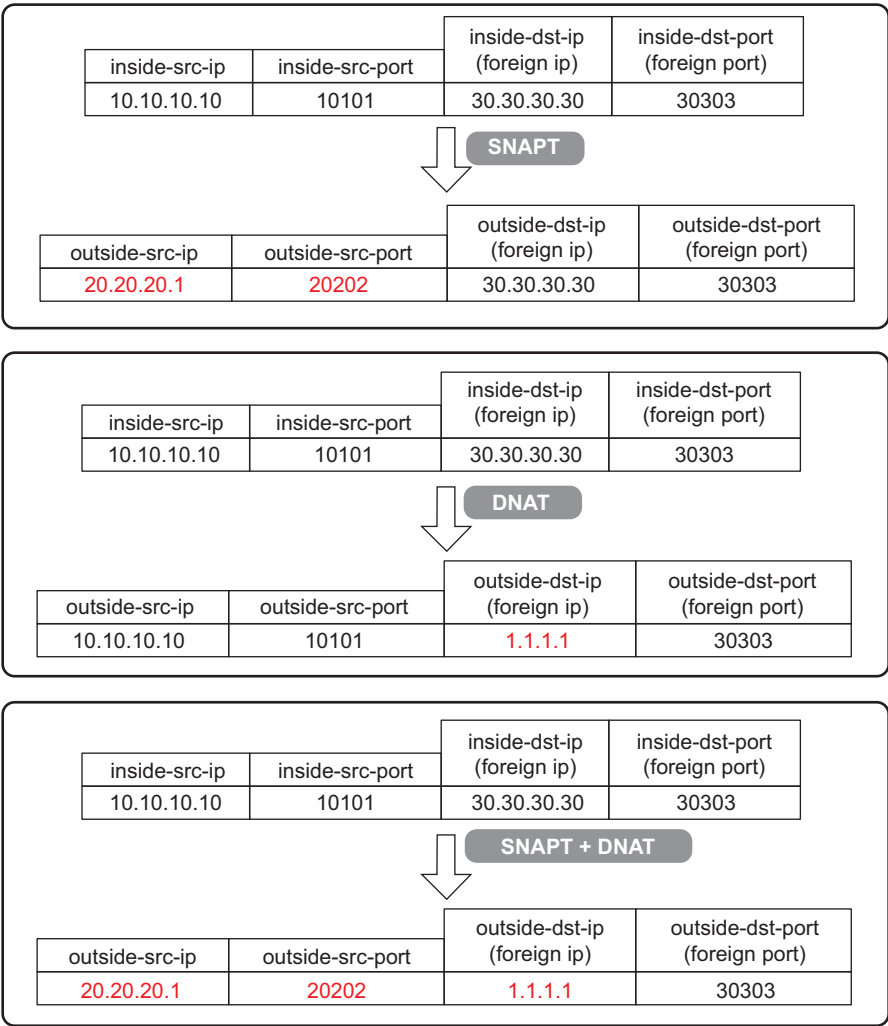
In certain cases SNAPT is required along with DNAT. In other cases only DNAT is required without SNAPT. The following table shows the supported combinations of SNAPT and DNAT in SR OS.

**Table 35** Supported Combinations of SNAPT and DNAT

|          | SNAPT | DNAT-Only | SNAPT + DNAT |
|----------|-------|-----------|--------------|
| LSN44    | X     | X         | X            |
| L2-Aware | X     |           | X            |

The SNAPT/DNAT address translations are shown in [Figure 60](#).

Figure 60 IP Address/Port Translation Modes



0923

7.7.2 Forwarding Model in DNAT

NAT forwarding in SR OS is implemented in two stages:

- Traffic is first directed towards the MS-ISA. This is performed via a routing lookup, via a filter or via a subscriber-management lookup (L2-Aware NAT). DNAT does not introduce any changes to the steering logic responsible for directing traffic from the I/O line card towards the MS-ISA.

- Once traffic reaches the MS-ISA, translation logic is performed. DNAT functionality will incur an additional lookup in the MS-ISA. This lookup is based on the protocol type and the destination port of the packets, as defined in the nat-classifier.

As part of the NAT state maintenance, the SR OS maintains the following fields for each DNATed flow:

<inside host /port, outside IP/port, *foreign IP address*/port, *destination IP address*/port, protocol (TCP,TCP,ICMP)> Note that the inside host in LSN is inside the IP address and in L2-Aware NAT it is the <inside IP address + subscriber-index>. The subscriber index is carried in session-id of the L2TP.

The *foreign IP address* represents the destination IP address in the original packet, while the *destination IP address* represents the DNAT address (translated destination IP address).

### 7.7.3 DNAT Traffic Selection via NAT Classifier

Traffic intended for DNAT processing is selected via a nat classifier. The nat classifier has configurable protocol and destination ports. The inclusion of the classifier in the NAT policy is the trigger for performing DNAT.

The configuration of the nat classifier determines whether:

- a specific traffic defined in the match criteria is DNATed while the rest of the traffic is transparently passed through the nat classifier, OR
- a specific traffic defined in the match criteria is transparently passed through the nat classifier while the rest of the traffic is DNATed.

Classifier cannot drop traffic (no action drop). However, a non-reachable destination IP address in DNAT will cause traffic to be black-holed.

### 7.7.4 Configuring DNAT

DNAT is enabled in the **config>service>nat>nat-policy** context.

```
config>service>nat
nat-policy <nat-policy-name> create
dnat
dnat-only router <router-instance> nat-group <nat-group-id>
nat-classifier <classifier-name>
exit
```

DNAT function is triggered by the presence of the nat classifier (nat-classifier command), referenced in the NAT policy.

DNAT-only option is configured in case where SNAPT is not required. This command is necessary in order to determine the outside routing context and the nat-group when SNAPT is not configured. Pool (relevant to SNAPT) and DNAT-only configuration options within the NAT policy are mutually exclusive.

### 7.7.4.1 DNAT Traffic Selection and Destination IP Address Configuration

DNAT traffic selection is performed via a nat-classifier. Nat-classifier is defined under **config>service>nat** hierarchy and is referenced within the **nat-policy**.

```
configure>service>nat
nat-classifier <name> create
default-DNAT-ip-address <ip-addr>
default-action {DNAT|forward} [ip-addr <ip-address>]
entry 1 create
action {DNAT|forward} [ip-addr <ipv4-address>]
match protocol {tcp | udp}
dst-port range start <port-number> end <port-number>
exit
exit
exit
exit
```

**default-dnat-ip-address** is used in all match criteria that contain DNAT action without specific destination IP address. However, the **default-dnat-ip-address** is ignored in cases where IP address is explicitly configured as part of the action within the match criteria.

**default-action** is applied to all packets that do not satisfy any match criteria.

**forward** (forwarding action) has no effect on the packets and will transparently forward packets through the nat-classifier.

By default, packets that do not match any matching criteria are transparently passed through the classifier.



### 7.7.4.2 Micro-Netting Original Source (Inside) IP Space in DNAT-Only Case

In order to forward upstream and downstream traffic for the same NAT binding to the same MS-ISA, the original source IP address space must be known in advance and consequently hashed on the inside ingress towards the MS-ISAs and micro-netted on the outside.

This will be performed with the following CLI:

```
router | service vprn <id>
nat
inside
classic-lsn-max-subscriber-limit <max>
dnat-only
source-prefix <nat-prefix-list-name>

service nat
nat-prefix-list <name> application dnat-only-subscribers create
prefix <ip-prefix>
```

The **classic-lsn-max-subscriber-limit** parameter was introduced by deterministic NAT and it is reused here. This parameter affects the distribution of the traffic across multiple MS-ISA in the upstream direction traffic. Hashing mechanism based on source IPv4 addresses/prefixes is used to distribute incoming traffic on the inside (private side) across the MS-ISAs. Hashing based on the entire IPv4 address will produce the most granular traffic distribution, while hashing based on the IPv4 prefix (determined by prefix length) will produce less granular hashing. For further details about this command, consult the CLI command description.

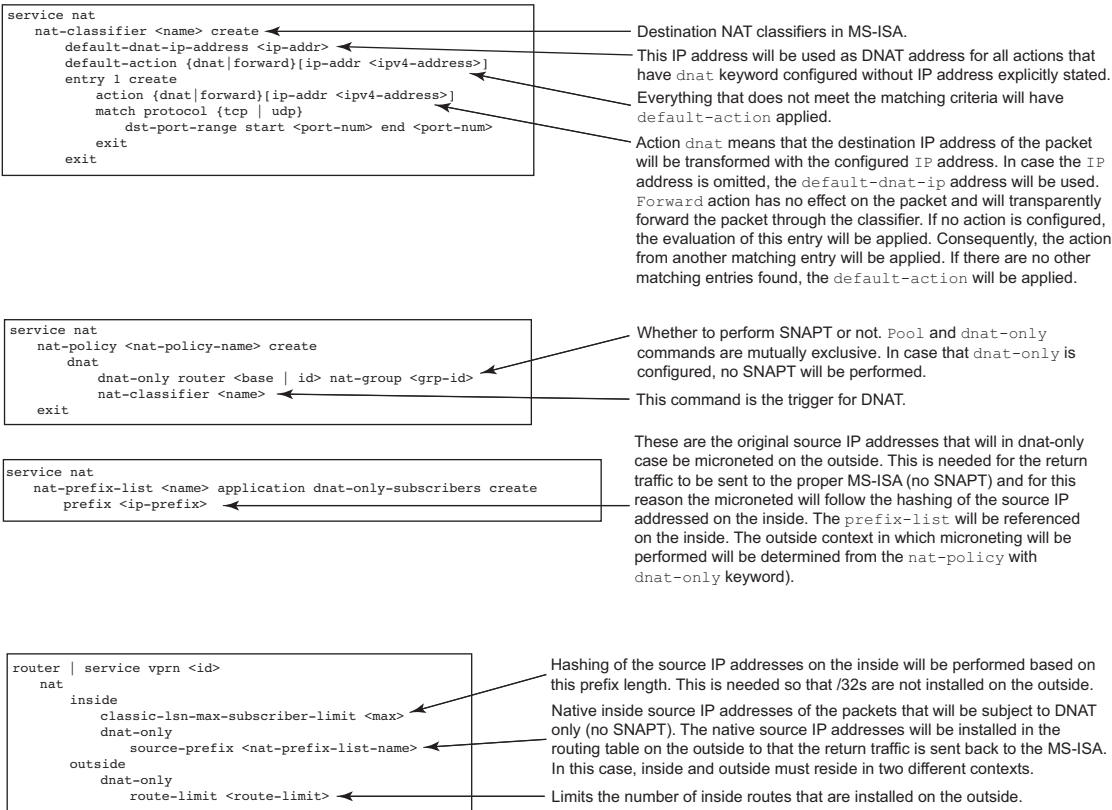
The source IP prefix is defined in the nat-prefix-list and then applied under the DNAT-only node in the inside routing context. This will instruct the SR OS to create micro-nets in the outside routing context. The number of routes installed in this fashion is limited by the following configuration:

```
router | service vprn <id>
nat
outside
dnat-only
route-limit <route-limit>
```

The configurable range is 1-128K with the default value of 32K.

DNAT provisioning concept is shown in [Figure 61](#).

Figure 61 DNAT Provisioning Model



0924

## 7.8 LSN – Multiple NAT Policies per Inside Routing Context

### 7.8.1 Restrictions

The following restrictions apply to multiple NAT policies per inside routing context

- There is no support for L2-Aware NAT.
- DS-Lite and NAT64 diversion to NAT is supported only through IPv6 filters.
- A maximum of 8 different NAT policies per inside routing context are supported. For routing based NAT diversion, this limit is enforced during the configuration of the NAT policies within the inside routing context. In case of a filter-based NAT diversion, the filter instantiation will fail if the number of different nat-policies per inside routing context exceeds 8.
- The default NAT policy is counted towards this limit (8).

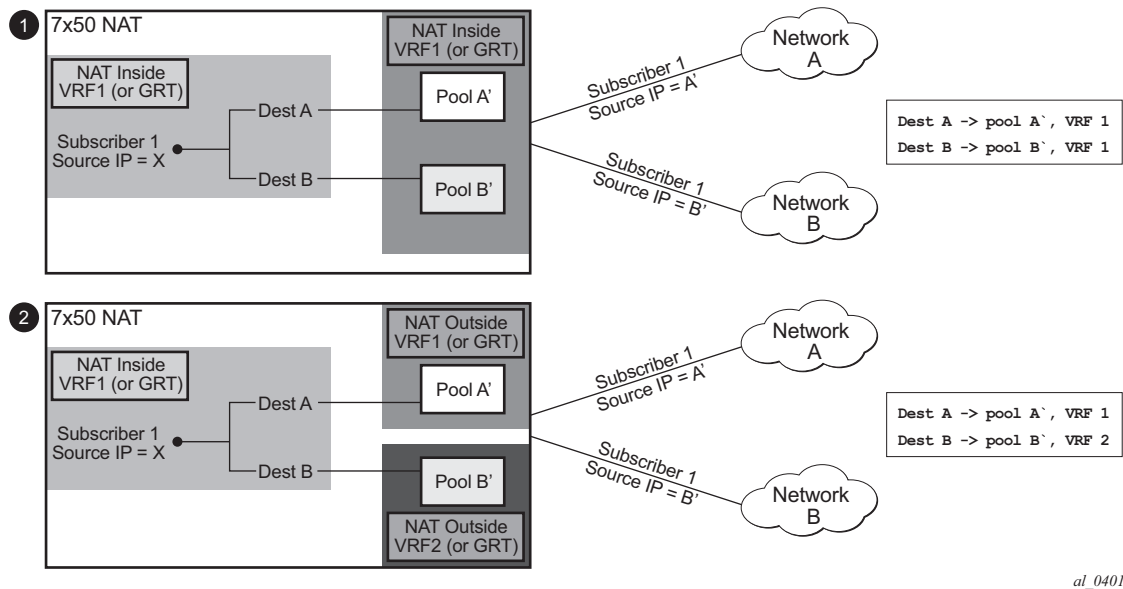
### 7.8.2 Multiple NAT Policies Per Inside Routing Context

The selection of the NAT pool and the outside routing context is performed through the NAT policy. Multiple NAT policies can be used within an inside routing context. This feature effectively allows selective mapping of the incoming traffic within an inside routing context to different NAT pools (with different mapping properties, such as port-block size, subscriber-limit per pool, address-range, port-forwarding-range, deterministic vs non-deterministic behavior, port-block watermarks, and so on) and to different outside routing contexts. NAT policies can be configured:

- via filters as part of the **action nat** command.
- via routing with the **destination-prefix** command within the inside routing context

The concept of the NAT pool selection mechanism based on the destination of the traffic via routing is shown in [Figure 62](#).

Figure 62 Pool Selection Based on Traffic Destination

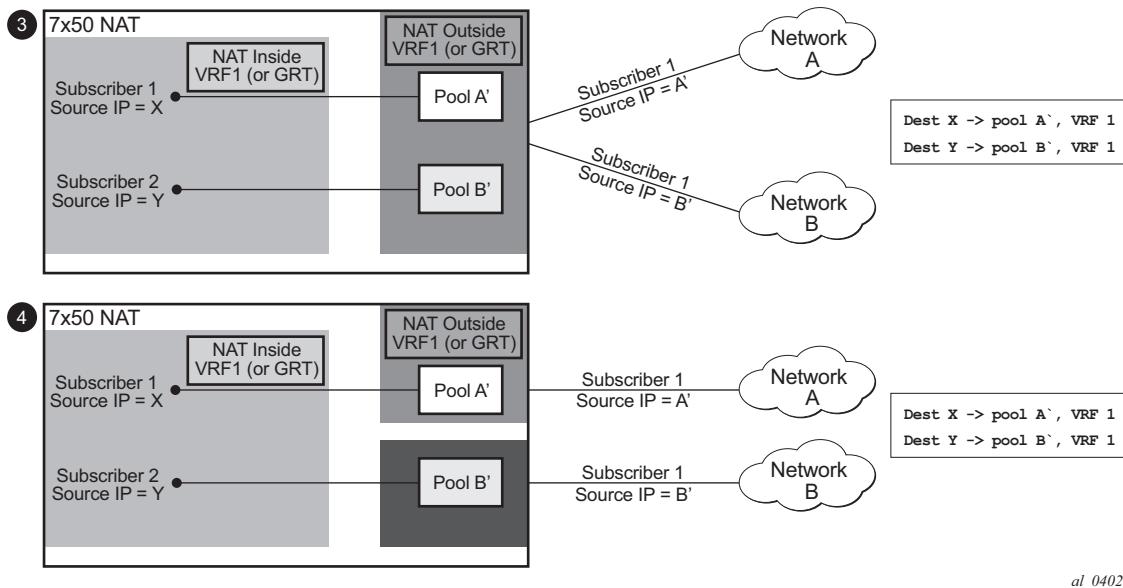


al\_0401

Diversion of the traffic to NAT based on the source of the traffic is shown in [Figure 63](#).

Only filter-based diversion solution is supported for this case. The filter-based solution can be extended to a 5 tuple matching criteria.

Figure 63 NAT Pool Selection Based on the Inside Source IP Address



al\_0402

The following considerations must be taken into account when deploying multiple NAT policies per inside routing context:

- The inside IP address can be mapped into multiple outside IP addresses based on the traffic destination. The relationship between the inside IP and the outside IP is 1:N.
- In case where the source IP address is selected as a matching criteria for a NAT policy (or pool) selection, the inside IP address will always stay mapped to the same outside IP address (relationship between the inside IP and outside IP address is, in this case, 1:1)
- Static Port Forwards (SPF) — Each SPF can be created only in one pool. This means that the pool (or NAT policy) must be an input parameter for SPF creation.

### 7.8.3 Routing Approach for NAT Diversion

The routing approach relies on upstream traffic being directed (or diverted) to the NAT function based on the **destination-prefix** command in the **configure>service>vprn/router>nat>inside** CLI context. In other words, the upstream traffic will be NATed only if it matches a preconfigured destination IP prefix. The **destination-prefix** command creates a static route in the routing table of the inside routing context. This static route will divert all traffic with the destination IP address that matches the created entry, towards the MS-ISA. The NAT function itself will be performed once the traffic is in the proper context in the MS-ISA.

The CLI for multiple NAT policies per inside routing context with routing based diversion to NAT is the following:

```
service vprn/router
 nat
 inside
 destination-prefix <ip-prefix/length> nat-policy <policy-name>]
 :
 :
```

or, for example:

```
service vprn/router
 nat
 inside
 destination-prefix 10.20.10.0/24 nat-policy policy-1
 destination-prefix 10.30.30.0/24 nat-policy policy-1
 destination-prefix 10.40.40.0/24 nat-policy policy-2
```

Different destination prefixes can reference a single NAT policy (policy-1 in this case).

In case that the destination-policy does not directly reference the NAT policy, the default NAT policy will be used. The default NAT policy is configured directly in the **vprn/router>nat>inside** context.

Once that **destination-prefix** command referencing the NAT policy is configured, an entry in the routing table will be created that will direct the traffic to the MS-ISA.

## 7.8.4 Filter-Based Approach

A filter-based approach will divert traffic to NAT based on the IP matching criteria shown in the CLI below.

```
*A:right-a21>config>filter>ip-filter>entry# match
- match [protocol <protocol-id>]
- no match

<protocol-id> : protocol numbers - [0..255] (Decimal,
 Hexadecimal, or Binary representation).
 Supported IANA IP protocol names -
 none|crtp|crudp|egp|eigrp|encap|ether-ip|
 gre|icmp|idrp|igmp|igp|ip|ipv6|ipv6-frag|ipv6-icmp|
 ipv6-no-nxt|ipv6-opts|ipv6-route|isis|iso-ip|l2tp|
 ospf-igp|pim|pnni|ptp|rdp|rsvp|sctp|stp|tcp|udp|vrrp
 * - udp/tcp wildcard

[no] dst-ip - Configure dest. ip match condition
[no] dst-port - Configure destination port match condition
[no] port - Configure port match condition
[no] src-ip - Configure source ip match condition
[no] src-port - Configure source port match condition
```

The CLI for the filter-based diversion in conjunction with multiple NAT policies is shown below:

```
filter
 entry
 action nat [nat-policy <nat-policy-name>]
```

The association with the NAT policy is made once the filter is applied to the SAP.

## 7.8.5 Multiple NAT Policies with DS-Lite and NAT64

DS-Lite and NAT64 diversion to NAT with multiple nat-policies is supported only through IPv6 filters:

```
configure
```

```
filter
 ipv6-filter
 entry <entry-id> [create]
 action nat nat-type <nat-type> [nat-policy <nat-policy-name>]
 exit
 exit
exit
exit
exit
```

Where the **nat-type** parameter can be either **dslite** or **NAT64**.

The DS-Lite AFTR address and NAT64 destination prefix configuration under the corresponding (DS-Lite or NAT64) **router/vprn>nat>inside** context is mandatory. This is even when only filters are desired for traffic diversion to NAT.

For example, every AFTR address and NAT64 prefix that is configured as a match criteria in the filter, must also be duplicated in the **router/vprn>nat>inside** context. However, the opposite is not required.

IPv6 traffic with the destination address outside of the AFTR/NAT64 address/prefix will follow normal IPv6 routing path within the 7750 SR.

## 7.8.6 Default NAT Policy

The default **nat-policy** is always mandatory and must be configured under the **router/vprn>nat>inside** context. This default NAT policy can reference any configured pool in the desired ISA group. The pool referenced in the default NAT policy can be then overridden by the NAT policy associated with the destination-prefix in LSN44 or by the **NAT policy** referenced in the ipv4/ipv6-filter used for NAT diversion in LSN44/DS-Lite/NAT64.

The NAT CLI nodes will fail to activate (be brought out of the **no shutdown** state), unless a valid NAT policy is referenced in the **router/vprn>nat>inside** context.

## 7.8.7 Scaling Considerations

Each subscriber using multiple policies is counted as one subscriber for the **inside** resources scaling limits (such as the number of subscribers per MS-ISA), and counted as one subscriber per (subscriber and policy combination) for the **outside** limits (**subscriber-limit** subscribers per IP; **port-reservation** port/block reservations per subscriber).

## 7.8.8 Multiple NAT Policies and SPF Configuration Considerations

Any given Static Port Forward (SPF) can be created only in one pool. This pool, which is referenced through the NAT policy, has to be specified at the SPF creation time, either explicitly through the configuration request or implicitly via defaults.

Explicit request will be submitted either via SAM or via CLI:

```
tools perform nat port-forwarding-action lsn
- lsn create router <router-instance> [b4 <ipv6-address>] [aftr <ipv6-
address>] ip <ip-
address> protocol {tcp|udp} [port <port>] lifetime <lifetime> [outside-ip <ipv4-
address>] [outside-port <port>] [nat-policy <nat-policy-name>]
```

In the absence of the NAT policy referenced in the SPF creation request, the default **nat-policy** command under the **vprn/router>nat>inside** context will be used.

The consequence of this is that the operator must know the NAT policy in which the SPF is to be created. The SPF cannot be created via PCP outside of the pool referenced by the default NAT policy, since PCP does not provide means to communicate NAT policy name in the SPF creation request.

The static port forward creation and their use by the subscriber types must follow these rules:

- Default NAT policy — Any subscriber type can use an SPF created in the pool referenced by the default NAT policy
- Deterministic LSN44 NAT policy — Only deterministic LSN44 subscribers matching the configured prefix can use the SPF created in the pool referenced by the deterministic LSN44 prefix NAT policy
- Deterministic DS-Lite NAT policy — Only deterministic DS-Lite subscribers matching the configured prefix can use the SPF created in the pool referenced by the deterministic DS-Lite prefix NAT policy
- LSN44 filter based NAT policy — Only LSN44 subscribers matching the configured filter entry can use the SPF created in the pool referenced by the non-deterministic LSN44 NAT policy within the filter
- DS-Lite filter based NAT policy — Only DS-Lite subscribers matching the configured filter entry can use the SPF created in the pool referenced by the DS-Lite NAT policy within the filter
- NAT64 filter based NAT policy — Only NAT64 subscribers matching the configured filter entry can use the SPF created in the pool referenced by the NAT64 NAT policy within the filter



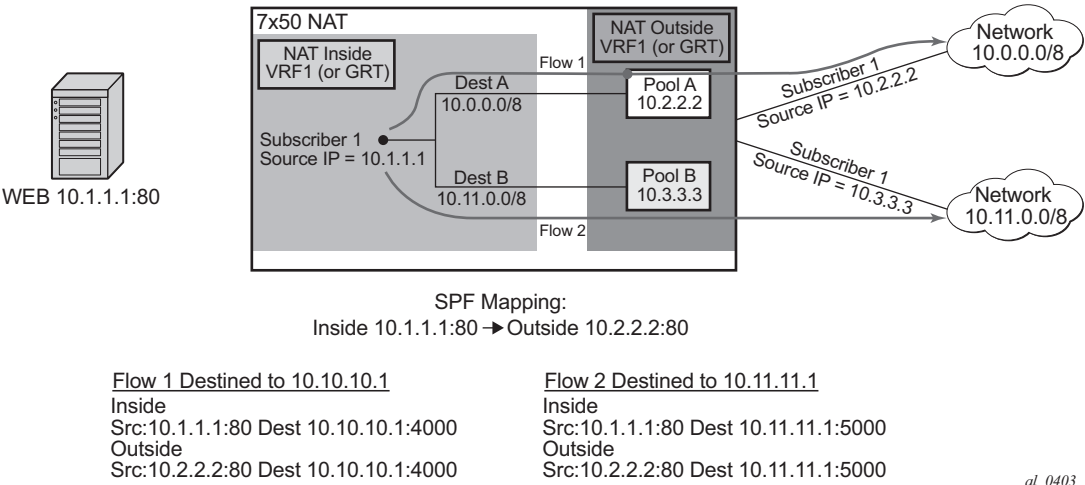
When the last relevant policy for a certain subscriber type is removed from the virtual router, the associated port forwards are automatically deleted.

7.8.8.1 Multiple NAT Policies and Forwarding Considerations

Figure 64 and Figure 65 describe certain scenarios that are more theoretical and are less likely to occur in reality. However, they are described here for the purpose of completeness.

Figure 64 represents the case where traffic from the WEB server 10.1.1.1 is initiated toward the destined network 10.11.0.0/8. Such traffic will end up translated in the Pool B and forwarded to the 10.11.0.0/8 network even though the static port forward has been created in Pool A. In this case the NAT policy rule (dest 10.11.0.0/8 pool B) will determine the pool selection in the upstream direction (even though the SPF for the WEB server already exists in the Pool A).

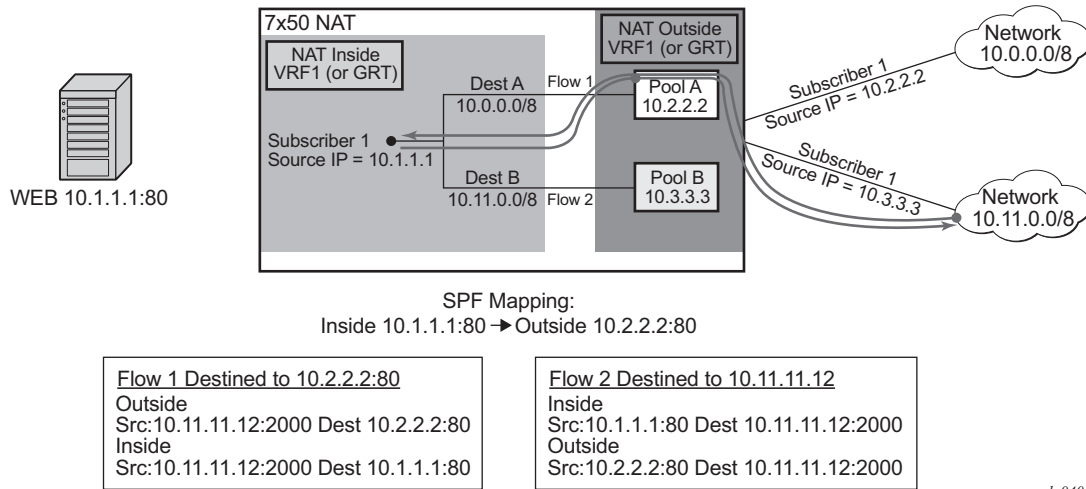
Figure 64      SPF With Multiple NAT Policies



The next example in Figure 65 shows a case where the Flow 1 is initiated from the outside. Since the partial mapping matching this flow already exist (created by SPF) and there is no more specific match (FQF) present, the downstream traffic will be mapped according to the SPF (through Pool A to the Web server). At the same time, a more specific entry (FQF) will be created (initiated by the very same outside traffic). This FQF will now determine the forwarding path for all traffic originating from the inside that is matching this flow. This means that the Flow 2 (reverse of the Flow 1) will not be mapped to an IP address from the pool B (as the policy dictates) but instead to the Pool A which has a more specific match.

A more specific match would be in this case fully qualified flows (FQF) that contains information about the foreign host: <host, inside IP/port, outside IP/port, foreign IP address/port, protocol>.

**Figure 65 Bypassing NAT Policy Rule**



## 7.8.9 Logging

When multiple NAT policies per inside routing context are deployed, a new *policy-id* parameter is added to certain syslog messages. The format of the policy-id is:

```
plcy-id XX
```

where XX is an arbitrary unique number per inside routing context assigned by the router. This number, represents the corresponding NAT policy. Since the maximum number of NAT policies in the inside routing context is 8, the *policy-id* value is also a numerical value in the range 1 — 8.

Introduction of the *policy-id* in logs is necessary due to the bulk-operations associated with multiple NAT policies per inside routing context. A bulk operation, for example, represents the removal of the *nat-policy* from the configuration, shutting down the NAT pool, or removing an IP address range from the pool. Removing a NAT accounting policy in case of RADIUS NAT logging will not trigger a summarization log since an acct-off message is sent. Such operations have a tendency to be heavy on NAT logging since they affect a large number of NAT subscribers at once. Summarization logs are introduced to prevent excessive logging during bulk operations. For example, the NAT policy deletion can be logged with a single

(summarized) entry containing the policy-id of the NAT policy that was removed and the inside *svc-id*. Since all logs contain the policy-id, a single summarization *free* log can be compared to all *map2* logs containing the same policy-id to determine for which subscribers the NAT mappings have ceased. Map and Free logs are generated when the port-block for the subscribers are allocated and de-allocated.

Summarization log is always generated on the CPM, regardless of whether the RADIUS logging is enabled or not. A summarization log simply cannot be generated via RADIUS logging since the RADIUS accounting message streams (start/interim-updates/stop) are always generated per subscriber. In other words, for RADIUS logging, the summarization log would need to be sent to each subscriber, which defeats the purpose of the summarization logs.

A summarization log on the CPM is generated:

- When the NAT policy is removed — With a single NAT policy per inside routing context, a summarization log is generated with only one field: inside *svc-id* (**vprn** or **base**). This is sufficient since there is only one NAT policy per inside routing context. To determine subscribers for which NAT mappings are terminated, the operator should search all most recent map logs matching the service-id from the summarization log.

With multiple NAT policies per inside routing context, the inside *svc-id* **and** the *policy-id* are included in the summarization log (no outside IPs, outside *svc-id*, port-block or source IP).

A log search based on the *policy-id* and inside *svc-id* should reveal all subscribers whose mappings were affected by the NAT policy removal.

- When the pool is shutdown — The router will send a summarization log that includes the outside *svc-id* and all IP address ranges configured in the pool. No other parameters are included in the summarization log.

A log search based on the outside IP address and outside *svc-id* should reveal all subscribers for which the NAT mappings have ceased.

- When an IP address-range is removed from the pool. The router will send a summarization log that includes the outside *svc-id* and the IP address range that has been removed. No other parameters are included in the summarization log.

A log search based on the outside IP addresses in the range and the outside *svc id* should reveal all subscribers for which the NAT mappings have ceased.

- When the last AFTR address is removed.
- When DS-Lite/NAT64 node is shutdown.

- When deterministic NAT prefixes are created or removed.

Summarization logs in RADIUS logging:

The summarization log for bulk operation while RADIUS logging is generated only in the CPM (syslog). This means that for bulk operations with RADIUS logging, the operator will have to rely on RADIUS logging as well as on the CPM logging.

An open log sequence in RADIUS, for example a map for the <inside IP 1, outside IP 1,port-block 1> followed at some later time with a map for <inside IP 2, outside IP 1, port-block 1>, is an indication that the free log for <inside IP 1, outside IP 1,port-block 1> is missing. This means that either the free log for <inside IP 1, outside IP 1,port-block 1> was lost or that a policy, pool, and address-range was removed from the configuration. In the latter case, the operator should look in the CPM log for the summarization message.

The summarization logs are enabled via the event control 2021 `tmnxNatLsnSubBlksFree` which is by default suppressed. The event control 2021 is also used to report when all blocks for the subscriber are freed.

## 7.9 L2-Aware NAT Destination-Based Multiple NAT Policies

Multiple NAT policies for a L2-Aware subscriber can be selected based on the destination IP address of the packet. This allows the operator to assign different NAT pools and outside routing contexts based on the traffic destinations.

The mapping between the destination IP prefix and the NAT policy is defined in a nat-prefix-list. This nat-prefix-list is applied to the L2-Aware subscriber via a sub-profile. Once the subscriber traffic arrives to the MS-ISA where NAT is performed, an additional lookup based on the destination IP address of the packet will be executed to select the specific NAT policy (and consequently the outside NAT pool). Failure to find the specific NAT policy based on the destination IP address lookup will result in selection of the default NAT policy referenced in the sub-profile.

CLI example:

```

echo "Service Configuration"
#-----
service
 nat
 nat-policy "l2aw nat policy" create
 pool "l2aw-nat-pool" router 1
 exit
 nat-policy "another-l2aw-nat-policy" create
 pool "another-l2aw-nat-pool" router 2
 exit
 nat-policy "default-nat-policy" create
 pool "default-nat-pool" router Base
 exit

 nat-prefix-list "prefixlist1" application l2-aware-dest-to-policy create
 prefix 192.168.0.0/30 nat-policy "l2aw-nat-pol"
 prefix 192.168.0.64/30 nat-policy "l2aw-nat-pol"
 prefix 192.168.0.128/30 nat-policy "l2aw-nat-pol"
 prefix 192.168.1.0/30 nat-policy "another-l2aw-nat-pol"
 prefix 192.168.1.64/30 nat-policy "another-l2aw-nat-pol"
 prefix 192.168.1.128/30 nat-policy "another-l2aw-nat-pol"
 exit
exit
#-----
echo "Subscriber-mgmt Configuration"
#-----
subscriber-mgmt
 sub-profile "sub_profile" create
 nat-policy "def-nat-policy"
 nat-prefix-list "prefixlist1"
 exit
```

As displayed in the example, multiple IP prefixes can be mapped to the same NAT policy.

The NAT prefix list cannot reference the default NAT policy. The default NAT policy is the one that is referenced directly under the sub-profile.

## 7.9.1 Logging

In L2-Aware NAT with multiple nat-policies, the NAT resources are allocated in each pool associated with the subscriber. This NAT resource allocation is performed at the time when the ESM subscriber is instantiated. Each NAT resource allocation will be followed by log generation.

For example, if RADIUS logging is enabled, one Alc-NAT-Port-Range VSA per NAT policy will be included in the acct START/STOP message.

[Alc-Nat-Port-Range = "192.168.20.1 1024-1055 router base **nat-pol-1**"

Alc-Nat-Port-Range = "193.168.20.1 1024-1055 router base **nat-pol-2**".

Alc-Nat-Port-Range = "194.168.20.1 1024-1055 router base" **nat-pol-3.**]

### 7.9.1.1 RADIUS Logging and Nat-Policy Change via CoA

Nat-policy change for L2-Aware NAT is supported via sub-profile change triggered in CoA. However, change of sub-profile alone via CoA will not trigger generation of new Radius accounting message and thus NAT events related to NAT policy change will not be promptly logged. For this reason, each CoA initiating the sub-profile change in NAT environment should:

- Change the sla-profile **OR**
- Include the Alc-Trigger-Acct-Interim VSA in the CoA messages.

Note that the sla-profile will have to be changed and not just refreshed. In other words replacing the existing sla-profile with the same one will not trigger a new accounting message.

Both of the above events will trigger an accounting update at the time when CoA is processed. This will keep NAT logging current.

The information about NAT resources for logging purposes is conveyed in the following RADIUS attributes:

- Alc-Nat-Port-Range-Freed VSA 10361036 → NAT resources released due to CoA.
- Alc-Nat-Port-Range VSA → NAT resources in use. These can be the existing NAT resources which were not affected by CoA or they can be new NAT resource allocated due to CoA.

NAT logging behavior due to CoA will depend on the deployed accounting mode of operation. This is described in Table 1. Note that **interim-update** keyword must be configured for host/session accounting in order for Interim-Update messages to be triggered:

```
configure
 subscriber-mgmt
 radius-accounting-policy <name>
 session-accounting interim-update
configure
 subscriber-mgmt
 radius-accounting-policy <name>
 host-accounting interim-update
```

Table Legend:

AATR - Alc-Acct-Triggered-Reason VSA → This VSA is optionally carried in Interim-Update messages that are triggered by CoA.

ATAI - Alc-Trigger-Acct-Interim VSA → this VSA can be carried in CoA to trigger Interim-Update message. The string carried in this VSA is reflected in the triggered Interim-Update message.

I-U – Interim-Update Message

**Table 36 NAT-Policy Change and CoA in L2Aware NAT**

|                                             | Host or session accounting                                                                            | Queue-instance accounting                                                                             | Comments                                |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------|
| <b>CoA</b><br>Sub-prof change +<br>ATAI VSA | Single I-U with:<br>— released NAT info<br>— unchanged NAT info<br>— new NAT info<br>— AATR<br>— ATAI | Single I-U with:<br>— released NAT info<br>— unchanged NAT info<br>— new NAT info<br>— AATR<br>— ATAI | Single I-U message is triggered by CoA. |

**Table 36 NAT-Policy Change and CoA in L2Aware NAT (Continued)**

|                                                                       | Host or session accounting                                                                                                                                  | Queue-instance accounting                                                                                                                   | Comments                                                                                                                                                         |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CoA</b><br>Sub-profile change<br>+<br>Sla-profile change           | First I-U:<br>— released NAT info<br>— unchanged NAT info<br>— new NAT info<br><br>Second I-U:<br>— unchanged NAT info<br>— new NAT info                    | Acct Stop:<br>— released NAT info<br>— unchanged NAT info<br>— new NAT info<br><br>Acct Start:<br>— unchanged NAT info<br>— new NAT info    | Two accounting messages are triggered in succession.                                                                                                             |
| <b>CoA</b><br>Sub-profile change                                      | —                                                                                                                                                           | —                                                                                                                                           | No accounting messages are triggered by CoA. The next regular I-U messages will contain:<br>— old (released) NAT info<br>— unchanged NAT info<br>— new NAT info. |
| <b>CoA</b><br>Sub-profile change+<br>Sla-profile-change +<br>ATAI VSA | First I-U:<br>— released NAT info<br>— unchanged NAT info<br>— new NAT info<br><br>Second I-U<br>— unchanged NAT info<br>— new NAT info<br>— AATR<br>— ATAI | Acct Stop:<br>— re-released NAT info<br>— unchanged NAT info<br>— new NAT info<br><br>Acct Start:<br>— unchanged NAT info<br>— new NAT info | Two accounting messages are triggered in succession.                                                                                                             |

For example, the second CoA row describes the outcome triggered by CoA carrying new sub and sla profiles. In host/session accounting mode this will create two Interim-Update messages. The first Interim-Messages will carry information about:

- the released NAT resources at the time when CoA is activated.
- existing NAT resources that are not affected by CoA.
- new NAT resources allocated at the time when CoA is activated.

The second Interim-Update message will carry information about the NAT resources that are in use (existing and new) once CoA is activated.



From this, the operator can infer which NAT resources are released by CoA and which NAT resources continue to be in use once CoA is activated.

### 7.9.1.2 Delay Between the NAT Resource Allocation and Logging During CoA

Nat-policy change induced by CoA will trigger immediate log generation (for example acct STOP or INTERIM-UPDATE) indicating that the nat resources have been released. However, the NAT resources (outside IP addresses and port-blocks) in SR OS will not be released for another five seconds. This delay is needed to facilitate proper termination of traffic flow between the NAT user and the outside server during the NAT policy transition. A typical example of this scenario is the following:

- HTTP traffic is redirected to a WEB portal for authentication. Only when the user is authenticated, access to the Internet will be granted along with a new NAT policy that will provide more NAT resources (larger port-ranges, and so on).
- Once the user is authenticated, CoA will be used to change the user forwarding properties (HTTP-redirect is removed and the NAT policy is changed). However, CoA must be sent before the authentication acknowledgment (ACK) message is sent, otherwise the next new HTTP request would be redirected again.
- Authentication acknowledgment is sent to the NAT user following the CoA which removed the HTTP redirect and instantiated a new NAT policy. Since the original communication between the WEB portal and the NAT user was relying on the original NAT policy, the NAT resources associated with the original NAT policy must be preserved to terminate this communication gracefully. Hence the delay of five seconds before the NAT resources are freed.

Stale port forwards will similarly to other stale dynamic mappings be released after five seconds. Note that static port forwards will be kept on the CPM.

New CoAs related to NAT will be rejected (NAK'd) in case that the previous change is in progress (during the 5seconds interval until the stale mappings are purged).

## 7.9.2 Static Port Forwards

Unless the specific NAT policy is provided during Static Port Forward (SPF) creation (SPF creation command), the port forward will be created in the pool referenced in the default NAT policy.

Nat-policy can be part of the command used to modify or delete SPF. If the NAT policy is not provided, then the behavior will be:

- if there is only one match, the port forward will be modified or deleted.
- if there is more than one match, modify or delete port forward must specify a NAT policy. Otherwise, the modify or delete action will fail.

A match is considered when at least these parameters from the modify or delete command are matched (mandatory parameters in the **spf** command):

- subscriber identification string
- inside IP address
- inside port
- protocol

For a Layer 2-Aware NAT, an alternative AAA interface can be used to specify SPF. An alternative AAA interface and CLI-based port forwards are mutually exclusive. Refer to the 7750 SR and VSR RADIUS Attributes Reference Guide for more details.

### 7.9.3 L2-Aware Ping

Similar to the non-L2-Aware **ping** command, understanding how the ICMP Echo Request packets are sourced in L2-Aware ping is crucial for the proper execution of this command and the interpretation of its results. The ICMP Echo Reply packets must be able to reach the source IP address that was used in ICMP Echo Request packets on the SR OS node on which the L2-Aware **ping** command was executed. See [Figure 66](#).

The return packet (the ICMP Echo reply sent by the targeted host) is subject to L2-Aware NAT routing executed in the MS-ISA. The L2-Aware NAT routing process looks at the destination IP address of the upstream packet and then directs the packet to the correct outside routing context. The result of this lookup is a NAT policy that references the NAT pool in an outside routing context. This outside routing context must be the same as the one from which the L2-Aware **ping** command was sourced. Otherwise, the L2-Aware **ping** command fails.

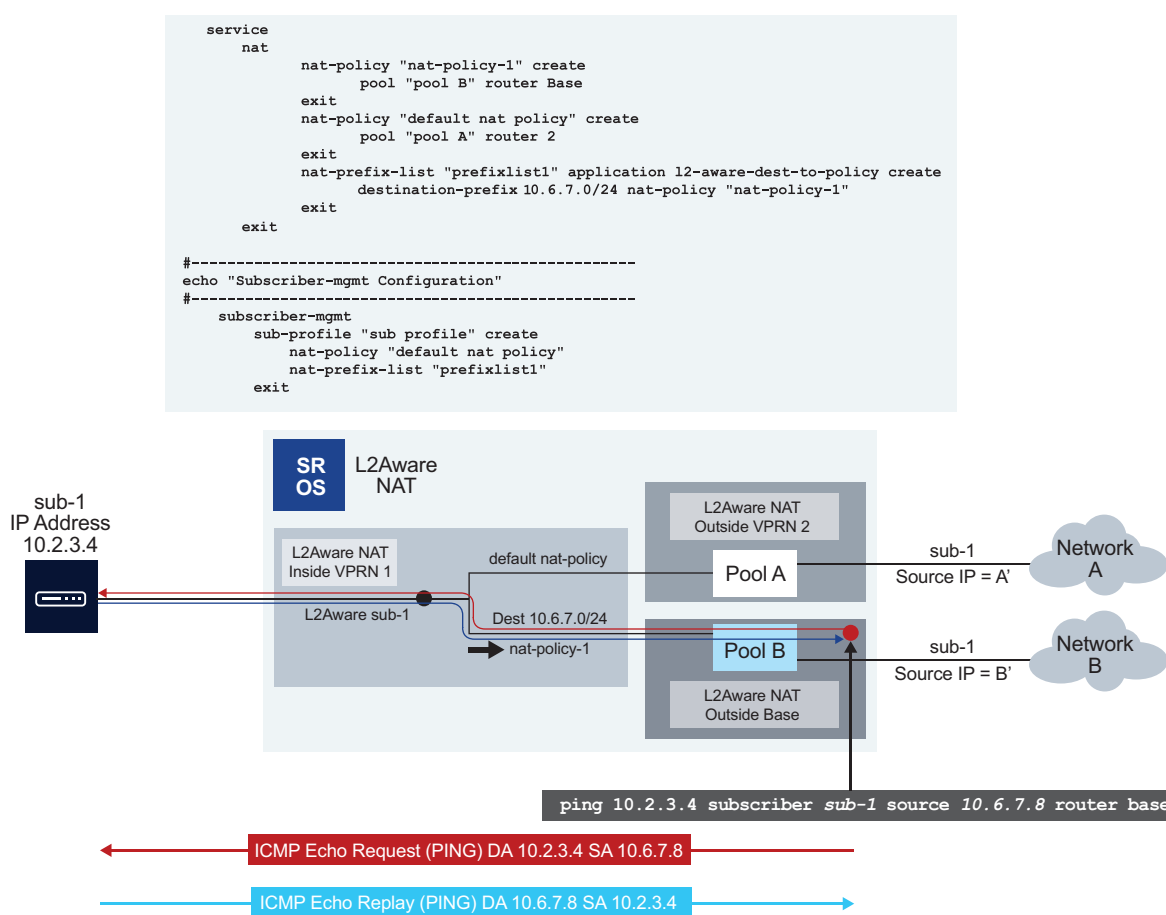
The L2-Aware **ping** command can be run in two modes:

- Basic mode (**ping ip-address subscriber subscriber-id**) in which the *subscriber-id* is a required field in order to differentiate subscriber hosts that assigned the same IP address (although each host has its own instantiation of this IP address).
- Extended mode where additional parameters can be selected, the two most important being the source IP address (source) and the routing context (router):  
**ping ip-address subscriber subscriber-id source ip-address router router-id**

Figure 66 shows the traffic flow for an L2-Aware **ping** command targeting the subscriber's IP address 10.2.3.4, sourced from the Base routing context using an arbitrary source IP address of 10.6.7.8 (it is not required that this IP address belong to the L2-Aware ping originating node).

When the host 10.2.3.4 replies, the incoming packets with the destination IP address of 10.6.7.8 are matched against the destination-prefix 10.6.7.0/24 referencing the nat-policy-1. nat-policy-1 contains the Pool B which resides in the Base routing context. Hence, the loop is closed and the execution of the L2-Aware **ping** command is successful.

**Figure 66**      **L2-Aware Ping**



SW0097

L2-Aware ping is always sourced from the outside routing context, never from the inside routing context. If the router is not specifically configured as an option in the L2-Aware **ping** command, the Base routing context is selected by default. If that the Base routing context is not one of the outside routing contexts for the subscriber, the L2-Aware **ping** command execution fails with the following error message:

“MINOR: OAM #2160 router ID is not an outside router for this subscriber.”

## **7.9.4 UPnP**

UPnP will use the default NAT policy.

## 7.10 NAT and CoA

RADIUS Change of Authorization (CoA) can be used in subscriber management (ESM) to modify the NAT behavior of the subscriber. This can be performed by:

- Replacing a NAT policy in a subscriber profile for the L2-Aware NAT subscriber.
- Replacing or removing a NAT policy within the IP filter for the ESM subscriber using LSN44, DS-Lite or NAT64.
- Modifying DNAT parameters directly via CoA for the L2-Aware subscriber.

### 7.10.1 CoA and NAT Policies

The behavior for NAT policy changes via CoA for LSN and L2-Aware NAT is summarized in [Table 37](#).

**Table 37 NAT Policy Changes via CoA**

| Action                     | Outcome                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                      | Remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | L2-Aware                                                                                                                                                                                                                                                                                                                                                                      | LSN                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CoA - replacing NAT policy | <p>Stale flows using the old NAT policy are cleared after 5 seconds.<br/>New flows immediately start using a new NAT policy.</p> <p><b>Restrictions:</b></p> <ul style="list-style-type: none"> <li>• Allowed only when the previous change is completed (need to wait for a 5 second interval during which the stale mappings caused by previous CoA are purged).</li> </ul> | <p>Stale flows using the old NAT policy continue to exist and are used for traffic forwarding until they are naturally timed-out or TCP- terminated.<br/>The exception to this is when the reference to the NAT policy in the filter was the last one for the inside VRF. In this scenario, the flows from the removed NAT policy are cleared immediately.<br/>New flows immediately start using new NAT policy.</p> | <p>A NAT policy change via CoA is performed by changing the sub-profile for the ESM subscriber or by changing the ESM subscriber filter in the LSN case. 1</p> <p>A sub-profile change alone does not trigger accounting messages in L2-aware NAT and consequently the logging information is lost.</p> <p>To ensure timely RADIUS logging of the NAT policy change in L2-aware NAT, each CoA must, in addition to the sub-profile change, also:</p> <ul style="list-style-type: none"> <li>• Change the sla-profile2 or</li> <li>• Include the Alc-Trigger-Acct-Interim VSA in the CoA messages.</li> </ul> <p>Both of the above events will trigger an accounting update at the time when CoA is processed. This keeps NAT logging current.</p> |

**Table 37 NAT Policy Changes via CoA (Continued)**

| Action | Outcome                                                                                                                                                                                                                                                                          |     | Remarks |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---------|
|        | L2-Aware                                                                                                                                                                                                                                                                         | LSN |         |
|        | (cont.) <ul style="list-style-type: none"><li>• Not allowed if L2-Aware subscriber has multiple hosts <b>and</b> the new prefix-list contains one or more 1:1 NAT policies.</li><li>• Not allowed if the new NAT policy references to a pool in a different NAT group.</li></ul> |     |         |

1. In non-ESM environments, the NAT policy can be changed by replacing the interface filter via CLI for LSN case.

2. The SLA profile will have to be changed and not just *refreshed*. In other words, replacing the existing SLA profile with the same one will not trigger a new accounting message.

## 7.10.2 CoA and DNAT

Adding, removing or replacing DNAT parameters in LSN44 can be achieved through NAT policy manipulation in an IP filter for ESM subscriber. The rules for NAT policy manipulation via CoA are given in [Table 37](#).

In L2-Aware NAT, CoA can be used to:

- Enable or disable DNAT functionality while leaving the Source Network Address and Port Translation (SNAPT) uninterrupted.
- Modify the default destination IP address in DNAT.

Once the DNAT configuration is modified via CoA (enable or disable DNAT or change the default DNAT IP address), the existing flows affected by the change remain active for 5 more seconds while the new flows are created in accordance with the new configuration. After a 5 second timeout, the stale flows are cleared from the system.

The RADIUS attribute used to perform DNAT modifications is a composite attribute with the following format:

Alc-DNAT-Override (234) = "{<DNAT\_state> | <DNAT-ip-addr>},[nat-policy]"

where: *DNAT state* = none | disable → is mutually exclusive with the **DNAT-ip-addr** parameter.

DNAT-ip-addr = Provides an implicit enable with the destination IPv4 address in dotted format (a.b.c.d) → is mutually exclusive with DNAT-state parameter.

nat-policy = nat-policy *name* → This is an optional parameter. If it is not present, then the default NAT policy is assumed.

#### For example:

Alc-DNAT-Override=none → This will negate any previous DNAT related override in the **default** nat-policy. Consequently, the DNAT functionality will be set as originally defined in the **default** nat-policy. In case that the 'none' value is received while DNAT is already enabled, a CoA ACK will be sent back to the originator.

Alc-DNAT-Override =none,nat-pol-1 → This will re-enable DNAT functionality in the specific NAT policy with the name *nat-policy-1*.

Alc-DNAT-Override =none,10.1.1.1 → The DNAT-state and DNAT-ip-addr parameters are mutually exclusive within the same Alc-DNAT-Override attribute. Although a CoA ACK reply will be returned to the RADIUS server, an error log message is generated in the SR OS indicating that the attempted override failed.

Alc-DNAT-Override =10.1.1.1 → This will change the default DNAT IP address to 1.1.1.1 in the default NAT policy. In case DNAT was disabled prior to receiving this CoA, it will be implicitly enabled.

Alc-DNAT-Override =10.1.1.1,nat-pol-1 → This will change the default DNAT IP address to 10.1.1.1 in the specific NAT policy named *nat-policy-1*. DNAT will be implicitly enabled if it was disabled prior to receiving this CoA.

The combination of sub-fields with the Alc-DNAT-Override RADIUS attribute and the corresponding actions are shown in [Table 38](#).

**Table 38**      **CoA and DNAT**

| DNAT-State | DNAT-ip-addr | NAT Policy   | DNAT Action in L2-Aware NAT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------|--------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none       | -            | -            | <p>Re-enable DNAT in the default NAT policy.</p> <p>If DNAT was enabled prior to receiving this CoA, then no specific action will be carried out by the SR OS with the exception of sending the CoA ACK back to the CoA server.</p> <p>This negates any previous DNAT-related override in the default nat-policy. Consequently, the DNAT functionality will be set as originally defined in the default nat-policy.</p> <p>If the DNAT classifier is not present in the default nat-policy when this CoA is received, an error log message is raised.</p> |
| none       | -            | nat-pol-name | <p>Re-enable DNAT in the referenced NAT policy.</p> <p>This will negate any previous DNAT related override in the referenced nat-policy. Consequently, the DNAT functionality will be set as originally defined in the referenced nat-policy.</p> <p>If the DNAT classifier is not present in the referenced nat-policy when this CoA is received, a CoA ACK reply will be returned to the RADIUS server and an error log message is generated in the SR OS indicating that the attempted override has failed.</p>                                        |
| none       | a.b.c.d      | -            | <p>These two parameters are mutually exclusive in the same Alc-DNAT-Override attribute.</p> <p>Although a CoA ACK reply will be returned to the RADIUS server, an error log message is generated in SR OS indicating that the attempted override has failed.</p>                                                                                                                                                                                                                                                                                          |
| none       | a.b.c.d      | nat-pol-name | <p>DNAT-state and DNAT-ip-address parameters are mutually exclusive in the same Alc-DNAT-Override attribute.</p> <p>Although a CoA ACK reply will be returned to the RADIUS server, an error log message is generated in SR OS indicating that the attempted override has failed.</p>                                                                                                                                                                                                                                                                     |
| disable    | -            | -            | <p>Disable DNAT in the default NAT policy.</p> <p>If the DNAT classifier is not present in the default nat-policy when this CoA is received, a CoA ACK reply will be returned to the RADIUS server and an error log message is generated in the SR OS indicating that the attempted override has failed.</p>                                                                                                                                                                                                                                              |



**Table 38 CoA and DNAT (Continued)**

| DNAT-State | DNAT-ip-addr | NAT Policy              | DNAT Action in L2-Aware NAT                                                                                                                                                                                                                                                                         |
|------------|--------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| disable    | -            | nat-pol-name            | Disable DNAT in the referenced NAT policy.<br>If the DNAT classifier is not present in the referenced nat-policy when this CoA is received, a CoA ACK reply will be returned to the RADIUS server and an error log message is generated in SR OS indicating that the attempted override has failed. |
| disable    | a.b.c.d      | -                       | The DNAT-state and DNAT-ip-address parameters are mutually exclusive in the same Alc-DNAT-Override attribute.<br>Although a CoA ACK reply will be returned to the RADIUS server, an error log message is generated in SR OS indicating that the attempted override has failed.                      |
| disable    | a.b.c.d      | nat-pol-name            | The DNAT-state and DNAT-ip-address parameters are mutually exclusive in the same Alc-DNAT-Override attribute.<br>Although a CoA ACK reply will be returned to the RADIUS server, an error log message is generated in the SR OS indicating that the attempted override has failed.                  |
| -          | a.b.c.d      | -                       | The default destination IP address is changed in the default NAT policy.                                                                                                                                                                                                                            |
| -          | a.b.c.d      | nat-pol-name            | The default destination IP address is changed in the referenced NAT policy.                                                                                                                                                                                                                         |
| -          | -            | -<br>or<br>nat-pol-name | A CoA NAK (error) is generated. Either DNAT-state or DNAT-ip-address parameters must be present in the Alc-DNAT-Override attribute.                                                                                                                                                                 |

If multiple Alc-DNAT-Override attributes with conflicting actions are received in the same CoA or Access-Accept, the action that occurred last will take precedence.

For example, if the following two Alc-DNAT-Override attributes are received in the same CoA, the last one takes effect and consequently DNAT will be disabled in the default NAT policy:

*Alc-DNAT-Override* = "10.1.1.1"

*Alc-DNAT-Override* = "disable"

### 7.10.3 Modifying an Active NAT Prefix List or Nat Classifier via CLI

The following table describes the outcome when the active NAT prefix list or NAT classifier is modified via CLI.

**Table 39**      **Modifying Active NAT Prefix List or NAT Classifier**

| Action                                                        | Outcome                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                               | Remarks                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               | L2-Aware                                                                                                                                                                                                                                                                                                          | LSN                                                                                                                                                                           |                                                                                                                                                                                                                                                                                               |
| CLI – Modifying prefix in the NAT prefix list                 | Existing flows are always checked whether they comply with the NAT prefix list that is currently applied in the subscriber profile for the subscriber. If the flows do not comply with the current NAT prefix list, they are cleared after 5 seconds. The new flows immediately start using the updated settings. | Changing the prefix in the NAT prefix list will internally re-subnet the outside IP address space.                                                                            | A NAT prefix list is used with multiple NAT policies in L2-Aware NAT and for downstream Internal subnet in DNAT-only scenario for LSN.<br><br>The prefix can be modified (added, removed, remapped) at any time in the NAT prefix list, while the NAT policy must be first shut down via CLI. |
| CLI – Modifying or replacing the NAT classifier               | Existing flows are always checked whether they comply with the NAT classifier that is currently applied in the active NAT policy for the subscriber. If the flows do not comply with the current NAT classifier, they are cleared after 5 seconds. The new flows immediately start using the updated settings.    | Changing the NAT classifier have the same effect as in L2-Aware NAT; all existing flows using the NAT classifier are checked whether they comply with this classifier or not. | The NAT classifier is used for DNAT.<br>NAT classifier is referenced in the NAT policy.                                                                                                                                                                                                       |
| CLI - Removing or adding NAT policy in NAT prefix list        | Blocked                                                                                                                                                                                                                                                                                                           | Not applicable                                                                                                                                                                |                                                                                                                                                                                                                                                                                               |
| CLI - Removing or adding NAT policy in the subscriber profile | Blocked                                                                                                                                                                                                                                                                                                           | Not applicable                                                                                                                                                                |                                                                                                                                                                                                                                                                                               |

**Table 39**      **Modifying Active NAT Prefix List or NAT Classifier (Continued)**

| Action                                                                                 | Outcome        |                                                                                                                                                                                                                                                                                       | Remarks |
|----------------------------------------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                                        | L2-Aware       | LSN                                                                                                                                                                                                                                                                                   |         |
| CLI - Removing, adding or replacing NAT prefix list under the rtr/nat/inside/DNAT-only | Not applicable | This action will trigger internally re-subnet the source address space according to the new NAT prefix list. However, the current flows in the MS ISA are not affected by this change. In other words, they are not removed if the associated prefix is removed from the prefix list. |         |

## 7.11 Port Control Protocol (PCP)

PCP is a protocol that operates between subscribers and the NAT directly. This makes the protocol similar to DHCP or PPP in that the subscriber has a limited but direct control over the NAT behavior.

PCP is designed to allow the configuration of static port-forwards, obtain information about existing port forwards and to obtain the outside IP address from software running in the home network or on the CPE.

PCP runs on each MS-ISA as its own process and make use of the same source-IP hash algorithm as the NAT mappings themselves. The protocol itself is UDP based and is request/response in nature, in some ways, similar to UPnP.

PCP operates on a specified loopback interface in a similar way to the local DHCP server. It operates on UDP and a specified (in CLI) port. As Epoch is used to help recover mappings, a unique PCP service must be configured for each NAT group.

When epoch is lowered, there is no mechanism to inform the clients to refresh their mappings en-masse. External synchronization of mappings is possible between two chassis (epoch does not need to be synchronized). If epoch is unsynchronized then the result will be clients re-creating their mapping on next communication with the PCP server.

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Version = 1 | R | OpCode | Reserved (16 bits) |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Requested Lifetime |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
:
: (optional) opcode-specific information
:
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
:
: (optional) PCP Options
:
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The R-bit (0) indicates request and (1) indicates response. This is a request so (0).

OpCode defined as:

Requested Lifetime: Lifetime 0 means delete.

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Version = 1 | R | OpCode | Reserved | Result Code |

```

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Lifetime |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Epoch |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
: : :
: (optional) OpCode-specific response data :
: : :
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
: (optional) Options :
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

As this is a response, R = (1).

The Epoch field increments by 1 every second and can be used by the client to determine if state needs to be restored. On any failure of the PCP server or the NAT to which it is associated Epoch must restart from zero (0).

Result Codes:

- 0 SUCCESS, success.
- 1 UNSUPP\_VERSION, unsupported version.
- 2 MALFORMED\_REQUEST, a general catch-all error.
- 3 UNSUPP\_OPCODE, unsupported OpCode.
- 4 UNSUPP\_OPTION, unsupported option. Only if the Option was mandatory.
- 5 MALFORMED\_OPTION, malformed option.
- 6 UNSPECIFIED\_ERROR, server encountered an error
- 7 MISORDERED\_OPTIONS, options not in correct order

Creating a Mapping

Client Sends

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Protocol | Reserved (24 bits) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Internal port | Suggested external port |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
: :
: Suggested External IP Address (32 or 128, depending on OpCode): :
: :
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

MAP4 opcode is (1). Protocols: 0 – all; 1 – ICMP; 6 – TCP; 17 – UDP.

MAP4 (1), PEER4 (3) and PREFER\_FAILURE are supported. FILTER and THIRD\_PARTY are not supported.

## 7.12 Universal Plug and Play Internet Gateway Device Service

Universal Plug and Play (UPnP), which is a set of specifications defined by the UPnP forum. One specification is called Internet Gateway Device (IGD) which defines a protocol for clients to automatically configure port mappings on a NAT device. Today, many gaming, P2P, VoIP applications support the UPnP IGD protocol. The SR OS supports the following UPnP version 1 **InternetGatewayDevice version 1** features:

- Supports only L2-Aware NAT hosts.
- Distributed subscriber management is not supported.
- The UPnP server runs on NAT ISA and only serves the local L2-Aware NAT hosts on the same ISA.
- The UPnP server can be enabled per subscriber by configuring a **upnp-policy** in the sub-profile.
- UPnP discovery is supported.
- UPnP eventing is not supported.
- The following IGD devices and services are supported:
  - InternetGatewayDevice
    - WANDevice
    - WANConnectionDevice
    - WANIPConnection service
- For WANIPConnection services:
  - Optional state variables in a WANIPConnection service are not supported.
  - Optional actions in a WANIPConnection services are not supported.
  - Wildcard ExternalPort is not supported.
  - Only supports wildcard RemoteHost.
  - Up to 64 bytes of port mapping description are supported.
  - The SR OS supports a vendor specific action **X\_ClearPortMapping**. This clears all port mappings of the subscriber belonging to the requesting host. This action has no in or out arguments.
- If the NewExternalPort in an addPortMapping request is same as the external port of one existing UPnP port mapping:
  - If NewInternalClient is different from InternalClient of existing mapping, then system the will reject the request.
  - If NewInternalClient is same as InternalClient of existing mapping:

- With strict-mode on — If the source IP address of the request is same as InternalClient of existing mapping, then the request is accepted; otherwise the request is rejected.
- With strict-mode off, the request is accepted.
- The system also supports the Alc-UPnP-Sub-Override-Policy RADIUS VSA which can be included in access-accept or CoA request. It can be used to override the **upnp-policy** configured in sub-profile or disable UPnP for the subscriber. See RADIUS reference guide for detail usage.

## 7.12.1 Configuring UPnP IGD Service

**Step 1.** Configure L2-Aware NAT.

**Step 2.** Create a **upnp-policy**:

**Step 3.** Configure the **upnp-policy** as created in Step 2 in the subscriber profile:

```
config>service
 upnp
 upnp-policy "test" create
 no description
 http-listening-port 5000
 mapping-limit 100
 no strict-mode
 exit

config>subscr-mgmt
 sub-profile "l2nat-upnp" create
 nat-policy "l2"
 upnp-policy "test"
exit
```



## 7.13 NAT Point-to-Point Tunneling Protocol (PPTP) Application Layer Gateway (ALG)

PPTP is defined in RFC 2637, *Point-to-Point Tunneling Protocol (PPTP)*, and is used to provide VPN connection for home/mobile users to gain secure access to the enterprise network. Encrypted payload is transported over GRE tunnel that is negotiated over TCP control channel. In order for PPTP traffic to pass through NAT, the NAT device must correlate the TCP control channel with the corresponding GRE tunnel. This mechanism is referred to as PPTP ALG.

### 7.13.1 PPTP Protocol

There are two components of PPTP:

- Step 1.** TCP control connection between the two endpoints.
- Step 2.** An IP tunnel operating between the same endpoints. These are used to transport GRE encapsulated PPP packets for user sessions between the endpoints. PPTP uses an extended version of GRE to carry user PPP packets.

The control connection is established from the PPTP clients (for example, home users behind the NAT) to the PPTP server which is located on the outside of the NAT. Each session that carries data between the two endpoints can be referred as call. Multiple sessions (or calls) can carry data in a multiplexed fashion over a tunnel. The tunnel protocol is defined by a modified version of GRE. Call ID in the GRE header is used to multiplex sessions over the tunnel. The Call-ID is negotiated during the session/call establishment phase.

#### 7.13.1.1 Supported Control Messages

Control Connection Management — The following messages are used to maintain the control connection.

- Start-Control-Connection-Request
- Start-Control-Connection-Reply
- Stop-Control-Connection-Request
- Stop-Control-Connection-Reply
- Echo-Request

- Echo-Reply

The remaining control message types are sent over the established TCP session to open/maintain sessions and to convey information about the link state:

Call Management — Call management messages are used to establish/terminate a session/call and to exchange information about the multiplexing field (Call-id). Call-IDs must be captured and translated by the NAT. The call management messages are:

- Outgoing-Call-Request (contains Call ID)
- Outgoing-Call-Reply (contains Call ID and peer's Call-ID)
- Call-Clear-Request (contains Call ID)
- Call-Disconnect-Notify (contains Call ID)

Error Reporting — This message is sent by the client to indicate WAN error conditions that occur on the interface supporting PPP.

- Wan-Error-Notify (contains Call ID and Peer's Call ID)

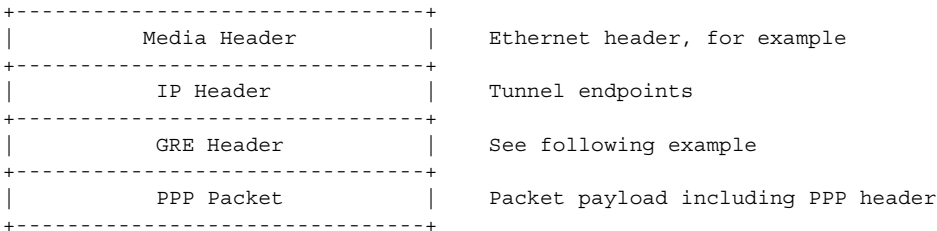
PPP Session Control — This message is sent in both directions to setup PPP-negotiated options.

- Set-Link-Info (contains Call ID and Peer's Call ID)

Once Call-ID is negotiated by both endpoints, it is inserted in GRE header and used as multiplexing field in the tunnel that carries data traffic.

### 7.13.1.2 GRE Tunnel

A GRE tunnel is used to transport data between two PPTP endpoints. The packet transmitted over this tunnel has the following general structure:



The GRE header contains the Call ID of the peer for the session for which the GRE packet belongs.

```

0 1 2 3
0 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|C|R|K|S|s|Recur|A| Flags | Ver | Protocol Type |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Key (HW) Payload Length | Key (LW) Call ID |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Sequence Number (Optional) |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Acknowledgment Number (Optional) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

## 7.13.2 PPTP ALG Operation

PPTP ALG is aware of the control session (Start Control Connection Request/Replay) and consequently it captures the Call ID field in all PPTP messages that carry that field. In addition to translating inside IP and TCP port, the PPTP ALG process data beyond the TCP header in order to extract the Call ID field and translate it inside of the Outgoing Call Request messages initiated from the inside of the NAT.

The GRE packets with corresponding Call IDs are translated through the NAT as follows:

- The inside source IP address is replaced by the outside IP address and vice versa for traffic in the opposite direction. This is standard IP address translation technique. The key is to keep the outside IP address of the control packets and corresponding data packets (GRE tunnel) the same.
- The Call-ID in the GRE packets in the direction outside to inside will be translated by the NAT according to the mappings that were created during session negotiation.

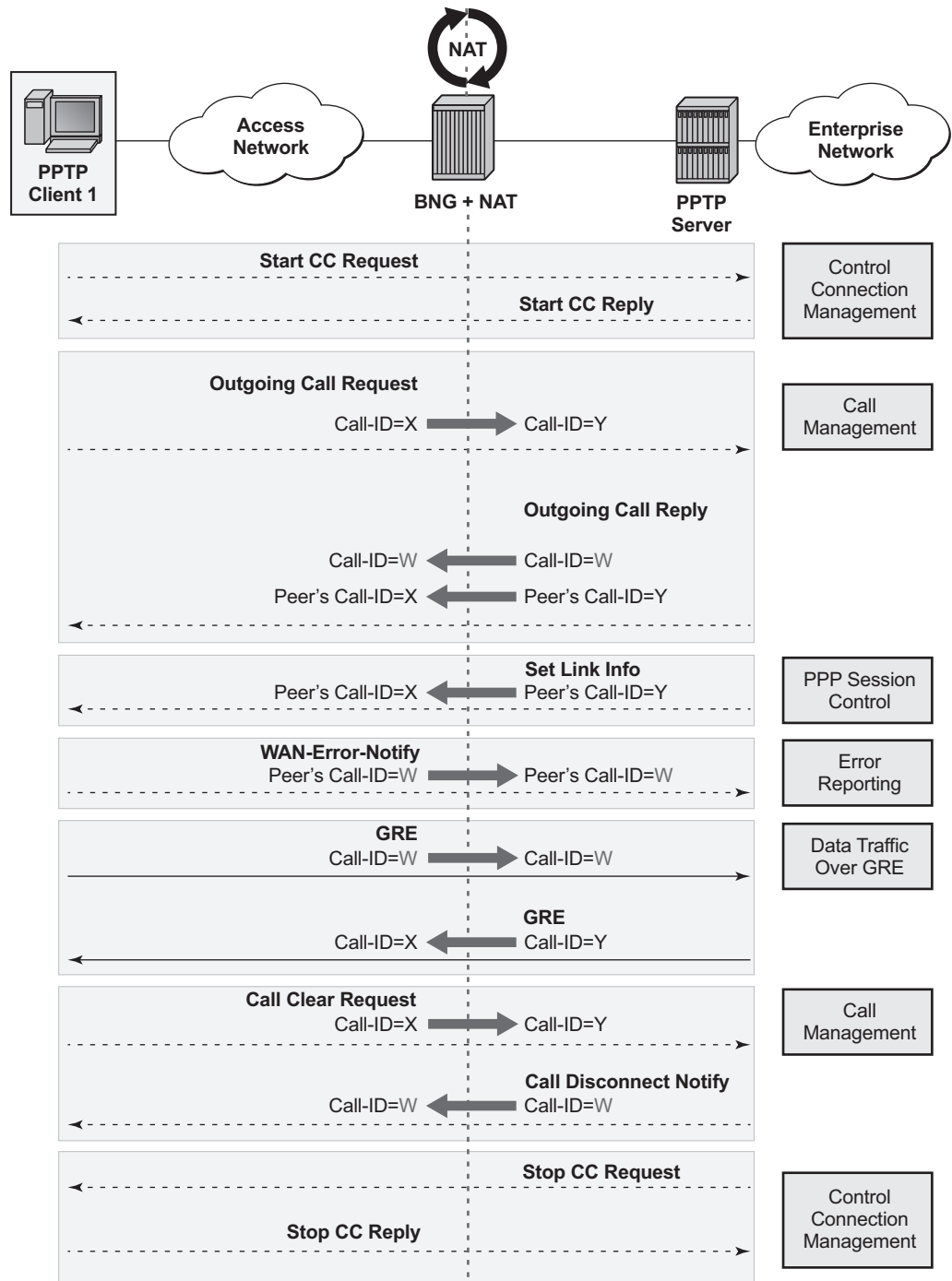
In addition, the following applies:

- GRE packets are translated and passed through the NAT only if they can be matched to an existing PPTP call for which the mapping already exists.

- Translation of the Call-IDs advertised by the PPTP server in the Outgoing Call Reply control message (this message is sent from the outside of the NAT to the inside) are not translated. Subsequently the Call ID in such messages are transparently passed through the NAT. There is no need to translate those Call IDs as their uniqueness between the two endpoints are guaranteed by the selection algorithm of the PPTP server. This can be thought of as destination TCP/UDP ports. They are not translated in the NAT. Instead only the source ports are translated.
- PPTP session initiation in the outside to inside direction through the NAT is not supported.
- Call-ID's are allocated and used in the same fashion as the outside TCP/UDP ports (random with parity). They are taken from the same port range as ICMP ports.

The basic principle of PPTP NAT ALG is shown in [Figure 67](#).

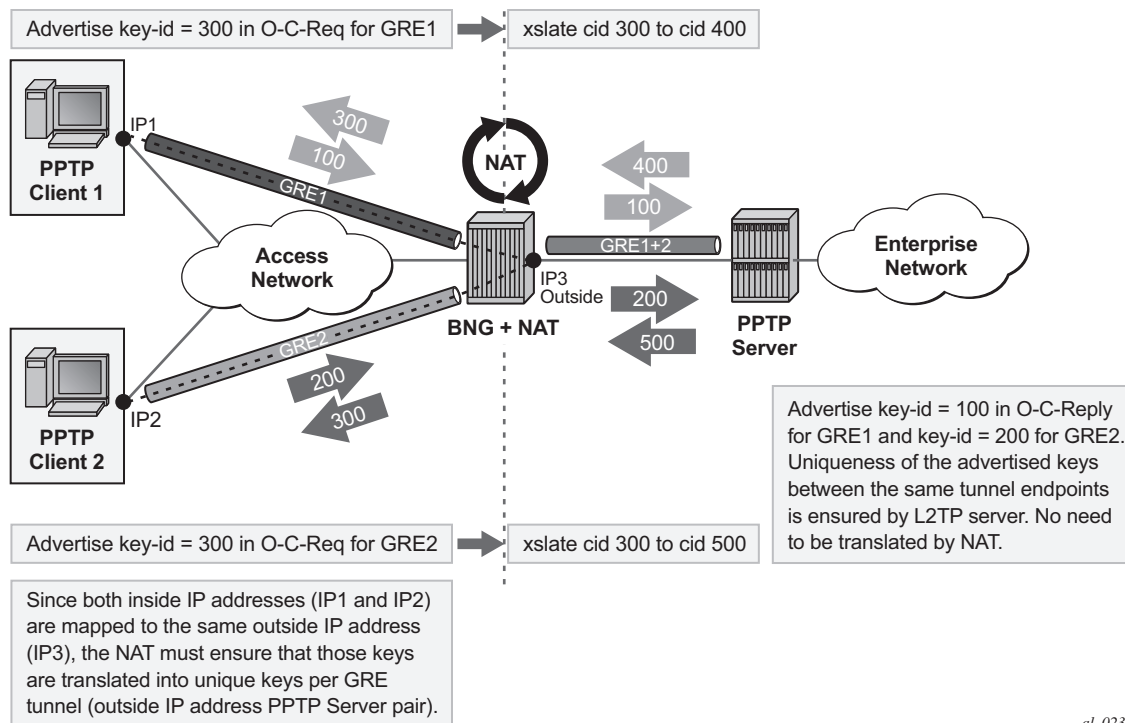
**Figure 67 NAT PPTP Operation**



al\_0238

The scenario where multiple clients behind the NAT are terminated to the same PPTP server is shown in [Figure 68](#). In this case, it is possible that the source IP addresses of the two PPTP clients are mapped to the same outside address of the NAT. Since the endpoints of the GRE tunnel from the NAT to the PPTP server will be the same for both PPTP clients (although their real source IP addresses are different), the NAT must ensure the uniqueness of the Call-IDs in the outbound data connection. This is where Call-ID translation in the NAT becomes crucial.

**Figure 68 Merging of Endpoints in NAT**



### 7.13.3 Multiple Sessions Initiated From the Same PPTP Client Node

The routers supports a deployment scenario where multiple calls (or tunnels) are established from a single PPTP node within a single control connection. In this case, there is only one set of Start-Control-Connection-Req/Reply messages (one control channel) and multiple sets of Outgoing-Call-Req/Reply messages.

## **7.13.4 Selection of Call IDs in NAT**

Call-Id are taken from the same pool as the ICMP port ranges. Port-ranges and Call-IDs are both 16-bit values. Call-id selection mechanism is the same as the outside TCP/UDP port selection mechanism (random with parity).

## 7.14 Modifying Active Nat-Prefix-List or NAT Classifier via CLI

The following table describes the outcome when the active nat-prefix-list or NAT classifier is modified via CLI.

**Table 40** Modifying Active NAT Prefix List or NAT Classifier

| Action                                                            | Outcome                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                     | Remarks                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                   | L2-Aware                                                                                                                                                                                                                                                                                                                   | LSN                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                         |
| CLI –<br>Modifying<br>prefix in the<br>NAT prefix<br>list         | Existing flows are always checked whether they comply with the NAT prefix list that is currently applied in the sub-profile for the subscriber. If the flows do not comply with the current NAT prefix list, they are cleared after 5 seconds.<br><br>The new flows will immediately start using the updated settings.     | Changing the prefix in the NAT prefix list will internally re-subnet the outside IP address space.                                                                                  | Nat-prefix list is used with multiple NAT policies in L2-Aware NAT and for downstream internal subnet in dNAT-only scenario for LSN.<br><br>Prefix can be modified (added, removed, remapped) at any time in the NAT prefix list, while the NAT policy must be first shut down via CLI. |
| CLI –<br>Modifying<br>the NAT<br>classifier                       | Existing flows are always checked whether they comply with the NAT classifier that is currently applied in the active NAT policy for the subscriber. If the flows do not comply with the current NAT classifier, they are cleared after 5 seconds.<br><br>The new flows will immediately start using the updated settings. | Changing the NAT classifier has the same effect as in L2-Aware NAT; all existing flows using the NAT classifier are checked to see whether or not they comply with this classifier. | The NAT classifier is used for dNAT.<br>The NAT classifier is referenced in the NAT policy.                                                                                                                                                                                             |
| CLI -<br>Removing/<br>adding NAT<br>policy in nat-<br>prefix-list | Blocked                                                                                                                                                                                                                                                                                                                    | Not Applicable                                                                                                                                                                      |                                                                                                                                                                                                                                                                                         |



**Table 40**      **Modifying Active NAT Prefix List or NAT Classifier (Continued)**

| Action                                                                                                          | Outcome        |                                                    | Remarks |
|-----------------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------------|---------|
|                                                                                                                 | L2-Aware       | LSN                                                |         |
| CLI -<br>Removing/<br>adding/<br>replacing<br>NAT policy<br>in sub-<br>profile                                  | Blocked        | Not Applicable                                     |         |
| CLI -<br>Removing/<br>adding/<br>replacing<br>NAT prefix-<br>list under<br>the rtr/nat/<br>inside/dnat-<br>only | Not Applicable | Internally re-subnet,<br>no effect on the<br>flows |         |

## 7.15 NAT Logging

LSN logging is extremely important to the Service Providers (SP) who are required by the government agencies to track source of suspicious Internet activities back to the users that are hidden behind the LSN device.

The 7750 SR supports several modes of logging for LSN applications. Choosing the right logging model will depend on the required scale, simplicity of deployment and granularity of the logged data.

For most purposes logging of allocation/de-allocation of outside port-blocks and outside IP address along with the corresponding LSN subscriber and inside service-id will suffice.

In certain cases port-block based logging is not satisfactory and per flow logging is required.

### 7.15.1 Syslog/SNMP/Local-File Logging

The simplest form of LSN and L2-Aware NAT logging is via logging facility in the 7750 SR, commonly called logger. Each port-block allocation/de-allocation event will be recorded and send to the system logging facility (logger). Such an event can be:

- Recorded in the system memory as part of regular logs.
- Written to a local file.
- Sent to an external server via syslog facility.
- Sent to a SNMT trap destination.

In this mode of logging, all applications in the system share the same logger.

Syslog/SNMP/Local-File logging on LSN is mutually exclusive with NAT RADIUS-based logging.

Syslog/SNMP/local-file logging must be separately enabled for LSN and L2-Aware NAT in log even-control. The following displays relevant MIB events:

```
2012 tmnxNatPlBlockAllocationLsn
2013 tmnxNatPlBlockAllocationL2Aw
```

### 7.15.1.1 Filtering LSN Events to System Memory

In this example a single port-block [1884-1888] is allocated/de-allocated for the inside IP address 10.5.5.5 which is mapped to the outside IP address 198.51.100.1. Consequently the event is logged in the memory as.

```
2 2012/07/12 16:40:58.23 WEST MINOR: NAT #2012 Base NAT
"{2} Free 198.51.100.1 [1884-1888] -- vprn10 10.5.5.5 at 2012/07/12 16:40:58"

1 2012/07/12 16:39:55.15 WEST MINOR: NAT #2012 Base NAT
"{1} Map 198.51.100.1 [1884-1888] -- vprn10 10.5.5.5 at 2012/07/12 16:39:55"
```

Once the desired LSN events are enabled for logging via event-control configuration, they can be logged to memory via standard log-id 99 or be filtered via a custom log-id, such as in this example (log-id 5):

Configuration:

```
*A:left-a20>config>log# info

 filter 1
 default-action drop
 entry 1
 action forward
 match
 application eq "nat"
 numbr eq 2012
 exit
 exit
 exit
 event-control "nat" 2001 suppress
 event-control "nat" 2002 suppress
 event-control "nat" 2003 suppress
 event-control "nat" 2004 suppress
 event-control "nat" 2005 suppress
 event-control "nat" 2006 suppress
 event-control "nat" 2007 suppress
 event-control "nat" 2008 suppress
 event-control "nat" 2009 suppress
 event-control "nat" 2010 suppress
 event-control "nat" 2011 suppress
 event-control "nat" 2012 generate
 event-control "nat" 2014 suppress
 event-control "nat" 2015 suppress
 event-control "nat" 2017 suppress
 syslog 10
 exit
 log-id 5
 filter 1
 from main
 to memory
 exit

```

```
*A:left-a20# show log event-control "nat"
=====
Log Events
=====
Application
ID# Event Name P g/s Logged Dropped

2001 tmnxNatPlL2AwBlockUsageHigh WA thr 0 0
2002 tmnxNatIsaMemberSessionUsageHigh WA thr 0 0
2003 tmnxNatPlLsnMemberBlockUsageHigh WA thr 0 0
2007 tmnxNatL2AwSubIcmpPortUsageHigh WA thr 0 0
2008 tmnxNatL2AwSubUdpPortUsageHigh WA thr 0 0
2009 tmnxNatL2AwSubTcpPortUsageHigh WA thr 0 0
2010 tmnxNatL2AwSubSessionUsageHigh WA thr 0 0
2012 tmnxNatPlBlockAllocationLsn MI sup 0 0
2013 tmnxNatPlBlockAllocationL2Aw MI sup 0 0
2014 tmnxNatResourceProblemDetected MI thr 0 0
2015 tmnxNatResourceProblemCause MI thr 0 0
2016 tmnxNatPlAddrFree MI sup 0 0
2017 tmnxNatPlLsnRedActiveChanged WA thr 0 0
2018 tmnxNatPcpSrvStateChanged MI thr 0 0
2020 tmnxNatMdaActive MI thr 0 0
2021 tmnxNatLsnSubBlksFree MI sup 0 0
2022 tmnxNatDetPclyChanged MI thr 0 0
2023 tmnxNatMdaDetectsLoadSharingErr MI thr 0 0
2024 tmnxNatIsaGrpOperStateChanged MI thr 0 0
2025 tmnxNatIsaGrpIsDegraded MI thr 0 0
2026 tmnxNatLsnSubIcmpPortUsgHigh WA thr 0 0
2027 tmnxNatLsnSubUdpPortUsgHigh WA thr 0 0
2028 tmnxNatLsnSubTcpPortUsgHigh WA thr 0 0
2029 tmnxNatLsnSubSessionUsgHigh WA thr 0 0
2030 tmnxNatInAddrPrefixBlksFree MI sup 0 0
2031 tmnxNatFwd2EntryAdded MI sup 0 0
2032 tmnxNatDetPclyOperStateChanged MI thr 0 0
2033 tmnxNatDetMapOperStateChanged MI thr 0 0
2034 tmnxNatFwd2OperStateChanged WA thr 0 0
=====
```

The event description is given below:

tmnxNatPlL2AwBlockUsageHigh

The tmnxNatPlL2AwBlockUsageHigh notification is sent when the block usage of a Layer-2-Aware NAT address pool reaches its high watermark ('true') or when it reaches its low watermark again ('false').

tmnxNatIsaMemberSessionUsageHigh

The tmnxNatIsaMemberSessionUsageHigh notification is sent when the session usage of a NAT ISA group member reaches its high watermark ('true') or when it reaches its low watermark again ('false').

tmnxNatPlLsnMemberBlockUsageHigh

The tmnxNatPlLsnMemberBlockUsageHigh notification is sent when the block usage of a Large Scale NAT address pool reaches its high watermark ('true') or when it reaches its low watermark again ('false').

on a particular member MDA of its ISA group.

**tmnxNatLsnSubIcmpPortUsageHigh**

The tmnxNatLsnSubIcmpPortUsageHigh notification is sent when the ICMP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatLsnSubUdpPortUsageHigh**

The tmnxNatLsnSubUdpPortUsageHigh notification is sent when the UDP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatLsnSubTcpPortUsageHigh**

The tmnxNatLsnSubTcpPortUsageHigh notification is sent when the TCP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatL2AwSubIcmpPortUsageHigh**

The tmnxNatL2AwSubIcmpPortUsageHigh notification is sent when the ICMP port usage of a Layer-2-Aware NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatL2AwSubUdpPortUsageHigh**

The tmnxNatL2AwSubUdpPortUsageHigh notification is sent when the UDP port usage of a Layer-2-Aware NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatL2AwSubTcpPortUsageHigh**

The tmnxNatL2AwSubTcpPortUsageHigh notification is sent when the TCP port usage of a Layer-2-Aware NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatL2AwSubSessionUsageHigh**

The tmnxNatL2AwSubSessionUsageHigh notification is sent when the session usage of a Layer-2-Aware NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatLsnSubSessionUsageHigh**

The tmnxNatLsnSubSessionUsageHigh notification is sent when the session usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

**tmnxNatPlBlockAllocationLsn**

The tmnxNatPlBlockAllocationLsn notification is sent when an outside IP address and a range of ports is allocated to a NAT subscriber associated with a Large Scale NAT (LSN) pool, and when this allocation expires.

**tmnxNatPlBlockAllocationL2Aw**

The tmnxNatPlBlockAllocationL2Aw notification is sent when an outside IP address and a range of ports is allocated to

a NAT subscriber associated with a Layer-2-Aware NAT pool,  
and when this allocation expires.

**tmnxNatResourceProblemDetected**

The **tmnxNatResourceProblemDetected** notification is sent when  
the value of the object **tmnxNatResourceProblem** changes.

**tmnxNatResourceProblemCause**

The **tmnxNatResourceProblemCause** notification is to describe the cause  
of a NAT resource problem.

**tmnxNatPlAddrFree**

The **tmnxNatPlAddrFree** notification is sent when  
a range of outside IP addresses becomes free at once.

**tmnxNatPlLsnRedActiveChanged**

The **tmnxNatPlLsnRedActiveChanged** notification is related to NAT Redundancy  
sent when the value of the object **tmnxNatPlLsnRedActive** changes. The cause is  
explained in the **tmnxNatNotifyDescription** which is a printable character  
string.

**tmnxNatMdaActive**

The **tmnxNatMdaActive** notification is sent when  
the value of the object **tmnxNatIsaMdaStatOperState** changes from  
'primary' to any other value, or the other way around.  
The value 'primary' means that the MDA is active in the group.

**tmnxNatLsnSubBlksFree**

The **tmnxNatLsnSubBlksFree** notification is sent when  
all port blocks allocated to a Large Scale NAT (LSN) subscriber  
are released.

The NAT subscriber is identified with its subscriber ID  
**tmnxNatNotifyLsnSubId**.

To further facilitate the identification of the NAT subscriber,  
its type **tmnxNatNotifySubscriberType**,  
inside IP address **tmnxNatNotifyInsideAddr**  
and inside virtual router instance **tmnxNatNotifyInsideVRtrID**  
are provided.

The values of **tmnxNatNotifyMdaChassisIndex**, **tmnxNatNotifyMdaCardSlotNum**  
and **tmnxNatNotifyMdaSlotNum** identify the ISA MDA where the blocks were  
processed.

All notifications of this type are sequentially numbered with  
the **tmnxNatNotifyPlSeqNum**.

The value of **tmnxNatNotifyNumber** is the numerical identifier of the  
NAT policy used for this allocation; it can be used for correlation  
with the **tmnxNatPlBlockAllocationLsn** notification; the value zero  
means that this notification can be correlated with all the  
**tmnxNatPlBlockAllocationLsn** notifications of the subscriber.

**tmnxNatDetPlcyChanged**

The **tmnxNatDetPlcyChanged** notification is sent when  
something changed in the Deterministic NAT map.

[CAUSE] Such a change may be caused by a modification of the

tmnxNatDetPlycTable or the tmnxNatDetMapTable.

[EFFECT] Traffic flows of one or more given subscribers, subject to NAT, may be assigned different outside IP address and/or outside port.

[RECOVERY] Managers that rely on the offline representation of the Deterministic NAT map should get an updated copy.

tmnxNatMdaDetectsLoadSharingErr

The tmnxNatMdaDetectsLoadSharingErr notification is sent periodically at most every 10 seconds while a NAT ISA MDA detects that it is receiving packets erroneously, due to incorrect load-balancing by the ingress IOM.

The value of tmnxNatNotifyCounter is the incremental count of dropped packets since the previous notification sent by the same MDA.

[CAUSE] The ingress IOM hardware does not support a particular NAT function's load-balancing, for example an IOM-2 does not support deterministic NAT.

[EFFECT] The MDA drops all incorrectly load-balanced traffic.

[RECOVERY] Upgrade the ingress IOM, or change the configuration.

tmnxNatIsaGrpOperStateChanged

The tmnxNatIsaGrpOperStateChanged notification is sent when the value of the object tmnxNatIsaGrpOperState changes.

tmnxNatIsaGrpIsDegraded

The tmnxNatIsaGrpIsDegraded notification is sent when the value of the object tmnxNatIsaGrpDegraded changes.

tmnxNatLsnSubIcmpPortUsqHigh

The tmnxNatLsnSubIcmpPortUsqHigh notification is sent when the ICMP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

The subscriber is identified with its inside IP address or prefix tmnxNatNotifyInsideAddr in the inside virtual router instance tmnxNatNotifyInsideVRtrID.

tmnxNatLsnSubUdpPortUsqHigh

The tmnxNatLsnSubUdpPortUsqHigh notification is sent when the UDP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

The subscriber is identified with its inside IP address or prefix tmnxNatNotifyInsideAddr in the inside virtual router instance tmnxNatNotifyInsideVRtrID.

tmnxNatLsnSubTcpPortUsqHigh

The tmnxNatLsnSubTcpPortUsqHigh notification is sent when the TCP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

The subscriber is identified with its inside IP address or prefix

tmnxNatNotifyInsideAddr in the inside virtual router instance  
tmnxNatNotifyInsideVRtrID.

#### tmnxNatLsnSubSessionUsgHigh

The tmnxNatLsnSubSessionUsgHigh notification is sent when the session usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false').

The subscriber is identified with its inside IP address or prefix  
tmnxNatNotifyInsideAddr  
in the inside virtual router instance tmnxNatNotifyInsideVRtrID.

#### tmnxNatInAddrPrefixBlksFree

The tmnxNatInAddrPrefixBlksFree notification is sent when all port blocks allocated to one or more subscribers associated with a particular set of inside addresses are released by this system.

The type of subscriber(s) is indicated by tmnxNatNotifySubscriberType.

The set of inside IP addresses is associated with the virtual router instance indicated by tmnxNatNotifyInsideVRtrID and is of the type indicated by tmnxNatNotifyInsideAddrType

The set of inside IP addresses consists of the address prefix indicated with tmnxNatNotifyInsideAddr and tmnxNatNotifyInsideAddrPrefixLen unless these objects are empty and zero; if tmnxNatNotifyInsideAddr is empty and tmnxNatNotifyInsideAddrPrefixLen is zero, the set contains all IP addresses of the indicated type.

The values of tmnxNatNotifyMdaChassisIndex, tmnxNatNotifyMdaCardSlotNum and tmnxNatNotifyMdaSlotNum identify the ISA MDA where the blocks were processed.

All notifications of this type are sequentially numbered with the tmnxNatNotifyPlSeqNum.

This type of notification is typically the consequence of one or more configuration changes; the nature of these changes is indicated in the tmnxNatNotifyDescription.

#### tmnxNatFwd2EntryAdded

[CAUSE] The tmnxNatFwd2EntryAdded notification is sent when a row is added to or removed from the tmnxNatFwd2Table by other means than operations on the tmnxNatFwdAction;  
a conceptual row can be added to or removed from the table by operations on the tmnxNatFwdAction  
object group or otherwise, by means of the PCP protocol  
or automatically by the system, for example when a subscriber profile is changed.  
When the row is added, the value of the object  
tmnxNatNotifyTruthValue is 'true'; when the row is removed,  
it is 'false'.

[EFFECT] The specified NAT subscriber can start receiving inbound traffic flows.

[RECOVERY] No recovery required; this notification is the result of an operator or protocol action.



`tmnxNatDetPlcyOperStateChanged`

[CAUSE] The `tmnxNatDetPlcyOperStateChanged` notification is sent when the value of the object `tmnxNatDetPlcyOperState` changes. The cause is explained in the `tmnxNatNotifyDescription`.

`tmnxNatDetMapOperStateChanged`

[CAUSE] The `tmnxNatDetMapOperStateChanged` notification is sent when the value of the object `tmnxNatDetMapOperState` changes. The cause is explained in the `tmnxNatNotifyDescription`.

`tmnxNatFwd2OperStateChanged`

[CAUSE] The `tmnxNatFwd2OperStateChanged` notification is sent when the value of the object `tmnxNatFwd2OperState` changes. This is related to the state of the ISA MDA where the forwarding entry is located, or the availability of resources on that MDA.

In the case of Layer-2-Aware NAT subscribers, the `tmnxNatFwd2OperState` is 'down' while the subscriber is not instantiated. This would typically be a transient situation.

[EFFECT] The corresponding inward bound packets are dropped while the operational status is 'down'.

[RECOVERY] If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.

### 7.15.1.2 NAT Logging to a Local File

In this case, the destination of log-id 5 in the following example would be a local file instead of memory:

```
*A:left-a20>config>log# info

 file-id 5
 description "nat logging"
 location cf1:
 rollover 15 retention 12
 exit

 log-id 5
 filter 1
 from main
 to file 5
 exit
```

The events will be logged to a local file on the compact flash cf1 in a file under the /log directory.



**Note:** Logging to the compact flash (CF) represents a single point of failure. Performance (logs per second) of logging onto the CF is limited in comparison to other logging methods (RADIUS, Syslog, and IPFIX). Failure to generate logs due to failed a CF or performance limitation will result in dropped NAT traffic. For this reason, local NAT logging in the SR OS is recommended only in a lab environment.

### 7.15.2 SNMP Trap Logging

In case of SNMP logging to a remote node, the log destination should be set to SNMP destination. Allocation de-allocation of each port block will trigger sending a SNMP trap message to the trap destination.

```
*A:left-a20>config>log# info

 filter 1
 default-action drop
 entry 1
 action forward
 match
 application eq "nat"
 number eq 2012
 exit
 exit
 exit
```

```
snmp-trap-group 6
 trap-target "nat" address 192.168.1.10 port 9001 snmpv2c notify-
community "private"
 exit
log-id 6
 filter 1
 from main
 to snmp
 exit
```

```
⊕ Internet Protocol Version 4, Src: 1.1.1.1 (1.1.1.1), Dst: 114.0.1.10 (114.0.1.10)
⊖ User Datagram Protocol, Src Port: snmptrap (162), Dst Port: etlservicemgr (9001)
 Source port: snmptrap (162)
 Destination port: etlservicemgr (9001)
 Length: 358
 ⊕ Checksum: 0x0e2c [correct]
⊖ Simple Network Management Protocol
 version: v2c (1)
 community: private
 ⊖ data: snmpv2-trap (7)
 ⊖ snmpv2-trap
 request-id: 1
 error-status: noError (0)
 error-index: 0
 ⊖ variable-bindings: 14 items
 ⊕ 1.3.6.1.2.1.1.3.0: 19054240
 ⊕ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.6527.3.1.3.65.0.12 (iso.3.6.1.4.1.6527.3.1.3.65.0.12)
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.2.0:
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.4.0:
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.5.0: 50000001
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.8.0: 1894
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.9.0: 1898
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.10.0: 07dc070d00321b002b0000
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.13.0: 1
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.3.0:
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.6.0:
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.7.0: 1a000038
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.11.0:
 ⊕ 1.3.6.1.4.1.6527.3.1.2.65.2.17.0: 5
```

### 7.15.3 NAT Syslog

NAT logs can be sent to a syslog remote facility. A separate syslog message is generated for every port-block allocation/de-allocation.

```
*A:left-a20>config>log#info

...
 filter 1
 default-action drop
 entry 1
 action forward
```

```

 match
 application eq "nat"
 number eq 2012
 exit
 exit
exit
syslog 7
 address 192.168.1.10
exit

log-id 7
 filter 1
 from main
 to syslog 7
exit

```

-----

```

Internet Protocol Version 4, Src: 1.1.1.1 (1.1.1.1), Dst: 114.0.1.10 (114.0.1.10)
User Datagram Protocol, Src Port: syslog (514), Dst Port: syslog (514)
 Source port: syslog (514)
 Destination port: syslog (514)
 Length: 184
 Checksum: 0x3539 [correct]
 [Good Checksum: True]
 [Bad Checksum: False]
Syslog message: LOCAL7.INFO: Jul 13 15:04:53 1.1.1.1 TMNX: 35 Base NAT-INDETERMINATE-tmxNatPBlockAllocationLsn-2012 [NAT]: {45} Map 80.0.0.1 [1994-1998] -- vprn10 26.0.0.56 at 2012,
1011 1... = Facility: LOCAL7 - reserved for local use (23)
.... .110 = Level: INFO - informational (6)
Message: Jul 13 15:04:53 1.1.1.1 TMNX: 35 Base NAT-INDETERMINATE-tmxNatPBlockAllocationLsn-2012 [NAT]: {45} Map 80.0.0.1 [1994-1998] -- vprn10 26.0.0.56 at 2012/07/13 08:04:53\n

```

Severity level for this event can be changed via CLI:

```

*A:left-a20# configure log event-control "nat" 2012 generate
<severity-level>
cleared indeterminate critical major minor warning

```

## 7.15.4 LSN RADIUS Logging

LSN RADIUS logging (or accounting) is based on RADIUS accounting messages as defined in RFC 2866. It requires an operator to have RADIUS accounting infrastructure in place. For that reason, LSN RADIUS logging and LSN RADIUS accounting terms can be used interchangeably.

This mode of logging operation is introduced so that the shared logging infrastructure in 7750 SR can be offloaded by disabling syslog/SNMP/Local-file LSN logging. The result is increased performance and higher scale, particularly in cases when multiple BB-ISA cards within the same system are deployed to perform aggregated LSN functions.

An additional benefit of LSN RADIUS logging over syslog/SNMP/local-file logging is reliable transport. Although RADIUS accounting relies on unreliable UDP transport, each accounting message from the RADIUS client must be acknowledged on the application level by the receiving end (accounting server).

Each port-block allocation or de-allocation is reported to an external accounting (logging) server in the form of start, interim-update or stop messages. The type of accounting messages generated depends on the mode of operation:

- **START and STOP per port-block.** An accounting START is generated when a new port-block for the LSN subscriber is allocated. Similarly, the accounting STOP is generated when the port-block is released. Each accounting START/STOP pair of messages that are triggered by port block allocation/de-allocation within the same subscriber will have the same multi-acct-session-id (subscriber significant) but a different acct-session-id (port-block significant). This mode of operation is enabled by inclusion of multi-acct-session-id within the nat-accounting-policy.
- **START and STOP per subscriber.** An accounting START will be generated when the first port block for the NAT subscriber is allocated. Each consecutive port-block allocation/de-allocation will trigger an INTERIM-UPDATE messages with the same acct-session-id (subscriber significant). The termination cause attribute in acct STOP messages will indicate the reason for port-block de-allocation. De-allocation of the last port-block for the LSN subscriber will trigger an acct STOP message. There is no multi-acct-session-id present in this mode of operation.

The accounting messages are generated and reported directly from the BB-ISA card, therefore bypassing accounting infrastructure residing on the Control Plane Module (CPM).

LSN RADIUS logging is enabled per nat-group. To achieve the required scale, each BB-ISA card in the **nat-group** group with LSN RADIUS logging enabled runs a RADIUS client with its own unique source IP address. Accounting messages can be distributed to up to five accounting servers that can be accessed in round-robin fashion. Alternatively, in direct access mode, only one accounting server in the list is used. When this server fails, the next one in the list is used.

Configuration steps:

1. Configure **isa-radius-policy** under the **configure>aaa** CLI hierarchy. The **isa-radius-policy** command defines:
  - accounting destination
  - inclusion of RADIUS attributes that will be sent in accounting messages to the destination
  - source IP addresses per BB-ISA card (RADIUS client) in the NAT group
2. Apply this policy to the **nat-group**. This will automatically enable RADIUS accounting on every BB-ISA card in the group, provided that each BB-ISA card has an IP address.

```
*A:left-a20>config>aaa>isa-radius-plcy# info detail
description "radius accounting policy for NAT"
include-radius-attribute
 framed-ip-addr
 nas-identifier
 no nat-subscriber-string =>only relevant when subscriber aware NAT is enabled
 user-name
 inside-service-id
 outside-service-id
 outside-ip
 port-range-block
 hardware-timestamp
 release-reason
 multi-session-id
 frame-counters
 octet-counters
 session-time
 called-station-id
 no subscriber-data =>only relevant when subscriber aware NAT is enabled
exit
servers
 access-algorithm direct
 retry 3
 router "Base"
 source-address-range 192.168.1.20
 timeout sec 5
 server 1 create
 accounting
 ip-address 192.168.1.10
 secret "KlWIBi08CxTyM/YXaU2gQitOu8GgfSD7Oj5hjese27A" hash2
exit
```

Each BB-ISA card is assigned one unique IPv4 address from the **source-address-range** command and this IPv4 address must be accessible from the accounting server.

The IP addresses are consecutively assigned to each BB-ISA, starting from the IP address configured by this command. The number of IP addresses allocated internally by the system corresponds to the number of BB-ISAs in the system.

Each BB-ISA is provisioned automatically with the first free IP address available, starting from the IP address that is configured in the **source-address-range** command. Once a BB-ISA is removed from the system (or NAT group), it releases that IP address to be available to the next BB-ISA that comes online within the NAT group.

It is important to be mindful of the internally-allocated IP addresses, since they are not explicitly configured in the system (other than the first IP address in the **source-address-range** command). However, those internally-assigned IP addresses can be seen using show commands in the routing table.

In the following example there is only one BB-ISA card in the nat-group 1. Its source IP address is 192.168.1.20.

```
*A:left-a20# show router route-table
=====
Route Table (Router: Base)
=====
Dest Prefix[Flags] Type Proto Age Pref Next Hop[Interface Name]
Metric

80.0.0.1/
32 Remote NAT 02d18h24m 0 NAT outside: group 1 member 1 0
192.168.1.0/
28 Local Local 02d20h25m 0 radius 0
192.168.1.20/
32 Remote NAT 00h38m29s 0 NAT outside: group 1 member 1 0
```

It is possible to load-balance accounting messages over multiple logging servers by configuring the access-algorithm to round-robin mode. Once the LSN RADIUS accounting policy is defined, it will have to be applied to a nat-group:

```
*A:left-a20>config>isa>nat-group# info

active-mda-limit 1
radius-accounting-policy "nat-acct-basic"
mda 1/2
no shutdown
```

The RADIUS accounting messages for the case where a Large Scale NAT44 subscriber has allocated two port blocks in a logging mode where acct start/stop is generated per port-block is shown below.

Port-blocks allocation for the NAT44 subscriber:

```
Fri Jul 13 09:55:15 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Start
Acct-Multi-Session-Id = "500052cd2edcaeb97c2dad3d7c2dad3d"
Acct-Session-Id = "500052cd2edcaeb96206475d7c2dad3d"
```

```
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "LSN44@10.0.0.58"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.58
Alc-Nat-Outside-Ip-Addr = 198.51.100.1
Alc-Nat-Port-Range = "198.51.100.1 2024-2028 router base"
Acct-Input-Packets = 0
Acct-Output-Packets = 0
Acct-Input-Octets = 0
Acct-Output-Octets = 0
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 0
Event-Timestamp = "Jul 13 2012 09:54:37 PDT"
Acct-Unique-Session-Id = "21c45a8b92709fb8"
Timestamp = 1342198515
Request-Authenticator = Verified

Fri Jul 13 09:55:16 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Start
Acct-Multi-Session-Id = "500052cd2edcaeb97c2dad3d7c2dad3d"
Acct-Session-Id = "500052cd2edcaeb9620647297c2dad3d"
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "LSN44@10.0.0.58"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.58
Alc-Nat-Outside-Ip-Addr = 198.51.100.1
Alc-Nat-Port-Range = "198.51.100.1 2029-2033 router base"
Acct-Input-Packets = 0
Acct-Output-Packets = 5
Acct-Input-Octets = 0
Acct-Output-Octets = 370
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 1
Event-Timestamp = "Jul 13 2012 09:54:38 PDT"
Acct-Unique-Session-Id = "baf26e8a35e31020"
Timestamp = 1342198516
Request-Authenticator = Verified
```

### Port-blocks de-allocation

```
Fri Jul 13 09:56:18 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Stop
Acct-Multi-Session-Id = "500052cd2edcaeb97c2dad3d7c2dad3d"
Acct-Session-Id = "500052cd2edcaeb96206475d7c2dad3d"
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "LSN44@10.0.0.58"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.58
Alc-Nat-Outside-Ip-Addr = 198.51.100.1
Alc-Nat-Port-Range = "198.51.100.1 2024-2028 router base"
```



```
Acct-Terminate-Cause = Port-Unneeded
Acct-Input-Packets = 0
Acct-Output-Packets = 25
Acct-Input-Octets = 0
Acct-Output-Octets = 1850
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 64
Event-Timestamp = "Jul 13 2012 09:55:41 PDT"
Acct-Unique-Session-Id = "21c45a8b92709fb8"
Timestamp = 1342198578
Request-Authenticator = Verified

Fri Jul 13 09:56:20 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Stop
Acct-Multi-Session-Id = "500052cd2edcaeb97c2dad3d7c2dad3d"
Acct-Session-Id = "500052cd2edcaeb9620647297c2dad3d"
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "LSN44@10.0.0.58"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.58
Alc-Nat-Outside-IP-Addr = 198.51.100.1
Alc-Nat-Port-Range = "198.51.100.1 2029-2033 router base"
Acct-Terminate-Cause = Host-Request
Acct-Input-Packets = 0
Acct-Output-Packets = 25
Acct-Input-Octets = 0
Acct-Output-Octets = 1850
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 65
Event-Timestamp = "Jul 13 2012 09:55:42 PDT"
Acct-Unique-Session-Id = "baf26e8a35e31020"
Timestamp = 1342198580
Request-Authenticator = Verified
```

The inclusion of acct-multi-session-id in the NAT accounting policy will enable generation of start/stop messages for each allocation/de-allocation of a port-block within the subscriber. Otherwise, only the first and last port-block for the subscriber would generate a pair of start/stop messages. All port-block in between would trigger generation of interim-update messages.

The User-Name attribute in accounting messages is set to app-name@inside-ip-address, whereas the app-name can be any of the following: LSN44, DS-Lite or NAT64.

### 7.15.4.1 Periodic RADIUS Logging

Currently-allocated NAT resources (such as a public IP address and a port block for a NAT subscriber) can be periodically refreshed via Interim-Update (I-U) accounting messages. This functionality is enabled by the periodic RADIUS logging facility. Its primary purpose is to keep logging information preserved for long-lived sessions in environments where NAT logs are periodically and deliberately deleted from the service provider's network. This is typically the case in countries where privacy laws impose a limit on the amount of time that the information about customer's traffic can be retained/stored in service provider's network.

Periodic RADIUS logging for NAT is enabled by the following command:

```
configure
 aaa
 isa-radius-policy <name> create
 [no] periodic-update interval <hours> [rate-limit <r>]
```

The configurable interval dictates the frequency of I-U messages that are generated for each currently allocated NAT resource (such as a public IP address and a port block).

By default, the I-U messages are sent in rapid succession for a subscriber without any intentional delay inserted by SR OS. For example, a NAT subscriber with 8 NAT policies, each configured with 40 port ranges will generate 320 consecutive I-U messages at the expiration of the configured interval. This can create a surge in I-U message generation in cases where intervals are synchronized for multiple NAT subscribers. This can have adverse effects on the logging behavior. For example, the logging server can drop messages due to its inability to process the high rate of incoming I-U messages.

To prevent this, the rate of I-U message generation can be controlled by a **rate-limit** CLI parameter.

The periodic logging is applicable to both modes of RADIUS logging in NAT:

- Acct-Multi-Session-Id AVP is enabled.
  - In this case, accounting START/STOP messages are generated for each NAT resource (such as a public IP address and a port block) allocation/de-allocation. Acct-multi-session-id and acct-session-id messages in the periodic I-U messages for the currently allocated NAT resource will be inherited from the acct START messages related to the same NAT resource.
- Acct-Multi-Session-Id AVP is disabled.

- In this case, the acct START is generated for the first allocated NAT resource for the subscriber (a public IP address and a port block) and the acct STOP message is generated when the last NAT resource for the subscriber is released. All of the in-between port block allocations for the same subscriber will trigger I-U messages with the same acct-session-id as the one contained in the acct START message. To differentiate between the port-block allocations, releases and updates within the I-U messages for the same NAT subscriber, the Alc-Acct-Triggered-Reason AVP will be included in every periodic I-U message. Sending the Alc-Acct-Triggered-Reason AVP is configuration dependent (enabled in the **isa-radius-policy>acct-include-attributes** context).
- The supported values for Alc-Acct-Triggered-Reason AVP in I-U messages will be:
  - Alc-Acct-Triggered-Reason=Nat-FREE (19) Generated when the port-block is released.
  - Alc-Acct-Triggered-Reason=Nat-MAP (20) Generated when the port-block is allocated.
  - Alc-Acct-Triggered-Reason = Nat-UPDATE (21) Generated during periodically scheduled I-U update.

The log for each port-block periodic update is carried in a separate I-U message.

#### 7.15.4.1.1 Message Pacing

Periodic I-U message output can be paced in order to avoid congestion at the logging server. Pacing is controlled by the **rate-limit** option of the **periodic-update** command.

As an example, consider the following hypothetical case:

- 1 million NAT subscribers came up within 1 hour (16,666 NAT-subs per minute).
- On average, each NAT subscriber allocates two port blocks.
- This means that 2 million logs will be sent to the logging server.
- If the **rate-limit** value is set to 100 (messages per second), on average it would take over 5 hours to send all those messages at the given rate.
- In this case, it would be prudent to set the interval value to at least 6 hours, or increase the **rate-limit** value so there is no time overlap between the old and new logs.

In case of an MS-ISA switchover or a NAT multi-chassis redundancy switchover, there is a chance that a large number of subscribers will become active at approximately the same time on the newly active MS-ISA (or chassis). This will cause a large number of logs to be sent in a relatively short amount of time, which may overwhelm the logging server. The **rate-limit** parameter is designed to help in such situations.

### 7.15.4.2 RADIUS Logging and L2-Aware NAT

Logging of L2-Aware NAT is supported via accounting policy associated with the ESM subscriber (outside of NAT). In addition to ESM subscriber specific attributes, the NAT port-ranges and outside IP address (**nat-port-range** command in regular ESM accounting policy) are reported in the same accounting messages.

```
Fri Jul 13 11:57:38 2012
 Acct-Status-Type = Start
 NAS-IP-Address = 10.1.1.1
 User-Name = "l2-aware-nat"
 Framed-IP-Address = 198.51.100.100
 Framed-IP-Netmask = 255.255.255.0
 Class = 0x6c322d61776172652d636c737373
 Calling-Station-Id = "remote-l2-aware0"
 NAS-Identifier = "left-a20"
 Acct-Session-Id = "D896FF0000001150006F7C"
 Event-Timestamp = "Jul 13 2012 11:57:00 PDT"
 NAS-Port-Type = Ethernet
 NAS-Port-Id = "1/1/5:5.13"
 ADSL-Agent-Circuit-Id = "l2-aware-nat"
 ADSL-Agent-Remote-Id = "remote-l2-aware0"
 Alc-Subsc-ID-Str = "l2-aware-1"
 Alc-Subsc-Prof-Str = "l2-aware-nat"
 Alc-SLA-Prof-Str = "tp_sla_prem"
 Alc-Nat-Port-Range = "10.0.0.1 1024-1079 router base"
 Alc-Client-Hardware-Addr = "2001:db8:65:05:13:01"
 Acct-Delay-Time = 0
 Acct-Authentic = RADIUS
 Acct-Unique-Session-Id = "6bbbd5a110313b47"
 Timestamp = 1342205858
 Request-Authenticator = Verified
```

RADIUS accounting initiated by BB-ISA card is not supported for L2-Aware NAT.

Syslog/SNMP/Local-file logging can be enabled simultaneously with L2-Aware NAT RADIUS accounting (which is in this case regular ESM RADIUS accounting).

## 7.15.5 LSN and L2-Aware NAT Flow Logging

LSN and L2-aware NAT flow logging allows each BB-ISA card to export the creation and deletion of NAT flows to an external server. A NAT flow, or a Fully Qualified Flow, consists of the following parameters: inside IP, inside port, outside IP, outside port, foreign IP, foreign port, and protocol (UDP, TCP, ICMP).

```
Owner : LSN-Host@10.10.10.101
Router : 1
Policy : mnp
FlowType : UDP
Inside IP Addr : 10.10.10.101
Inside Port : 20001
Outside IP Addr : 192.168.20.28
Outside Port : 2001
Foreign IP Addr : 192.168.5.4
Foreign Port : 20001
Dest IP Addr : 192.168.5.4
Nat Group : 1
Nat Group Member : 1
```

The foreign IP address is the original IPv4 destination address as received by NAT on the inside. The destination IP address is the translated foreign IP address if that destination NAT is active (the destination NAT translates the destination IPv4 address of the packet).

Additional information, such as the inside or outside service ID and subscriber string, can be added to a flow record.

Flow logging can be deployed as an alternative to port-range logging or can be complementary (providing a more granular log for offline reporting or compliance). Certain operators have legal and compliance requirements that require extremely detailed logs, created per flow, to be exportable from the NAT node.

Because the setup rate of new flows is excessive, logging to an internal facility (like compact flash) is not possible except in debugging mode (which must specify match criteria down to the inside IP and service level).

Flow logging can be enabled on a per-NAT policy basis and, consequently, it is initiated from each BB-ISA card. The flow records can be exported to an external collector in an IPFIX format or a syslog format, both of which use UDP as the transport protocol. These UDP streams are stateless due to the significant volume of transactions. However they do contain sequence numbers so packet loss can be identified. They egress the chassis at the **fc nc**.

IPFIX and SYSLOG flow logging are configured using respective flow logging policies (such as **ipfix-export-policy** and **syslog-export-policy**). Each flow logging policy supports two destinations (collectors). One **ipfix-export-policy** and one **syslog-export-policy** can be used simultaneously in any one NAT group.

### 7.15.5.1 IPFIX Flow Logging

IPFIX defines two different types of messages that are sent from the IPFIX exporter (SR OS NAT node). The first contains a template set which is an IPFIX message that defines fields for subsequent IPFIX messages but contains no actual data of its own. The second IPFIX message type contains data sets. Here, the data is passed using the previous template set message to define the fields. This means an IPFIX message is not passed as sets of TLV, but instead, data is encoded with a scheme defined through the template set message.

While an IPFIX message can contain both a template set and data set, the SR OS node sends template set messages periodically without any data, whereas the data set messages are sent on demand and as required. When IPFIX is used over UDP, the default retransmission frequency of the template set messages defaults to 10 minutes. The interval for retransmission is configurable in CLI with a minimum interval of one minute and a maximum interval of 10 minutes. When the exporter first initializes, or when a configuration change occurs, the template set is sent out three times, one second apart. Templates are sent before any data sets, assuming that the collector is enabled, so that an IPFIX collector can establish the data template set.

Although the UDP transport is unreliable, the IPFIX sequence number is a 32-bit number that contains the total number of IPFIX data records sent for the UDP transport session prior to the receipt of the new IPFIX message. The sequence number starts with 0 and rolls over once it reaches 4,294,967,268.

The default packet size is 1500 bytes unless another value has been defined in the configuration (the range is 512 bytes through 9212 bytes inclusively). Traffic is originated from a random high port to the collector on port 4739. Multiple create and delete flow records are stuffed into a single IPFIX packet (although the mappings created are not delayed) until stuffing an additional data record would exceed MTU or a timer expires. The timer is not configurable and is set to 250 milliseconds (that is, should any mapping occur, a packet is sent within 250 milliseconds of that mapping being created)

Each collector has a 50-packet buffering space. If, due to excessive logging, the buffering space becomes unavailable, new flows are denied and the deletion of flows is delayed until buffering space becomes available.

Two collector nodes can be defined in the same IPFIX export policy for redundancy purposes.

### 7.15.5.2 Template Formats

The SR OS supports two data formats. Their selection is controlled through CLI:

```
configure
 service
 ipfix
 ipfix-export-policy <name> [create]
 template-format {format1|format2}
```

The difference between the two formats is related to the fields conveying information about the translated source IP addresses and ports (outside IP addresses and ports).

Format1 carries information about translated (outside) IP address in the sourceIPv4Address information element while in format2 this information element is replaced by the postNATSourceIPv4Address. Further, format1 does not convey any information about the translated source port (post-NAT) while a new information element postNAPTsourceTransportPort is introduced in format2 to carry this information.

Both formats use proprietary information element AluNatSubString carrying the original source IP address, before NAT is performed.

The template and data sets are formatted according to RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

Standardized data fields are defined in RFC 5102, *Information Model for IP Flow Information Export*, and in IANA registry <https://www.iana.org/assignments/ipfix/ipfix.xhtml#ipfix-information-elements>.

In addition to standardized data fields, IPFIX supports vendor-proprietary data fields which contains an Enterprise Number specific to each vendor.

The supported information elements and their description for each format is provided in Table 41. EN in Table 41 stands for Enterprise Number (0 = IETF, 637 = Nokia) and IE-Id represents Information Element Identifier.

**Table 41** IPFIX Fields and Formats

| Field                      | EN, IE-Id | Format 1                                                                                                                                                                                                | Format 2                                                                                                                                                                                                |
|----------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| flowId                     | 0, 148    | A unique (per-observation domain ID) ID for this flow. Used for tracking purposes only (opaque value). The flow ID in a create and a delete mapping record must be the same for a specific NAT mapping. | A unique (per-observation domain ID) ID for this flow. Used for tracking purposes only (opaque value). The flow ID in a create and a delete mapping record must be the same for a specific NAT mapping. |
| sourceIPv4Address          | 0, 8      | The outside (translated) IP address used in the NAT mapping.<br>In format2, this is replaced by postNATSourceIPv4Address.                                                                               | N/A                                                                                                                                                                                                     |
| postNATSourceIPv4Address   | 0, 255    | N/A                                                                                                                                                                                                     | The outside (translated) IP address used in the NAT mapping.<br>This replaces the sourceIPv4Address field from format1.                                                                                 |
| destinationIPv4Address     | 0, 12     | The foreign or remote IP address used in the NAT mapping.                                                                                                                                               | The foreign or remote IP address used in the NAT mapping.                                                                                                                                               |
| sourceTransportPort        | 0, 7      | The outside (translated) source port used in the NAT mapping.                                                                                                                                           | This is the original source port (before NAT translation) on the inside                                                                                                                                 |
| postNAPTsourceTrasportPort | 0, 227    | N/A                                                                                                                                                                                                     | The outside (translated) source port used in the NAT mapping                                                                                                                                            |
| destinationTransportPort   | 0, 11     | The destination port used in the NAT mapping.                                                                                                                                                           | The destination port used in the NAT mapping.                                                                                                                                                           |
| flowStartMillisisends      | 0, 152    | The timestamp of when the flow was created (chassis NTP derived) in milliseconds from epoch.                                                                                                            | The timestamp of when the flow was created (chassis NTP derived) in milliseconds from epoch.                                                                                                            |
| flowEndMilliseconds        | 0, 153    | The timestamp of when the flow was destroyed (chassis NTP derived) in milliseconds from epoch.                                                                                                          | The timestamp of when the flow was destroyed (chassis NTP derived) in milliseconds from epoch.                                                                                                          |



**Table 41 IPFIX Fields and Formats (Continued)**

| Field               | EN, IE-Id | Format 1                                                                                                                                                                                                                                                                                                                                                                                                          | Format 2                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| protocolIdentifier  | 0, 4      | Protocol (UDP, TCP, ICMP)                                                                                                                                                                                                                                                                                                                                                                                         | Protocol (UDP, TCP, ICMP)                                                                                                                                                                                                                                                                                                                                                                                         |
| flowEndReason       | 0, 136    | <p>The reasons for flow termination. The following Flow End Reasons are supported:</p> <ul style="list-style-type: none"> <li>• 0x01: Idle Timeout. A mapping expired (because of UDP or TCP timeout)</li> <li>• 0x03: end of Flow Detected. A mapping closed (only used for TCP after a FIN or RST).</li> <li>• 0x04: forced end. Collects all other reasons included administrative or failure case.</li> </ul> | <p>The reasons for flow termination. The following Flow End Reasons are supported:</p> <ul style="list-style-type: none"> <li>• 0x01: Idle Timeout. A mapping expired (because of UDP or TCP timeout)</li> <li>• 0x03: end of Flow Detected. A mapping closed (only used for TCP after a FIN or RST).</li> <li>• 0x04: forced end. Collects all other reasons included administrative or failure case.</li> </ul> |
| paddingOctets       | 0, 210    | Padding                                                                                                                                                                                                                                                                                                                                                                                                           | N/A                                                                                                                                                                                                                                                                                                                                                                                                               |
| aluInsideServiceId  | 637, 91   | The 16-bit service ID representing the inside service ID. This field is not applicable in L2-aware NAT and is set to NULL in this case.                                                                                                                                                                                                                                                                           | The 16-bit service ID representing the inside service ID. This field is not applicable in L2-aware NAT and is set to NULL in this case.                                                                                                                                                                                                                                                                           |
| aluOutsideServiceId | 637, 92   | The 16-bit service ID representing the outside service ID.                                                                                                                                                                                                                                                                                                                                                        | The 16-bit service ID representing the outside service ID.                                                                                                                                                                                                                                                                                                                                                        |
| aluNatSubString     | 637, 93   | <p>A variable 8B aligned string that represents the NAT subscriber construct (as currently used in the <b>tools&gt;dump&gt;service&gt;nat&gt;session</b> commands). The original IP source address, before NAT is performed is included in this string.</p> <p>For example:<br/>LSN-Host@10.10.10.101</p>                                                                                                         | <p>A variable 8B aligned string that represents the NAT subscriber construct (as currently used in the <b>tools&gt;dump&gt;service&gt;nat&gt;session</b> commands). The original IP source address, before NAT is performed is included in this string.</p> <p>For example:<br/>LSN-Host@10.10.10.101</p>                                                                                                         |

### 7.15.5.3 Template Format1 and Format2

Table 42 and Table 43 show information elements that are present in data sets during flow creation and deletion for the two formats. Each template set carries a unique template ID that is used to match the corresponding data set that carries the same ID in the set header (Set Id field).

**Table 42**      **Template Format 1**

| Flow Creation Template Set |          | Flow Deletion Templates Set |          |
|----------------------------|----------|-----------------------------|----------|
| Description                | Size (B) | Description                 | Size (B) |
| flowId                     | 8        | flowId                      | 8        |
| sourceIPv4Address          | 4        | sourceIPv4Address           | 4        |
| destinationIPv4Address     | 4        | destinationIPv4Address      | 4        |
| sourceTransportPort        | 2        | sourceTransportPort         | 2        |
| destinationTransportPort   | 2        | destinationTransportPort    | 2        |
| flowStartMilliseconds      | 8        | flowEndMilliseconds         | 8        |
| protocolIdentifier         | 1        | protocolIdentifier          | 1        |
| paddingOctets              | 1        | flowEndReason               | 1        |
| aluInsideServiceID         | 2        | aluInsideServiceID          | 2        |
| aluOutsideServiceID        | 2        | aluOutsideServiceID         | 2        |
| aluNatSubString            | var      | aluNatSubString             | var      |

**Table 43**      **Template Format 2**

| Flow Creation Template Set  |          | Flow Deletion Templates Set |          |
|-----------------------------|----------|-----------------------------|----------|
| Description                 | Size (B) | Description                 | Size (B) |
| flowId                      | 8        | flowId                      | 8        |
| postNATSourceIPv4Address    | 4        | postNATSourceIPv4Address    | 4        |
| destinationIPv4Address      | 4        | destinationIPv4Address      | 4        |
| sourceTransportPort         | 2        | sourceTransportPort         | 2        |
| postNAPTSourceTransportPort | 2        | postNAPTSourceTransportPort | 2        |
| destinationTransportPort    | 2        | destinationTransportPort    | 2        |

**Table 43**      **Template Format 2 (Continued)**

| Flow Creation Template Set |          | Flow Deletion Templates Set |          |
|----------------------------|----------|-----------------------------|----------|
| Description                | Size (B) | Description                 | Size (B) |
| flowStartMilliseconds      | 8        | protocolIdentifier          | 1        |
| protocolIdentifier         | 1        | flowEndReason               | 1        |
| paddingOctets              | 1        | flowEndMilliseconds         | 8        |
| aluInsideServiceID         | 2        | aluInsideServiceID          | 2        |
| aluOutsideServiceID        | 2        | aluOutsideServiceID         | 2        |
| aluNatSubString            | var      | aluNatSubString             | var      |

### 7.15.5.4 Configuration Example

Large Scale NAT44 Flow Logging with Format2:

1. A collector node along with other local transport parameters must be defined through an IPFIX export policy.

```
*A:BNG1>config>service>ipfix# info detail

 ipfix-export-policy "flow-logging" create
 no description
 template-format format2
 collector router "Base" ip 192.168.115.1 create
 mtu 1500
 source-address 192.0.2.2
 template-refresh-timeout min 5
 no shutdown
 exit
exit
```

To export flow records using UDP stream, the BB-ISA card must be configured with an appropriate IPv4 address within a designated VPRN. This address (/32) acts as the source for sending all IPFIX records and is shared by all ISA.

2. Once the IPFIX export policy is defined, it must be applied within the NAT policy:

```
*A:BNG1>config>service>nat# info

 nat-policy "mnp" create
 pool "mnp" router Base
 ipfix-export-policy "flow-logging"
exit
```

Flow creation and flow deletion templates for format2, as captured in Wireshark, are shown in [Figure 69](#).

**Figure 69**      **Format2 Templates**

```

Cisco NetFlow/IPFIX
 Version: 10
 Length: 148
 Timestamp: Oct 31, 2017 04:33:36.000000000 central Daylight Time
 FlowSequence: 0
 Observation Domain Id: 1179650
 Set 1
 FlowSet Id: Data Template (v10 [IPFIX]) (2)
 FlowSet Length: 64
 Template (Id = 256, Count = 11)
 Template Id: 256
 Field Count: 11
 Field (1/11): flowId
 Field (2/11): postNATSourceIPv4Address
 Field (3/11): IP_DST_ADDR
 Field (4/11): L4_SRC_PORT
 Field (5/11): postNAPTSourceTransportPort
 Field (6/11): L4_DST_PORT
 Field (7/11): flowStartMilliseconds
 Field (8/11): PROTOCOL
 Field (9/11): 91 [pen: Alcatel-Lucent (previously was 'Alcatel Data Network')]
 Field (10/11): 92 [pen: Alcatel-Lucent (previously was 'Alcatel Data Network')]
 Field (11/11): 93 [pen: Alcatel-Lucent (previously was 'Alcatel Data Network')]
 Set 2
 FlowSet Id: Data Template (v10 [IPFIX]) (2)
 FlowSet Length: 68
 Template (Id = 257, Count = 12)
 Template Id: 257
 Field Count: 12
 Field (1/12): flowId
 Field (2/12): postNATSourceIPv4Address
 Field (3/12): IP_DST_ADDR
 Field (4/12): L4_SRC_PORT
 Field (5/12): postNAPTSourceTransportPort
 Field (6/12): L4_DST_PORT
 Field (7/12): PROTOCOL
 Field (8/12): flowEndReason
 Field (9/12): flowEndMilliseconds
 Field (10/12): 91 [pen: Alcatel-Lucent (previously was 'Alcatel Data Network')]
 Field (11/12): 92 [pen: Alcatel-Lucent (previously was 'Alcatel Data Network')]
 Field (12/12): 93 [pen: Alcatel-Lucent (previously was 'Alcatel Data Network')]

```

IPFIX flow creation data set, as captured in Wireshark, is shown in [Figure 70](#).

**Figure 70 Flow Creation Data Set**

```

Cisco NetFlow/IPFIX
Version: 10
Length: 74
Timestamp: Oct 30, 2017 20:33:45.000000000 Central Daylight Time
FlowSequence: 0
Observation Domain Id: 1179650
Set 1
 FlowSet Id: (Data) (256)
 FlowSet Length: 58
 Flow 1
 Flow Id: 216172784529768566
 Post NAT Source IPv4 Address: 192.168.20.24 (192.168.20.24)
 DstAddr: 192.168.5.4 (192.168.5.4)
 SrcPort: 20001
 Post NAT Source Transport Port: 2003
 DstPort: 20001
 Protocol: 17
 Enterprise Private entry: (Alcatel-Lucent (previously was 'Alcatel Data Network')) Type 91: value (hex bytes): 00 01
 Enterprise Private entry: (Alcatel-Lucent (previously was 'Alcatel Data Network')) Type 92: value (hex bytes): 00 00
 [Enterprise Private entry: (Alcatel-Lucent (previously was 'Alcatel Data Network')) Type 93: value (hex bytes): 4c 53
 String_len_short: 18
 StartTime: Oct 31, 2017 04:33:45.460000000 Central Daylight Time

```

IPFIX flow destruction data set, as captured in Wireshark, is shown in [Figure 71](#).

**Figure 71 Flow Destruction**

```

Cisco NetFlow/IPFIX
Version: 10
Length: 75
Timestamp: Oct 30, 2017 20:35:53.000000000 Central Daylight Time
FlowSequence: 1
Observation Domain Id: 1179650
Set 1
 FlowSet Id: (Data) (257)
 FlowSet Length: 59
 Flow 1
 Flow Id: 216172784529768566
 Post NAT Source IPv4 Address: 192.168.20.24 (192.168.20.24)
 DstAddr: 192.168.5.4 (192.168.5.4)
 SrcPort: 20001
 Post NAT Source Transport Port: 2003
 DstPort: 20001
 Protocol: 17
 Flow End Reason: Idle timeout (1)
 Enterprise Private entry: (Alcatel-Lucent (previously was 'Alcatel Data Network')) Type 91: value (hex bytes): 00 01
 Enterprise Private entry: (Alcatel-Lucent (previously was 'Alcatel Data Network')) Type 92: value (hex bytes): 00 00
 [Enterprise Private entry: (Alcatel-Lucent (previously was 'Alcatel Data Network')) Type 93: value (hex bytes): 4c 53
 String_len_short: 18
 EndTime: Jan 4, 1973 14:48:48.103230848 Central standard Time

```

### 7.15.5.5 Syslog Flow Logging

The format of syslog messages for NAT flow logging in SR OS adheres to RFC 3164, *The BSD Syslog Protocol*:

<PRI> <HEADER><MSG>

where:

- <PRI> (the “<” and “>” are included in the syslog message) is the configured facility\*8+severity (as described in the *7450 ESS*, *7750 SR*, *7950 XRS*, and *VSR System Management Guide* and RFC 3164).
- <HEADER> defines the MMM DD HH:MM:SS <hostname>. Two characters always appear for the day (DD) field. Single-digit days are preceded with a space character. Time is recorded as local time (and not UTC). The time zone designator is not shown in this example, but each event has its own timestamp where the time-zone designator is shown.
- <MSG> defines the <log-prefix>: <seq> <application [<subject>]: <message>\n

where:

- <log-prefix> is an optional 32-character string of text (default = 'TMNX') as configured in the **log-prefix** command.
- <seq> is the log event sequence number (always preceded by a colon and a space char).
- The [<subject>] field may be empty resulting in []:
- <message> display a custom message relevant to the log event.
- \n is the standard ASCII new line character (hex 0A).

**Table 44 Syslog Message Fields for NAT Flow Logging**

| Field Name                                                                           | Value                                                                                 | Comments                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PRI <ul style="list-style-type: none"> <li>• severity</li> <li>• facility</li> </ul> | <ul style="list-style-type: none"> <li>• Default: 6</li> <li>• Default: 16</li> </ul> | <ul style="list-style-type: none"> <li>• Configurable</li> <li>• Configurable</li> </ul>                                                                                                                                      |
| Timestamps                                                                           | MMM DD<br>HH:MM:SS                                                                    |                                                                                                                                                                                                                               |
| <hostname>                                                                           |                                                                                       | The IP address of the SR OS system that is generating the message.                                                                                                                                                            |
| <log-prefix>                                                                         |                                                                                       | Configurable. This can be used as a field to differentiate between the vendors. For example, NOK(ia) in log-prefix indicates that this is a log format from a Nokia node so the operator can apply parsing logic accordingly. |
| <seq>                                                                                |                                                                                       | Sequence numbers can be used for tracking if loss in transit occurs.                                                                                                                                                          |

**Table 44 Syslog Message Fields for NAT Flow Logging (Continued)**

| Field Name    | Value  | Comments                                                                     |
|---------------|--------|------------------------------------------------------------------------------|
| <application> | NAT    | The application that generated the log.                                      |
| [<subject>]:  | MDA ID | The BB-ISA on which the event occurred.                                      |
| <message>     |        | This is a custom part with specific information related to the event itself. |

The message portion contains information relevant to the respective log event, even if this information is already repeated outside of the message (for example, timestamp). The fields in the message part are separated by a single whitespace for easier parsing and are placed in the order shown [Table 45](#).

**Table 45 Message Fields**

| Field Name    | Value                                                                                                                                                            | Presence    | Comments                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAT type      | LSN44<br>NAT64                                                                                                                                                   | M(andatory) |                                                                                                                                                                                                                                                                                           |
| Event name    | SADD<br>SDEL                                                                                                                                                     | M           | SADD – session added event<br>SDEL – session deleted event                                                                                                                                                                                                                                |
| Timestamp     | <TimeStamp>:<br><Year> <Mon> <Day><br><hh:mm:ss:cs> <TZ>,<br>Year is 4-digit, Mon is<br>3-letter abbreviation,<br>TZ is a 1-5 character<br>time-zone designator. | M           | Since events can be combined in the same syslog message, each event is uniquely timestamped with the local time (not UTC), including the time zone designator. During daylight saving's time (summer), the time zone designator is replaced by the DST designator, which is configurable. |
| Protocol ID   | 1, 6, 17                                                                                                                                                         | M           | ICMP, UDP, TCMP                                                                                                                                                                                                                                                                           |
| Inside router | 0 to 2147483650                                                                                                                                                  | M           | 0 represents Base<br>1 to 2147483650 represents<br>VPRNs                                                                                                                                                                                                                                  |

**Table 45**      **Message Fields (Continued)**

| Field Name                                 | Value                                           | Presence   | Comments                                                                                                                                                |
|--------------------------------------------|-------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source IP address                          | IPv4 address in LSN44 and IPv6 address in NAT64 | M          |                                                                                                                                                         |
| Source port or ICMP identifier             | 0 to 65535                                      | M          |                                                                                                                                                         |
| Outside router                             | 0 to 2147483650                                 | M          |                                                                                                                                                         |
| Outside (post NAT) IP address              | IPv4 address                                    | M          |                                                                                                                                                         |
| Outside (post NAT) port or ICMP identifier | 0 to 65535                                      | M          |                                                                                                                                                         |
| Foreign IP address                         | IPv4 address                                    | O(ptional) | This is the original destination IPv4 address.                                                                                                          |
| Foreign port or ICMP identifier            | 0 to 65535                                      | O          |                                                                                                                                                         |
| Destination IP address                     | IPv4 address                                    | O          | It represents the translated destination IP address.                                                                                                    |
| Nat-policy                                 | <name>                                          | O          |                                                                                                                                                         |
| Sub-ID                                     | <sub-name>                                      | O          | “-” if requested by the configuration (includes the sub-id statement) but the sub-aware NAT is not enabled. Otherwise, the sub-ID in the sub-aware NAT. |

#### 7.15.5.5.1 Sequence Numbers

Each syslog message contains a sequence number. The sequence numbers are independently generated by each BB-ISA per collector, and they are monotonically increased by 1. The MDA ID carried in the syslog message is used to differentiate between the overlapping sequence numbers generated by different BB-ISAs in the same NAT group.



### 7.15.5.5.2 Timestamp

Each flow creation or deletion event is timestamped individually using the local time in the system. The event timestamp (including the time-zone designator) is carried in the message part of the log. This timestamp is carried in addition to the syslog timestamp which is generated at the time of syslog message generation and carried in the <HEADER> part of the syslog messages.

### 7.15.5.5.3 Event Aggregation

By default, flow logging events are transported to the collector as fast as they are generated. This does not imply that each event is transported individually, instead a few events can be still aggregated in a single message. However, this aggregation is not user controllable and it depends on the current condition in the system (events that are generated at approximately the same time).

To further optimize transport of logging events to the collector, the events can be aggregated in a controlled fashion. The flow logging events can be aggregated based on:

- Expiry of a configurable timer
- Transport message size — Logs are collected until the size of the syslog message reaches the MTU size

Whichever of the two conditions is met first will trigger the generation of a syslog frame carrying multiple events. The separating character between the logs in a syslog message is “|” surrounded by a whitespace on each side.

```
<186>Jan 11 18:51:22 135.221.38.108 NOK: 47 NAT [MDA 1/1]: NAT44 SADD 2017
Jan 11 18:51:22:50 PST 6 0 10.10.10.1 3000 20 11.11.11.11 5000 12.12.12.12 8000
pol-name-1 sub-1 | NAT44 SADD 2017 Jan 11 18:51:22:60 PST 6 0 10.10.10.2 4000
20 11.11.11.11 6000 13.13.13.13 9000 pol-name-1 sub-1\n
```

### 7.15.5.5.4 Syslog Transmission Rate Limit and Overload Conditions

The transmission rate of syslog messages can be limited by configuration. The rate limit is enforced in packets-per-seconds (pps). Once the rate limit is exceeded, NAT flow logs are buffered. An overload condition is characterized by exhaustion of this buffer space. This condition can occur due to imposed rate limit or the software speed limit. Once the buffer space is exhausted, new flow creation is denied, and the teardown of the existing flows are delayed until the buffer space becomes available. Rate limit determines how fast the buffers are freed (by sending packets to the collector).

## 7.16 DS-Lite and NAT64 Fragmentation

### 7.16.1 Overview

In general, fragmentation functionality is invoked when the size of a fragmentation eligible packet exceeds the size of the MTU of the egress interface/tunnel. Packets eligible for fragmentation are:

- IPv4 packets/fragments with the DF bit in the IPv4 header cleared. Fragmentation can be performed on any routing node between the source and the destination of the packet.
- IPv6 packets on the source node. Fragmentation of IPv6 packet on the transient routing nodes is not allowed.

The best practice is to avoid fragmentation in the network by ensuring adequate MTU size on the transient/source nodes. Drawbacks of the fragmentation are:

- Increased processing and memory demands to the network nodes (especially during reassembly process)
- Increased byte overhead
- Increased latency.

Fragmentation can be particularly deceiving in a tunneled environment whereby the tunnel encapsulation adds extra overhead to the original packet. This extra overhead could tip the size of the resulting packet over the egress MTU limit.

Fragmentation could be one solution in cases where the restriction in the mtu size on the packet's path from source to the destination cannot be avoided. Routers support IPv6 fragmentation in DS-Lite and NAT64 with some enriched capabilities, such as optional packet IPv6 fragmentation even in cases where DF-bit in corresponding IPv4 packet is set.

In general, the lengths of the fragments must be chosen such that resulting fragment packets fit within the MTU of the path to the packets destinations.

In downstream direction fragmentation can be implemented in two ways:

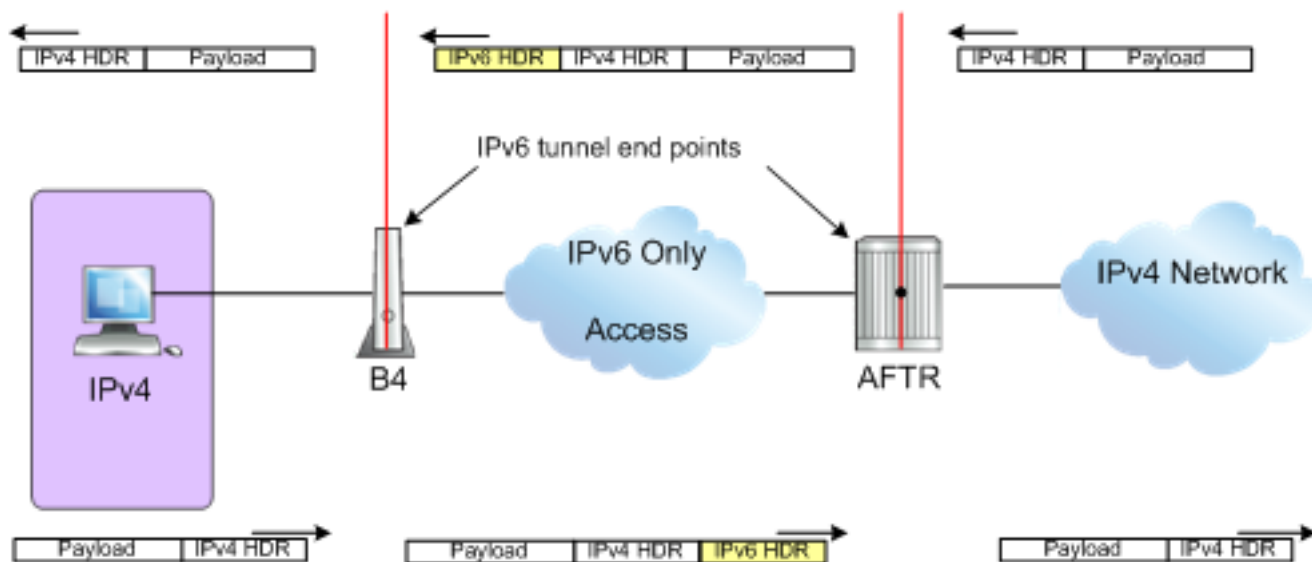
- IPv4 packet can be fragmented in the carrier IOM before it reaches ISA for any NAT function.
- IPv6 packet can be fragmented in the ISA, once the IPv4 packet is IPv6 encapsulated in DS-lite or IPv6 translated in NAT64.

In upstream direction, IPv4 packets can be fragmented once they are decapsulated in DS-lite or translated in NAT64. The fragmentation will occur in the IOM.

## 7.16.2 IPv6 Fragmentation in DS-Lite

In the downstream direction, the IPv6 packet carrying IPv4 packet (IPv4-in-IPv6) is fragmented in the ISA in case the configured DS-lite tunnel-mtu is smaller than the size of the IPv4 packet that is to be tunneled inside of the IPv6 packet. The maximum IPv6 fragment size will be 48bytes larger than the value set by the tunnel-mtu. The additional 48 bytes is added by the IPv6 header fields: 40 bytes for the basic IPv6 header + 8 bytes for extended IPv6 fragmentation header. NAT implementation in the routers does not insert any extension IPv6 headers other than fragmentation header.

**Figure 72 DS-Lite**



In case that the IPv4 packet is larger than the value set by the tunnel-mtu, the fragmentation action will depend on the configuration options and the DF bit setting in the header of the received IPv4 header:

- The IPv4 packet can be dropped regardless of the DF bit setting. IPv6 fragmentation is disabled.
- The IPv4 packet can be encapsulated in IPv6 packet and then the IPv6 can be fragmented regardless of the DF bit setting in the IPv4 tunneled packet. The IPv6 fragment payload is limited to the value set by the tunnel-mtu.

- The IPv4 packet can be encapsulated in IPv6 packet and then the IPv6 can be fragmented only if the DF bit is cleared. The IPv6 fragment payload is limited to the value set by the tunnel-mtu.

In case that the IPv4 packet is dropped due to fragmentation not being allowed, an ICMPv4 Datagram Too Big message will be returned to the source. This message will carry the information about the size of the MTU that is supported, in essence notifying the source to reduce its MTU size to the requested value (tunnel-mtu).

The maximum number of supported fragments per IPv6 packet is 8. Considering that the minimum standard based size for IPv6 packet is 1280bytes, 8 fragments is enough to cover jumbo Ethernet frames.

```
configure
[router] | [service vprn]
 nat
 inside
 dual-stack-lite
address <IPv6 Addr>
 tunnel-mtu bytes
 ip-fragmentation {disabled | fragment-ipv6 | fragment-ipv6-unless-
ipv4-df-set}
```

### 7.16.3 NAT64

Downstream fragmentation in NAT64 works in similar fashion. The difference between DS-lite is that in NAT64 the configured ipv6-mtu represents the mtu size of the ipv6 packet (as opposed to payload of the IPv6 tunnel in DS-lite). In addition, IPv4 packet in NAT64 is not tunneled but instead IPv4/v6 headers are translated. Consequently, the fragmented IPv6 packet size will be 28bytes larger than the translated IPv4 packet ? 20bytes difference in basic IP header sizes (40bytes IPv6 header vs 20byte IPv4 header) plus 8 bytes for extended fragmentation IPv6 header. The only extended IPv6 header that NAT64 generates is the fragmentation header.

In case that the IPv4 packet is dropped due to the fragmentation not being allowed, the returned ICMP message will contain MTU size of ipv6-mtu minus 28 bytes.

Otherwise the fragmentation options are the same as in DS-lite.

```
configure
[router] | [service vprn]
 nat
 inside
 nat64
 ipv6-mtu bytes
 ip-fragmentation {disabled | fragment-ipv6 | fragment-ipv6-unless-ipv4-
df-set}
```

## 7.17 DS-lite Reassembly

In a tunneled environment, such as DS-Lite, a fragmented packet must be reassembled in the end node before it is decapsulated. DS-Lite reassembly is implemented in-line, which means that the reassembly function runs in the same MS-ISA where native DS-Lite processing occurs. The presence of the Fragment Extension header in the IPv6 header signals the need for reassembly for all traffic destined to the AFTR in the upstream direction.

Fragments of a frame can be buffered for up to two seconds in an MS-ISA to wait for all the fragments of the original frame to arrive can be reassembled.

DS-Lite reassembly is performed only in the upstream direction.

### 7.17.1 Interpreting Fragmentation Statistics

Fragmentation statistics in DS-lite can be observed by issuing the following command:

**show isa nat-group <grp-id> mda <slot-id/mda-id> statistics**

The command output displays only relevant DS-lite fragmentation counters are shown. The remaining counters are removed from the output for easier reading.

```
show isa nat-group 1 mda 1/2 statistics
=====
ISA NAT Group 1 MDA 1/2
=====
--snip--
too many fragments for IP packet : 0
too many fragmented packets : 0
too many fragment holes : 0
too many frags buffered : 0
fragment list expired : 0
Reassembly Failures : 0
Fragments RX DSL : 0
Fragments RX DORMANT : 0
Fragments TX DSL : 0
Fragments TX DORMANT : 0
Fragments RX OUT : 0
Fragments TX OUT : 0
too many frag. lists for flow : 0
frag. list cleanup in progress : 0
--snip--
=====
```

To interpret these counters, familiarity with the following terms in the context of fragmentation is required:

**Packet** – An IP packet that is split into fragments (multiple frames) due to its original size being larger than the MTU configured on any node servicing this packet

**Fragment** – Frames that make up a packet. Multiple fragments (frames on the wire) are eventually reassembled into the original packet.

**Fragment list** – MS-ISA maintains a list of fragments belonging to a single packet. Each list represents a single fragmented packet and the list contains multiple fragments.

**Fragment hole** – A whole refers to a fragment or a group of consecutive fragments in a fragment list. Fragments of a packet are sequentially numbered from first to last and they must be reassembled in the same order in which they are fragmented. For example, if a packet contains 9 fragments but only fragments [1,3,5,9] are received by MS-ISA, then there are 3 holes in this list [2],[3,4],[6,7,8].

**Flow** – Identified by 5 tuple <src IP, dst IP, src Port, dst Port, protocol>. Flow can have many packets and each packet of a flow can be fragmented.

**Table 46**

| Counter Name                     | Description                                                                                                                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| too many fragments for IP packet | This counter increments if there are more than 20 fragments of a received single packet (the maximum number of fragments per packet is 20). In this case, all fragments of the packet are dropped.                                       |
| too many fragmented packets      | This counter increases if the maximum number of fragmented packets per MS-ISA is reached. Refer to the MS-ISA Scaling Guides for the maximum number of fragmented packets per MS-ISA (specifically, the max num of frag lists parameter) |
| too many fragment holes          | This counter increments if there are more than 11 holes tracked for a single packet. In this case, all fragments will be dropped.                                                                                                        |
| too many frags buffered          | This counter increases if the maximum number of fragments that can be stored on MS-ISA is reached.                                                                                                                                       |
| fragment list expired            | This counter increases if all fragments of single packets are not received within two seconds. In this case, all fragments of this packet are dropped.                                                                                   |

**Table 46** (Continued)

| Counter Name        | Description                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lists for flow      | This counter increases when more than five fragmented packets per flow are being maintained simultaneously in MS-ISA. In this case, the fragments of the sixth packets are dropped.                                                                                                                                                                                      |
| Reassembly Failures | This counter increases when the reassembly of a packets (once all fragments are received) failed. This can be due to the size of the first DS-lite IPv6 fragment is smaller than 1280B, or the total reassembled packet is too big (greater than 9212B).                                                                                                                 |
| Fragments RX DSL    | This counter increments only when a DS-lite packet/ fragment is received in the upstream direction that contains an IPv4 fragment. In other words, this counter is relevant only to IPv4 fragments inside of the DS-lite packet/ fragment that is received from the subscriber, and is not affected by DS-lite fragments.                                                |
| Fragments TX DSL    | This counter increments only in case that DS-lite packet/ fragment sent in the downstream direction contains an encapsulated IPv4 fragment (which is received from the public side). In other words, this counter is relevant only to IPv4 fragments inside of the DS-lite packet/fragment that is sent toward the subscriber, and is not affected by DS-lite fragments. |
| Fragments RX OUT    | This counter increments when an IPv4 fragment is received in the downstream direction, toward the subscriber.                                                                                                                                                                                                                                                            |
| Fragments TX OUT    | This counter increments when an IPv4 fragment is transmitted in the upstream direction (public side).                                                                                                                                                                                                                                                                    |

## 7.18 Enhanced Statistics in NAT — Histogram

The NAT command **histogram** displays compartmentalized port distribution per protocol for an aggregated number of subscribers. This allows operators to trend port usage over time and consequently adjust the configuration as the port demand per subscriber increase/decrease. For example, an operator may find that the port usage in a pools has increased over a period of time. Accordingly, the operator may plan to increase the number of ports per port block.

The feature is not applicable to pools which operate in one-to-one mode.

The output is organized in port buckets with the number of subscribers in each bucket.

```
tools dump nat histogram
- histogram router <router-instance> pool <pool-name> bucket-
size <[1..65536]> num-buckets <[2..50]>

<router-instance> : <router-name> | <service-id>
 router-name - "Base"
 service-id - [1..2147483647]
<pool-name> : [32 chars max]
```

For example:

```
tools dump nat histogram router "Base" pool "det" bucket-size 20 num-buckets 20
=====Usage histogram NAT pool "det" router "Base"=====
Num-ports Sub-TCP Sub-UDP Sub-ICMP

0-19 0 0 0
20-39 0 0 0
40-59 0 0 0
60-79 0 0 0
80-99 0 0 0
100-119 0 0 0
120-139 0 0 0
140-159 0 0 0
160-179 0 0 0
180-199 0 0 0
200-219 0 0 0
220-239 0 0 0
240-259 0 0 0
260-279 0 0 0
280-299 0 0 0
300-319 0 0 0
320-339 0 0 0
340-359 0 0 0
360-379 0 0 0
380- 0 0 0

```



The output of the **histogram** command can be periodically exported to an external destination via cron. The following is an example:

```
*A:Dut-A>config>system>script-control# info

 script "nat_histogram"
 location "ftp://*:~*192.8.62/nat-histogram.txt"
 no shutdown
 exit
 script-policy "dump_nat_histogram"
 results "ftp://*:~*192.168.8.62/nat_histogram_results.txt"
 script "nat_histogram"
 no shutdown
 exit
*A:Dut-A>config>system>cron# info

 schedule "nat_histogram_schedule"
 interval 600
 script-policy "dump_nat_histogram"
 no shutdown
 exit
```

The nat-histogram.txt file contains the command execution line. For example:

```
tools dump nat histogram router 4 pool "deterministic" bucket-size
10 num-buckets 10
```

This command will be executed every 10 minutes (600 seconds) and the output of the command will be written into a set of files on an external FTP server:

```
[root@ftp]# ls nat_histogram_results.txt*
nat_histogram_results.txt_20130117-153548.out
nat_histogram_results.txt_20130117-153648.out
nat_histogram_results.txt_20130117-153748.out
nat_histogram_results.txt_20130117-153848.out
nat_histogram_results.txt_20130117-153948.out
nat_histogram_results.txt_20130117-154048.out
[root@ftp]#
```

## 7.18.1 Configuration

```
tools dump nat histogram router <router-instance> pool <pool-name> bucket-
size <[1..65536]> num-buckets <[2..50]>
```

The output of this command displays the port usage in a given pool per protocol per subscriber. The output is organized in a configurable number of port-buckets.

In the following example there is 1 subscriber that is using between 20 and 39 UDP ports in the pool named **det**. The pool is configured in the Base routing instance.

```
tools dump nat histogram router "Base" pool "det" bucket-size 20 num-buckets 40
```

```
=====
Usage histogram NAT pool "det" router "Base"
=====
Num-ports Sub-TCP Sub-UDP Sub-ICMP

0-19 0 0 0
20-39 0 1 0
40-59 0 0 0
60-79 0 0 0
80-99 0 0 0
100-119 0 0 0
120-139 0 0 0
140-159 0 0 0
160-179 0 0 0
180-199 0 0 0
200-219 0 0 0
220-239 0 0 0
240-259 0 0 0
260-279 0 0 0
280-299 0 0 0
300-319 0 0 0
320-339 0 0 0
340-359 0 0 0
360-379 0 0 0
380-399 0 0 0
400-419 0 0 0
420-439 0 0 0
440-459 0 0 0
460-479 0 0 0
480-499 0 0 0
500-519 0 0 0
520-539 0 0 0
540-559 0 0 0
560-579 0 0 0
580-599 0 0 0
600-619 0 0 0
620-639 0 0 0
640-659 0 0 0
660-679 0 0 0
680-699 0 0 0
700-719 0 0 0
720-739 0 0 0
740-759 0 0 0
760-779 0 0 0
780- 0 0 0

No. of entries: 40
=====
```

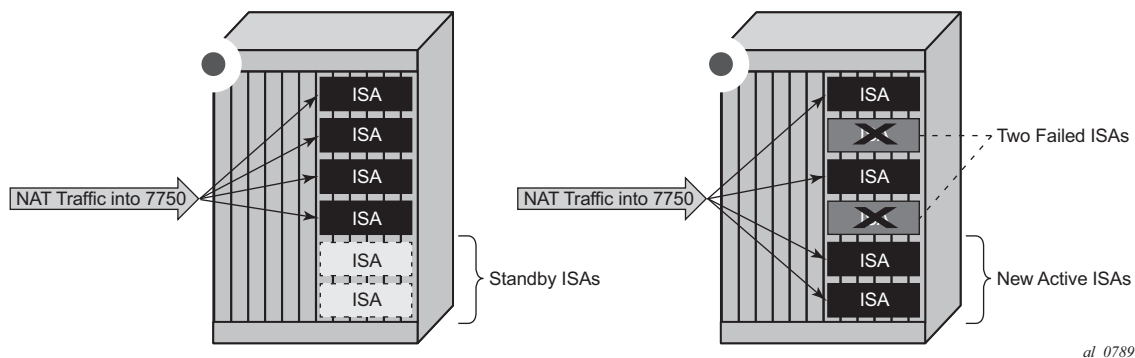
## 7.19 NAT Redundancy

NAT ISA redundancy helps protect against Integrated Service Adapter (ISA) failures. This protection mechanism relies on the CPM maintaining configuration copy of each ISA. In case that an ISA fails, the CPM restores the NAT configuration from the failed ISA to the remaining ISAs in the system. NAT configuration copy of each ISA, as maintained by CPM, is concerned with configuration of outside IP address and port forwards on each ISA. However, CPM does not maintain the state of dynamically created translations on each ISA. This will cause interruption in traffic until the translation are re-initiated by the devices behind the NAT.

Two modes of operation are supported:

- **Active-Standby** — In this mode of operation, any number of standby ISAs can be allocated for protection purposes. When there are no failures in the router, standby ISAs are idle, in a state ready to accept traffic from failed ISA. Mapping between the failed ISA and the standby ISA is always 1:1. This means that one standby ISA will entirely replace one failed ISA. In this respect, NAT bandwidth from the failed ISA is reserved and restored upon failure. This model is shown in [Figure 73](#).

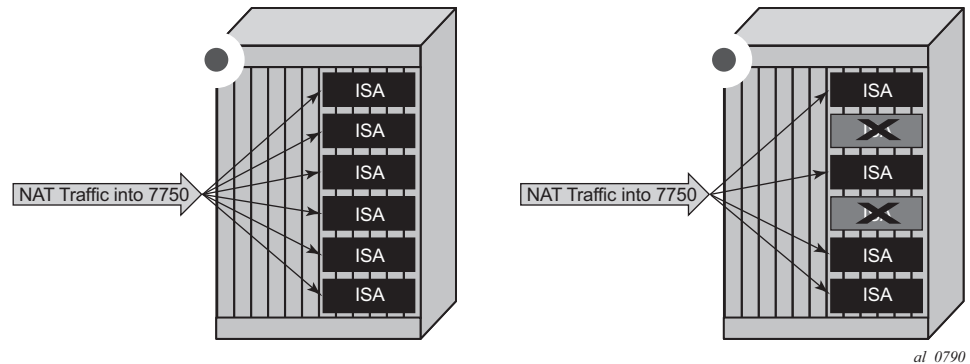
**Figure 73 Active-Standby Intra-Chassis Redundancy Model**



- **Active-Active** — In this mode all ISAs in the system are active. Once an ISA fails, its load is distributed across the remaining active ISA. In this mode of operation there is no bandwidth reservation across active ISA. Each ISA can operate at full speed at any given time. However, memory resources necessary to setup new translations from the failed ISAs are reserved. The reserved resources are:
  - Subscribers — Inside IPv4 addresses for LSN44, IPv6 prefixes for DS-lite/ NAT64 and L2-Aware subscriber.
  - Outside IPv4 addresses
  - Outside port-ranges.

By reserving memory resources it can be assured that failed traffic can be recovered by remaining ISAs, potentially with some bandwidth reduction in case that remaining ISAs operated at full or close to full speed before the failure occurred. Active-active ISA redundancy model is shown in [Figure 74](#).

**Figure 74 Active-Active Intra-Chassis Redundancy Model**



In case of an ISA failure, the member-id of the member ISA that failed is contained in the FREE log. This info is used to find the corresponding MAP log which also contains the member-id field.

In case of RADIUS logging, CPM summarization trap is generated (since RADIUS log is sent from the ISA – which is failed).

### 7.19.1 NAT Stateless Dual-Homing

Multi-chassis stateless NAT redundancy is based on a switchover of the NAT pool that can assume active (master) or standby state. The inside/outside routes that attract traffic to the NAT pool are always advertised from the active node (the node on which the pool is active).

This dual-homed redundancy based on the pool mastership state works well in scenarios where each inside routing context is configured with a single NAT policy (NATed traffic within this inside routing context will be mapped to a single NAT pool).

However, in cases where the inside traffic is mapped to multiple pools (with deterministic NAT and in case when multiple NAT policies are configured per inside routing context), the basic per pool multi-chassis redundancy mode can cause the inside traffic within the same routing instance to fail since some pools referenced from the routing instance might be active on one node while other pools might be active on the other node.

Imagine a case where traffic ingressing the same inside routing instance is mapped as follows (this mapping can be achieved via filters):

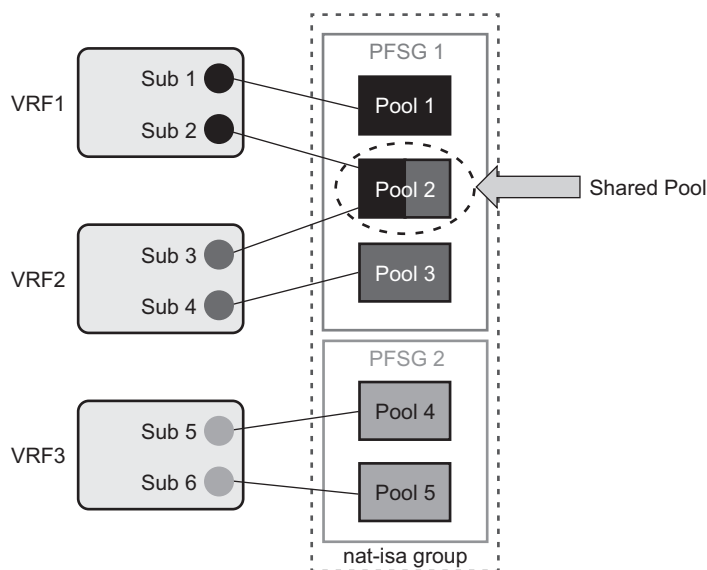
- Source ip-address A —> Pool 1 (nat-policy 1) active on Node 1
- Source ip-address B —> Pool 2 (nat-policy 2) active on Node 2

Traffic for the same destination is normally attracted only to one NAT node (the destination route is advertised only from a single NAT node). Assume that this node is Node 1 in the example. Once the traffic arrives to the NAT node, it will be mapped to the corresponding pool according to the mapping criteria (routing based or filter based). But if active pools are not co-located, traffic destined to the pool that is active on the neighboring node would fail. In our example traffic from the source ip-address B would arrive to the Node 1, while the corresponding Pool 2 is inactive on that node. Consequently the traffic forwarding would fail.

To remedy this situation, a group of pools targeted from the same inside routing context must be active on the same node simultaneously. In other words, the active pools referenced from the same inside routing instance must be co-located. This group of pools is referred to as Pool Fate Sharing Group (PFSG). The PFSG is defined as a group of all NAT pools referenced by inside routing contexts whereby at least one of those pools is shared by those inside routing contexts. This is shown in [Figure 73](#).

Even though only Pool 2 is shared between subscribers in VRF 1 and VRF 2, the remaining pools in VRF 1 and VRF 2 must be made part of PFSG 1 as well.

This will ensure that the inside traffic will be always mapped to pools that are active in a single box.

**Figure 75 Pool Fate Sharing Group**

al\_0409

There is always one lead pool in PFSG. The Lead pool is the only pool that is exporting/monitoring routes. Other pools in the PFSG are referencing the lead pool and they inherit its (activity) state. If any of the pools in PFSG fails, all the pools in the PFSG will switch the activity, or in another words they will share the fate of the lead pool (active/standby/disabled).

There is one lead pool per PFSG per node in a dual-homed environment. Each lead pool in a PFSG will have its own export route that must match the monitoring route of the lead pool in the corresponding PFSG on the peering node.

PFSG is implicitly enabled by configuring multiple pools to follow the same lead pool.

### 7.19.1.1 Configuration Considerations

Attracting traffic to the active NAT node (from inside and outside) is based on the routing.

On the outside, the active pool address range will be advertised. On the inside, the destination prefix or steering route (in case of filter based diversion to the NAT function) will be advertised by the node with the active pool.

The advertisement of the routes will be driven by the activity of the pools in the pool fate sharing group:

```
configure
router/service vprn
nat
outside
pool <name>
redundancy
export <ip-prefix/length>
monitor <ip-prefix/length>[no] shutdown
follow router <rtr-id> pool <master-pool>
```

For example:

```
router/service vprn
nat
outside
pool "nat0-pool" nat-group 1 type large-scale create
port-reservation ports 252
redundancy
follow router 500 pool "nat500-pool"
exit
address-range 192.168.12.0 192.168.12.10 create
exit
no shutdown
exit
exit
exit
```

A pool can be one of the following:

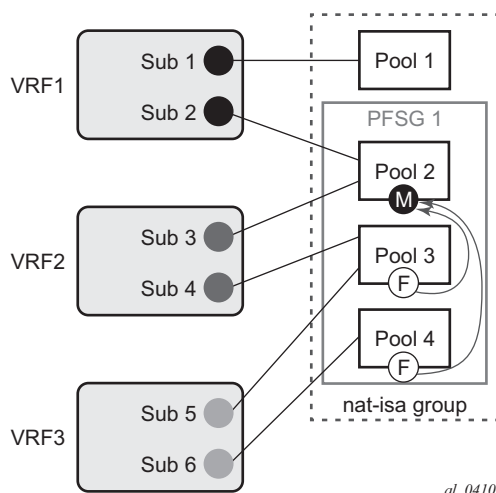
- A leading pool: configure export- and monitor-route and put in no shutdown
- A following pool: configure follow

Both sets of options are thus mutually exclusive.

For a leading pool redundancy will only be enabled when the redundancy node is in no shutdown. For a following pool, the administrate has no effect, and the redundancy will only be enabled when the leading pool is enabled.

Before a lead pool is enabled, consistency check will be performed to make sure that PFSG is properly configured and that the all pools in the given PFSG belong to the same NAT isa-group. PFSG is implicitly enabled by configuring multiple pools to follow the same lead pool. Adding or removing pools from the fate-share-group is only possible when the leading pool is disabled.

For example in the following case, the consistency check would fail since pool 1 is not part of the PFSG 1 (where it should be).

**Figure 76 Consistency Check**

### 7.19.1.2 Troubleshooting Commands

The following command displays the state of the leading pool (dual-homing section towards the bottom of the command output):

```
*A:Dut-B# show router 500 nat pool "nat500-pool"
=====
NAT Pool nat500-pool
=====
Description : (Not Specified)
ISA NAT Group : 1
Pool type : largeScale
Admin state : inService
Mode : auto (napt)
Port forwarding dyn blocks reserved : 0
Port forwarding range : 1 - 1023
Port reservation : 2300 blocks
Block usage High Watermark (%) : (Not Specified)
Block usage Low Watermark (%) : (Not Specified)
Subscriber limit per IP address : 65535
Active : true
Deterministic port reservation : (Not Specified)
Last Mgmt Change : 02/17/2014 09:41:43
=====
NAT address ranges of pool nat500-pool
=====
Range Drain Num-blk

192.168.1.0 - 192.168.1.255 0

No. of ranges: 1
=====
```



```
=====
NAT members of pool nat500-pool ISA NAT group 1
=====
Member Block-Usage-% Hi

1 < 1 N
2 < 1 N
3 < 1 N
4 < 1 N
5 < 1 N
6 < 1 N

No. of members: 6
=====
Dual-Homing
=====
Type : Leader
Export route : 10.0.0.3/32
Monitor route : 10.0.0.2/32
Admin state : inService
Dual-Homing State : Active
=====
Dual-Homing fate-share-group
=====
Router Pool Type

Base nat0-pool Follower
vprn500 nat500-pool Leader
vprn501 nat501-pool Follower
vprn502 nat502-pool Follower

No. of pools: 4
=====
```

The following command displays the state of the follower pool (dual-homing section towards the bottom of the command output):

```
*A:Dut-B# show router 501 nat pool "nat501-pool"
=====
NAT Pool nat501-pool
=====
Description : (Not Specified)
ISA NAT Group : 1
Pool type : largeScale
Admin state : inService
Mode : auto (napt)
Port forwarding dyn blocks reserved : 0
Port forwarding range : 1 - 1023
Port reservation : 2300 blocks
Block usage High Watermark (%) : (Not Specified)
Block usage Low Watermark (%) : (Not Specified)
Subscriber limit per IP address : 65535
Active : true
Deterministic port reservation : (Not Specified)
```

```

Last Mgmt Change : 02/17/2014 09:41:43
=====
NAT address ranges of pool nat501-pool
=====
Range Drain Num-blk

192.168.2.0 - 192.168.2.255 0
192.168.3.0 - 192.168.3.255 0

No. of ranges: 2
=====
NAT members of pool nat501-pool ISA NAT group 1
=====
Member Block-Usage-% Hi

1 < 1 N
2 < 1 N
3 < 1 N
4 < 1 N
5 < 1 N
6 < 1 N

No. of members: 6
=====
Dual-Homing
=====
Type : Follower
Follow-pool : "nat500-pool" router 500
Dual-Homing State : Active
=====
Dual-Homing fate-share-group
=====
Router Pool Type

Base nat0-pool Follower
vprn500 nat500-pool Leader
vprn501 nat501-pool Follower
vprn502 nat502-pool Follower

No. of pools: 4
=====

```

The following command lists all the pools that are configured along with the NAT inside/outside routing context.

```

*A:Dut-B# show service nat overview
=====
NAT overview
=====
Inside/ Policy/ Type
Outside Pool

vprn550 lsn-policy_unused default

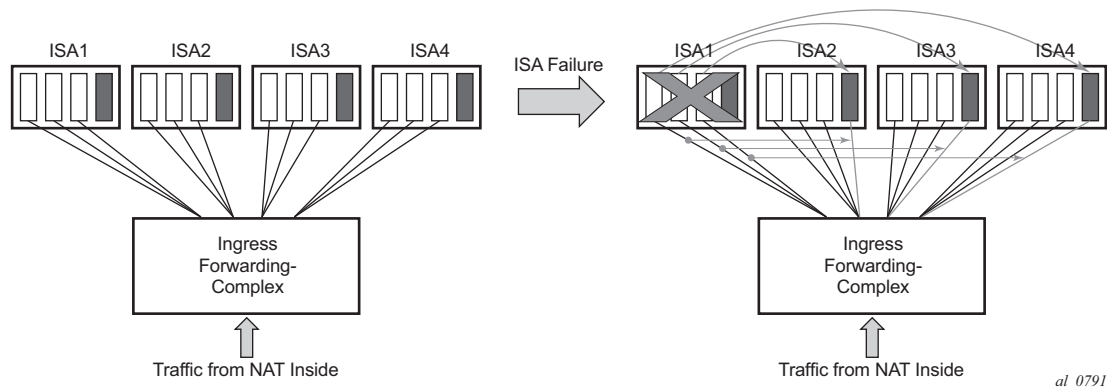
```

|         |                   |                    |
|---------|-------------------|--------------------|
| Base    | nat0-pool         |                    |
| vprn550 | lsn-policy_nat1   | destination prefix |
| vprn500 | nat500-pool       |                    |
| vprn550 | lsn-policy_nat2   | destination prefix |
| vprn501 | nat501-pool       |                    |
| vprn551 | lsn-policy_unused | default            |
| Base    | nat0-pool         |                    |
| vprn551 | lsn-policy_nat3   | destination prefix |
| vprn501 | nat501-pool       |                    |
| vprn551 | lsn-policy_nat4   | destination prefix |
| vprn502 | nat502-pool       |                    |
| vprn552 | lsn-policy_unused | default            |
| Base    | nat0-pool         |                    |
| vprn552 | lsn-policy_nat5   | destination prefix |
| vprn502 | nat502-pool       |                    |
| =====   |                   |                    |

### 7.19.2 Active-Active ISA Redundancy Model

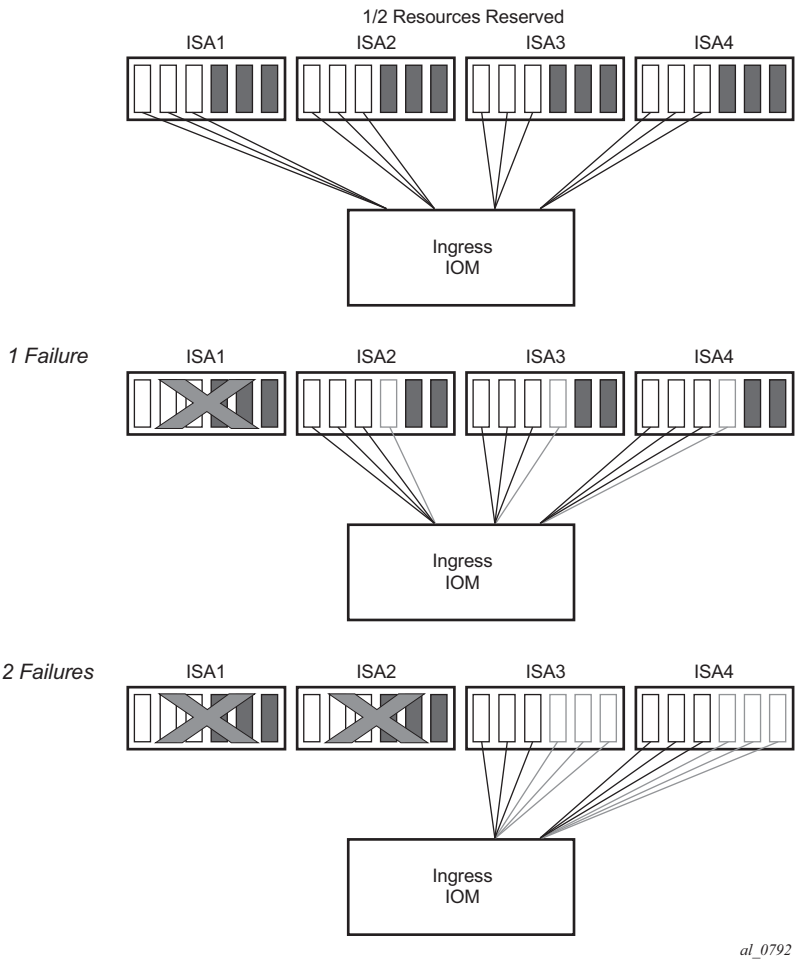
In active-active ISA redundancy, each ISA is subdivided into multiple logical ISAs. These logical sub-entities are referred to as members. NAT configuration of each member is saved in the CPM. In case that any one ISA fails, its members will be downloaded by the CPM to the remaining active ISAs. Memory resources on each ISA will be reserved in order to accommodate additional traffic from the failed ISAs. The amount of resources reserved per ISA will depend on the number of ISAs in the system and the number of simultaneously supported ISA failures. The number of simultaneous ISA failures per system is configurable. Memory reservation will affect NAT scale per ISA.

Traffic received on the inside will be forwarded by the ingress forwarding complex to a predetermined member ISAs for further NAT processing. Each ingress forwarding complex maintains an internal link per member. The number of these internal links will, among other factors, determine the maximum number of members per system and with this, the granularity of traffic distribution over remaining ISAs in case of an ISA failure. The segmentation of ISAs into members for a single failure scenario is shown in [Figure 77](#). The protection mechanism in this example is designed to cover for one physical ISA failure. Each ISA is divided into four members. Three of those will carry traffic during normal operation, while the fourth one will have resources reserved to accommodate traffic from one of the members in case of failure. When an ISA failure occurs, three members will be delegated to the remaining ISAs. Each member from the failed ISA will be mapped to a corresponding reserved member on the remaining ISAs.

**Figure 77** Load Distribution in Active-Active Intra-Chassis Redundancy Model

Active-active ISA redundancy model supports multiple failures simultaneously. The protection mechanism shown in [Figure 78](#) is designed to protect against two simultaneous ISA failures. As the previous case, each ISA is divided into six members, three of which are carrying traffic under normal circumstances while the remaining three members have reserved memory resources.

Figure 78 Multiple Failures



al\_0792

Table 47 shows resource utilization for a single ISA failure in relation to the total number of ISAs in the system. The resource utilization will affect only scale of each ISA. However, bandwidth per ISA is not reserved and each ISA can operate at full speed at any given time (with or without failures).

Table 47 Load Distribution in Active-Active ISA Redundancy Model Supporting Single ISA Failure

| Number of Physical ISAs per System | Number of Member ISAs per Physical ISA (active/reserved) | Resource Utilization Per System in Non-Failed Condition | Resource Utilization Per System With One Failed ISA |
|------------------------------------|----------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------|
| 2                                  | 1A 1R                                                    | 50%                                                     | 100%                                                |
| 3                                  | 2A 1R                                                    | 67%                                                     | 100%                                                |

**Table 47** Load Distribution in Active-Active ISA Redundancy Model Supporting Single ISA Failure (Continued)

| Number of Physical ISAs per System | Number of Member ISAs per Physical ISA (active/reserved) | Resource Utilization Per System in Non-Failed Condition | Resource Utilization Per System With One Failed ISA |
|------------------------------------|----------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------|
| 4                                  | 3A 1R                                                    | 75%                                                     | 100%                                                |
| 5                                  | 3A 1R                                                    | 75%                                                     | 95%                                                 |
| 6                                  | 2A 1R                                                    | 66%                                                     | 83%                                                 |
| 7                                  | 2A 1R                                                    | 66%                                                     | 80%                                                 |
| 8                                  | 2A 1R                                                    | 66%                                                     | 79%                                                 |
| 9                                  | 1A 1R                                                    | 50%                                                     | 61%                                                 |
| 10                                 | 1A 1R                                                    | 50%                                                     | 60%                                                 |
| 11                                 | 1A 1R                                                    | 50%                                                     | 59%                                                 |
| 12                                 | 1A 1R                                                    | 50%                                                     | 58%                                                 |
| 13                                 | 1A 1R                                                    | 50%                                                     | 58%                                                 |
| 14                                 | 1A 1R                                                    | 50%                                                     | 57%                                                 |

### 7.19.2.1 Start Up Conditions

During the first five minutes of system start up or nat-group activation, the system behaves as if all ISAs are operational. Consequently, ISAs are segmented in its members according to the configured maximum number of supported failures.

Upon expiration of this initial five minute interval, the system is re-evaluated. In case that one of more ISAs are found in faulty state during re-evaluation, the members of the failed ISAs will be distributed to the remaining ISAs that are operational.

### 7.19.2.2 Recovery

Once a failed ISA is recovered, the system will automatically accept it and traffic will be assigned to it. Traffic that is moved to the recovered ISA will be interrupted.

### 7.19.2.3 Adding Additional ISAs in the ISA Group

Adding additional ISAs in an operational nat-group requires reconfiguration of the active mda-limit for the nat-group (or the failed mda-limit for that matter). This is only possible when nat-group is in an administratively shutdown state.

## 7.19.3 L2-Aware Bypass

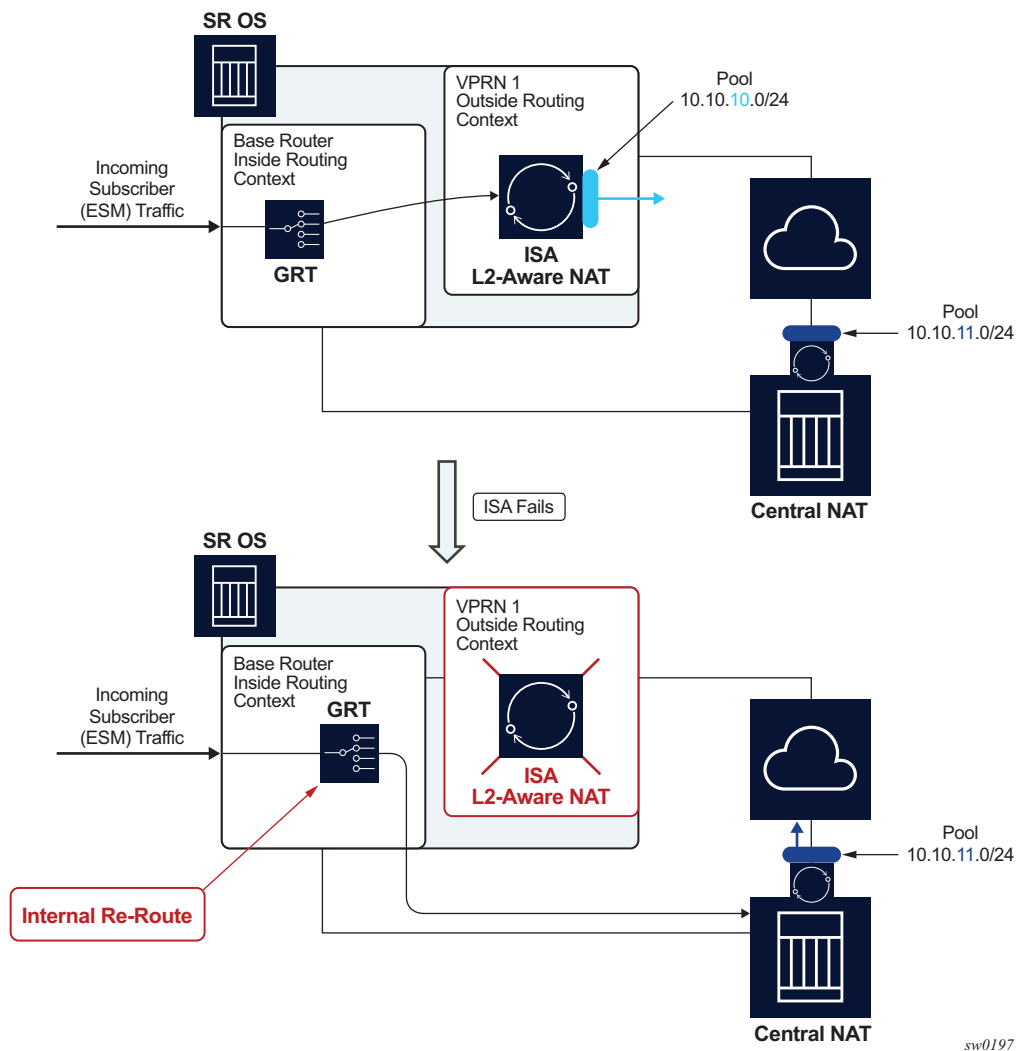
L2-Aware bypass provides the basis for traffic continuity if an MS-ISA fails. With L2-Aware bypass functionality disabled and without an intra-chassis redundancy scheme deployed (such as active/active or active/standby), the traffic to be processed by the failed MS-ISA is blackholed. This means that traffic continues to be sent to the failed MS-ISA. By enabling L2-Aware bypass, instead of being blackholed, the traffic is routed outside of the SR OS node without being NATed in accordance to the routing table in the inside routing context. The intent is that non-NATed traffic is intercepted by a central NAT node that performs the NAT function. This way, traffic served by the failed MS-ISA continues to be NATed by a central NAT node. The central NAT node provides redundancy for multiple SR OS nodes, thus reducing the need to equip each individual SR OS node with multiple MS-ISAs which are normally used in an active/active or active/standby intra-chassis redundancy mode.

This concept is shown in [Figure 79](#). The example shows the base router as an inside routing context where the global routing table (GRT) is used to decide where to send traffic if an MS-ISA is unavailable. Apart from this example, the inside routing context is not limited to the base router but instead can be an VPRN instance.

L2-Aware bypass is considered as an optional redundancy model in L2-Aware NAT which is mutually exclusive with other two MS-ISA redundancy modes (active/active and active/standby).

L2-Aware bypass is enabled with the following CLI:

```
configure
isa
 nat-group <id>
 redundancy {active-active|active-standby|l2aware-bypass}
```

**Figure 79 L2-Aware Bypass**



### 7.19.3.1 Sharing IP Addresses in L2-Aware NAT

L2-Aware NAT allows overlap of inside (private) IP addresses between Enhanced Subscriber Management (ESM) (or L2-Aware NAT) subscribers. For example, IP addresses assigned to hosts within, for example, subscriber SUB-1, can be identical to IP addresses assigned to hosts within, for example, subscriber SUB-2. This is possible by the subscriber-ID field (which must be unique in the system) that is a part of the NAT translation key. This way the return traffic (in downstream direction) belonging to different ESM subscribers with overlapping IP addresses can still be differentiated by a unique ESM subscriber-id field that is used in reverse NAT translation.

L2-Aware bypass functionality with a failed MS-ISA breaks the logic since traffic is not translated (NATed) in SR OS node, and therefore, the return traffic does not take subscriber-id field into forwarding consideration. For this reason, the overlap of inside (private) IP addresses between ESM subscribers is not supported by the L2-Aware bypass functionality for the routed traffic within the same inside routing context. In other words, private IP addresses must be unique across the subscribers within a specified inside routing context.

### 7.19.3.2 Recovery

Upon the recovery of the failed MS-ISA, all existing subscribers that are affected by the bypass continue to use the bypass. However, all new subscribers that come online after the recovery, are automatically L2-aware NATed (and therefore do not use the bypass).

Restoring bypassed subscribers to the L2-Aware NAT after the recovery, requires manual intervention by the operator. This is accomplished by executing the tools>perform>nat>recover-l2aw-bypass <slot/mda> command:

In L2-Aware NAT, the <subscriber to outside IP, port-block> mappings are allocated during the subscriber attachment phase (when the subscriber comes online) and are maintained in the CPM. As such, they are preserved in the CPM during MS-ISA failure. This means that the original mappings for the recovered subscribers continue to be used once the MS-ISA is recovered.

Be aware that only the partial mappings <subscriber to outside IP, port-block> are preserved. This does not include preservation of NAT sessions sometimes referred as fully qualified flows. NAT sessions are maintained in MS-ISA and they are lost during MS-ISA failures. Hence, this model provides stateless failover to an external NAT node.

The operator is notified about the MS-ISA failure by a log message or an SNMP trap. An example of such log is:

```
9 2017/06/07 11:32:49.748 UTC MINOR: NAT #2020 Base NAT
"The NAT MDA 5/1 is now inactive in group 2."
```

### 7.19.3.3 Default Bypass During Reboot or MS-ISA Provisioning

If enabled, L2-Aware bypass takes effect automatically if an MS-ISA does not become operational within 10 minutes of provisioning (configuring) or after a system boot-up.

### 7.19.3.4 Logging

Since partial mappings in L2-Aware NAT <subscriber to outside IP addresses, port block> are preserved in the CPM during an MS-ISA failure, no logging is generated for existing ESM/NAT subscribers when the MS-ISA fails or is recovered.

## 7.20 ISA Feature Interactions

This section describes the interaction between MS-ISA applications and other system features.

### 7.20.1 MS-ISA Use with Service Mirrors

All MS-ISA uses include support for service mirroring running with no feature interactions or impacts. For example, any service diverted to AA, IPsec, NAT, LNS, or supported combinations of MS-ISA application also supports service mirroring simultaneously.

### 7.20.2 LNS, Application Assurance and NAT

Multiple uses of MS-ISAs can be combined at one time by daisy-chaining use of the MS-ISAs. Services and subscribers terminated on the LNS ISA are full supported by Application Assurance per AA subscriber and service capabilities, and by the full NAT capabilities.

When Application Assurance and NAT are used in combination (for both ESM and SAP service contexts):

- AA is always on subscriber of NAT to be able to see the original (inside) subscriber IP tuple (IP + port numbers).
- AA subscriber ID includes the VRF context from the service, so shared or private subscriber IP as seen in Layer-2 Aware NAT is compatible with AA subscriber contexts.

### 7.20.3 Subscriber Aware Large Scale NAT44

Subscriber aware Large Scale NAT44 attempts to combine the positive attributes of Large Scale NAT44 and L2-Aware NAT, namely:

- The ability for some traffic to bypass the NAT function, such as IPTV traffic and VoIP traffic whenever a unique IP address per subscriber is used (for example, not L2-Aware NAT where all subs share the same IP). This can be achieved using existing Large Scale NAT44 mechanisms (ingress IP-filters)

- The use of RADIUS Acct for logging of port-ranges, including multiple port-range blocks.
- The use of subscriber-identification/RADIUS user-name to identify the customer to simplify management of Large Scale NAT44 subscribers.

Subscriber awareness in Large Scale NAT44 will facilitate release of NAT resources immediately after the BNG subscriber is terminated, without having to wait for the last flow of the subscriber to expire on its own (TCP timeout is 4hours by default).

The subscriber aware Large Scale NAT44 function leverages RADIUS accounting proxy built-in to the 7750 SR. The RADIUS accounting proxy allows the 7750 SR to inform Large Scale NAT44 application about individual BNG subscribers from the RADIUS accounting messages generated by a remote BNG and use this information in the management of Large Scale NAT44 subscribers. The combination of the two allows, for example, the 7750 SR running as a Large Scale NAT44 to make the correlation between the BNG subscriber (represented in the Large Scale NAT44 by the Inside IP Address) and RADIUS attributes such as User-Name, Alc-Sub-Ident-String, Calling-Station-Id or Class. These attributes can subsequently be used for either management of the Large Scale NAT44 subscriber, or in the NAT RADIUS Accounting messages generated by the 7750 SR Large Scale NAT44 application. Doing so will simplify both the administration of the Large Scale NAT44 and the logging function for port-range blocks.

As BNG subscribers authenticate and come online, the RADIUS accounting messages are 'snooped' via RADIUS accounting proxy which creates a cache of attributes from the BNG subscriber. BNG subscribers are correlated with the NAT subscriber via framed-ip address, and one of the following attributes that must be present in the accounting messages generated by BNG:

- User-name
- Subscriber id
- RADIUS Class attribute
- Calling-Station-id
- IMSI
- IMEI

Framed-ip address must also be present in the accounting messages generated by BNG.

Large Scale NAT44 Subscriber Aware application will receive a number of cached attributes which will then be used for appropriate management of Large Scale NAT44 subscribers, for example:

- Delete the Large Scale NAT44 subscriber when the BNG subscriber is terminated

- Report attributes in Large Scale NAT44 accounting messages according to configuration options

Creation and removal of RADIUS accounting proxy cache entries related to BNG subscriber is triggered by the receipt of accounting start/stop messages sourced by the BNG subscriber. Modification of entries can be triggered by interim-update messages carrying updated attributes. Cached entries can also be purged via CLI.

In addition to passing one of the above attributes in Large Scale NAT44 RADIUS accounting messages, a set of opaque BNG subscriber RADIUS attributes can optionally be passed in Large Scale NAT44 RADIUS accounting messages. Up to 128B of such opaque attributes will be accepted. The remaining attributes will be truncated.

Large Scale NAT44 subscriber instantiation can optionally be denied in case that corresponding BNG subscriber cannot be identified in Large Scale NAT44 via RADIUS accounting proxy.

Configuration guidelines:

Configure RADIUS accounting proxy functionality in a routing instance that will receive accounting messages from the remote or local BNG. Optionally forward received accounting message received by RADIUS accounting proxy to the final accounting destination (accounting server).

Point the BNG RADIUS accounting destination to the RADIUS accounting proxy – this way RADIUS accounting proxy will receive and ‘snoop’ BNG RADIUS accounting data.

BNG subscriber can be associated with two accounting policies, therefore pointing to two different accounting destinations. For example, one to the RADIUS accounting proxy, the other one to the real accounting server.

Configure subscriber aware Large Scale NAT44. From Large Scale NAT44 Subscriber Aware application reference the RADIUS Proxy accounting server and define the string that will be used to correlate BNG subscriber with the Large Scale NAT44 subscriber.

Optionally enable NAT RADIUS accounting that will include BNG subscriber relevant data.

(1)

```
*A:left-a20>config>service>vprn#
radius-proxy
server "proxy-acct" purpose accounting create
default-accounting-server-policy "lsn-policy"
description "two side server -interface:client ; default-
```

```

plcy:real server"
 interface "rad-proxy-loopback"
 secret "TEg1UEZzemRMyZXD1HvvQGkeGfoQ58MF" hash2
 no shutdown
 exit
exit

```

RADIUS accounting proxy will listen to accounting messages on interface 'rad-proxy-loopback'.

The name 'proxy-acct' as defined by the **server** command will be used to reference this proxy accounting server from Large Scale NAT44.

Received accounting messages can be relayed further from RADIUS accounting proxy to the accounting server which can be indirectly referenced in the default-accounting-policy 'lsn-policy'.

The lsn-policy is defined as:

```

*A:left-a20>config>aaa#
 radius-server-policy "lsn-policy" create
 servers
 router "Base"
 source-address 192.168.1.12
 server 1 name "192"
 exit
exit

```

This lsn-policy can then reference an external RADIUS accounting server with its own security credentials. This external accounting server can be configured in any routing instance.

```

*A:left-a20>config>router>radius-server# info

 server "192" address 192.168.1.10 secret "KRr7H.K3i0z90/
hj2BUSmdJUd1.zWrkE" hash2 port 1813 create
 description "real radius or acct server"
 exit

```

(2)

Two RADIUS accounting policies can be configured in BNG – one to the real radius server, the other one to the RADIUS accounting proxy.

```

*A:left-a20>config>subscr-mgmt>sub-prof# info

 radius-accounting-policy "real-acct-srvr" duplicate "lsn"
 egress
 agg-rate-limit 10000
 exit

*A:left-a20>config>subscr-mgmt>acct-plcy# info

```

```

 description "lsn radius-acct-policy"
update-interval 5
 include-radius-attribute
 acct-authentic
 acct-delay-time
 called-station-id
 calling-station-id remote-id
 circuit-id
 framed-interface-id
 framed-ip-addr
 framed-ip-netmask
 mac-address
 nas-identifier
 nas-port-id
 nas-port-type
 nat-port-range
 remote-id
 sla-profile
 sub-profile
 subscriber-id
 user-name
 alc-acct-triggered-reason
 exit
 session-id-format number
 radius-accounting-server
 router 10 (service id where proxy radius is configured)
 server 1 address 10.5.5.5 secret "cVilSIDvgH28Pd9QoN1f1E" hash2
(radius proxy IP address is 10.5.5.5 on interface "rad-proxy-
loopback"; the 'secret' is the same as configured on RADIUS accounting proxy)
 exit

```

(3)

Sub-aware Large Scale NAT44 references the RADIUS accounting proxy server 'proxy-acct' and defines the calling-station-id attribute from the BNG subscriber as the matching attribute:

```

*A:left-a20>config>service>vprn>nat>inside# info

 nat-policy "nat-base"
 destination-prefix 10.0.0.0/16
 subscriber-identification
 attribute vendor "standard" attribute-type "station-id"
 description "sub-aware CGN"
 radius-proxy-server router 10 name "proxy-acct"
 no shutdown
 exit

```

(4)

Optionally RADIUS NAT accounting can be enabled:

```
*A:left-a20>config>isa>nat-group# info

 active-mda-limit 1
 radius-accounting-policy "nat-acct-basic"
 mda 1/2
 no shutdown

*A:left-a20>config>aaa>isa-radius-plcy# info detail

 description "radius accounting policy for NAT"
 include-radius-attribute
 framed-ip-addr
 nas-identifier
 nat-subscriber-string
 user-name
 inside-service-id
 outside-service-id
 outside-ip
 port-range-block
 hardware-timestamp
 release-reason
 multi-session-id
 frame-counters
 octet-counters
 session-time
 called-station-id
 subscriber-data
 exit
 radius-accounting-server
 access-algorithm direct
 retry 3
 router "Base"
 source-address-range 192.168.1.20 192.168.1.20
 timeout sec 5
 server 1 address 192.168.1.10 secret "KlWIBi08CxTyM/
YXaU2gQitOu8GgfSD7Oj5hjese27A" hash2 port 1813
 exit

```

Such setup would produce a stream of following Large Scale NAT44 RADIUS accounting messages:

```
Mon Jul 16 10:59:27 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Start
Acct-Multi-Session-Id = "500456500365a4de7c29a9a07c29a9a0"
Acct-Session-Id = "500456500365a4de6201d7b87c29a9a0"
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "remote0"
Calling-Station-Id = "remote0"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.7
Alc-Nat-Outside-Ip-Addr = 198.51.100.1
```



```
Alc-Nat-Port-Range = "198.51.100.1 1054-1058 router base"
Acct-Input-Packets = 0
Acct-Output-Packets = 0
Acct-Input-Octets = 0
Acct-Output-Octets = 0
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 0
Event-Timestamp = "Jul 16 2012 10:58:40 PDT"
NAS-IP-Address = 10.1.1.1
User-Name = "cgn_1_ipoe"
Framed-IP-Netmask = 255.255.255.0
Class = 0x63676e2d636c6173732d7375622d6177617265
NAS-Identifier = "left-a20"
Acct-Session-Id = "D896FF0000000550045640"
Event-Timestamp = "Jul 16 2012 10:58:24 PDT"
NAS-Port-Type = Ethernet
NAS-Port-Id = "1/1/5:5.10"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Acct-Unique-Session-Id = "10f8bce6e5e7eb41"
Timestamp = 1342461567
Request-Authenticator = Verified

Mon Jul 16 11:03:56 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Interim-Update
Acct-Multi-Session-Id = "500456500365a4de7c29a9a07c29a9a0"
Acct-Session-Id = "500456500365a4de6201d7b87c29a9a0"
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "remote0"
Calling-Station-Id = "remote0"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.7
Alc-Nat-Outside-IP-Addr = 198.51.100.1
Alc-Nat-Port-Range = "198.51.100.1 1054-1058 router base"
Acct-Input-Packets = 0
Acct-Output-Packets = 1168
Acct-Input-Octets = 0
Acct-Output-Octets = 86432
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 264
Event-Timestamp = "Jul 16 2012 11:03:04 PDT"
Acct-Delay-Time = 5
NAS-IP-Address = 10.1.1.1
User-Name = "cgn_1_ipoe"
Framed-IP-Netmask = 255.255.255.0
Class = 0x63676e2d636c6173732d7375622d6177617265
NAS-Identifier = "left-a20"
Acct-Session-Id = "D896FF0000000550045640"
Acct-Session-Time = 279
Event-Timestamp = "Jul 16 2012 11:03:04 PDT"
NAS-Port-Type = Ethernet
NAS-Port-Id = "1/1/5:5.10"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
```

```
Acct-Unique-Session-Id = "10f8bce6e5e7eb41"
Timestamp = 1342461836
Request-Authenticator = Verified

Mon Jul 16 11:04:34 2012
NAS-IP-Address = 10.1.1.1
NAS-Identifier = "left-a20"
NAS-Port = 37814272
Acct-Status-Type = Stop
Acct-Multi-Session-Id = "500456500365a4de7c29a9a07c29a9a0"
Acct-Session-Id = "500456500365a4de6201d7b87c29a9a0"
Called-Station-Id = "00-00-00-00-01-01"
User-Name = "remote0"
Calling-Station-Id = "remote0"
Alc-Serv-Id = 10
Framed-IP-Address = 10.0.0.7
Alc-Nat-Outside-Ip-Addr = 198.51.100.1
Alc-Nat-Port-Range = "198.51.100.1 1054-1058 router base"
Acct-Terminate-Cause = Host-Request
Acct-Input-Packets = 0
Acct-Output-Packets = 1321
Acct-Input-Octets = 0
Acct-Output-Octets = 97754
Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 0
Acct-Session-Time = 307
Event-Timestamp = "Jul 16 2012 11:03:47 PDT"
NAS-IP-Address = 10.1.1.1
User-Name = "cgn_1_ipoe"
Framed-IP-Netmask = 255.255.255.0
Class = 0x63676e2d636c6173732d7375622d6177617265
NAS-Identifier = "left-a20"
Acct-Session-Id = "D896FF0000000550045640"
Acct-Session-Time = 279
Event-Timestamp = "Jul 16 2012 11:03:04 PDT"
NAS-Port-Type = Ethernet
NAS-Port-Id = "1/1/5:5.10"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Acct-Unique-Session-Id = "10f8bce6e5e7eb41"
Timestamp = 1342461874
Request-Authenticator = Verified
```

The matching accounting stream generated on the BNG is given below:

```
Mon Jul 16 10:59:11 2012
Acct-Status-Type = Start
NAS-IP-Address = 10.1.1.1
User-Name = "cgn_1_ipoe"
Framed-IP-Address = 10.0.0.7
Framed-IP-Netmask = 255.255.255.0
Class = 0x63676e2d636c6173732d7375622d6177617265
Calling-Station-Id = "remote0"
NAS-Identifier = "left-a20"
Acct-Session-Id = "D896FF0000000550045640"
Event-Timestamp = "Jul 16 2012 10:58:24 PDT"
NAS-Port-Type = Ethernet
```

```
NAS-Port-Id = "1/1/5:5.10"
ADSL-Agent-Circuit-Id = "cgn_1_ipoe"
ADSL-Agent-Remote-Id = "remote0"
Alc-Subsc-ID-Str = "CGN1"
Alc-Subsc-Prof-Str = "nat"
Alc-SLA-Prof-Str = "tp_sla_prem"
Alc-Client-Hardware-Addr = "2001:db8:65:05:10:01"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Acct-Unique-Session-Id = "9c1723d05e87c043"
Timestamp = 1342461551
Request-Authenticator = Verified

Mon Jul 16 11:03:51 2012
Acct-Status-Type = Interim-Update
NAS-IP-Address = 10.1.1.1
User-Name = "cgn_1_ipoe"
Framed-IP-Address = 10.0.0.7
Framed-IP-Netmask = 255.255.255.0
Class = 0x63676e2d636c6173732d7375622d6177617265
Calling-Station-Id = "remote0"
NAS-Identifier = "left-a20"
Acct-Session-Id = "D896FF0000000550045640"
Acct-Session-Time = 279
Event-Timestamp = "Jul 16 2012 11:03:04 PDT"
NAS-Port-Type = Ethernet
NAS-Port-Id = "1/1/5:5.10"
ADSL-Agent-Circuit-Id = "cgn_1_ipoe"
ADSL-Agent-Remote-Id = "remote0"
Alc-Subsc-ID-Str = "CGN1"
Alc-Subsc-Prof-Str = "nat"
Alc-SLA-Prof-Str = "tp_sla_prem"
Alc-Client-Hardware-Addr = "2001:db8:65:05:10:01"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Alcatel-IPD-Attr-163 = 0x00000001
Alc-Acct-I-Inprof-Octets-64 = 0x00010000000000000000
Alc-Acct-I-Outprof-Octets-64 = 0x000100000000000020468
Alc-Acct-I-Inprof-Pkts-64 = 0x00010000000000000000
Alc-Acct-I-Outprof-Pkts-64 = 0x0001000000000000052a
Alc-Acct-I-Inprof-Octets-64 = 0x00030000000000000000
Alc-Acct-I-Outprof-Octets-64 = 0x00030000000000000000
Alc-Acct-I-Inprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-I-Outprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-I-Inprof-Octets-64 = 0x00050000000000000000
Alc-Acct-I-Outprof-Octets-64 = 0x00050000000000000000
Alc-Acct-I-Inprof-Pkts-64 = 0x00050000000000000000
Alc-Acct-I-Outprof-Pkts-64 = 0x00050000000000000000
Alc-Acct-O-Inprof-Octets-64 = 0x00010000000000000000
Alc-Acct-O-Outprof-Octets-64 = 0x000100000000000003154
Alc-Acct-O-Inprof-Pkts-64 = 0x00010000000000000000
Alc-Acct-O-Outprof-Pkts-64 = 0x00010000000000000009a
Alc-Acct-O-Inprof-Octets-64 = 0x00030000000000000000
Alc-Acct-O-Outprof-Octets-64 = 0x00030000000000000000
Alc-Acct-O-Inprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-O-Outprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-O-Inprof-Octets-64 = 0x00050000000000000000
Alc-Acct-O-Outprof-Octets-64 = 0x00050000000000000000
Alc-Acct-O-Inprof-Pkts-64 = 0x00050000000000000000
```

```
Alc-Acct-O-Outprof-Pkts-64 = 0x00050000000000000000
Acct-Unique-Session-Id = "9c1723d05e87c043"
Timestamp = 1342461831
Request-Authenticator = Verified
```

```
Mon Jul 16 11:04:34 2012
Acct-Status-Type = Stop
NAS-IP-Address = 10.1.1.1
User-Name = "cgn_1_ipoe"
Framed-IP-Address = 10.0.0.7
Framed-IP-Netmask = 255.255.255.0
Class = 0x63676e2d636c6173732d7375622d6177617265
Calling-Station-Id = "remote0"
NAS-Identifier = "left-a20"
Acct-Session-Id = "D896FF0000000550045640"
Acct-Session-Time = 322
Acct-Terminate-Cause = User-Request
Event-Timestamp = "Jul 16 2012 11:03:47 PDT"
NAS-Port-Type = Ethernet
NAS-Port-Id = "1/1/5:5.10"
ADSL-Agent-Circuit-Id = "cgn_1_ipoe"
ADSL-Agent-Remote-Id = "remote0"
Alc-Subsc-ID-Str = "CGN1"
Alc-Subsc-Prof-Str = "nat"
Alc-SLA-Prof-Str = "tp_sla_prem"
Alc-Client-Hardware-Addr = "2001:db8:65:05:10:01"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Alc-Acct-I-Inprof-Octets-64 = 0x00010000000000000000
Alc-Acct-I-Outprof-Octets-64 = 0x000100000000000248c4
Alc-Acct-I-Inprof-Pkts-64 = 0x00010000000000000000
Alc-Acct-I-Outprof-Pkts-64 = 0x000100000000000005d9
Alc-Acct-I-Inprof-Octets-64 = 0x00030000000000000000
Alc-Acct-I-Outprof-Octets-64 = 0x00030000000000000000
Alc-Acct-I-Inprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-I-Outprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-I-Inprof-Octets-64 = 0x00050000000000000000
Alc-Acct-I-Outprof-Octets-64 = 0x00050000000000000000
Alc-Acct-I-Inprof-Pkts-64 = 0x00050000000000000000
Alc-Acct-I-Outprof-Pkts-64 = 0x00050000000000000000
Alc-Acct-O-Inprof-Octets-64 = 0x00010000000000000000
Alc-Acct-O-Outprof-Octets-64 = 0x00010000000000003860
Alc-Acct-O-Inprof-Pkts-64 = 0x00010000000000000000
Alc-Acct-O-Outprof-Pkts-64 = 0x000100000000000000b0
Alc-Acct-O-Inprof-Octets-64 = 0x00030000000000000000
Alc-Acct-O-Outprof-Octets-64 = 0x00030000000000000000
Alc-Acct-O-Inprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-O-Outprof-Pkts-64 = 0x00030000000000000000
Alc-Acct-O-Inprof-Octets-64 = 0x00050000000000000000
Alc-Acct-O-Outprof-Octets-64 = 0x00050000000000000000
Alc-Acct-O-Inprof-Pkts-64 = 0x00050000000000000000
Alc-Acct-O-Outprof-Pkts-64 = 0x00050000000000000000
Acct-Unique-Session-Id = "9c1723d05e87c043"
Timestamp = 1342461874
Request-Authenticator = Verified
```

## 7.21 Mapping of Address and Port Using Translation (MAP-T)

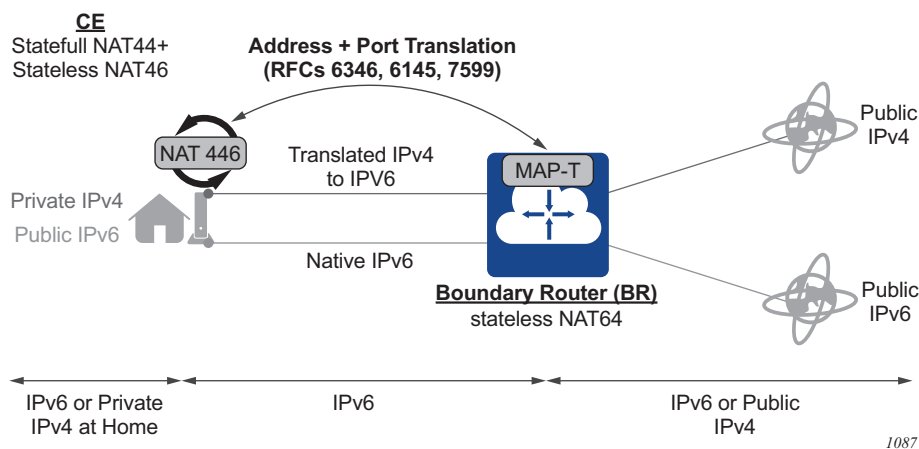


**Note:** The MAP-T feature and commands described in this section apply to the Nokia Virtualized Service Router (VSR) only.

MAP-T is a NAT technique defined in RFC 7599. Its key advantage is the decentralization of stateful NAT while enabling the sharing of public IPv4 addresses among the customer edge (CE) devices. In a nutshell, the CE performs the stateful NAT44 function and translates the resulting IPv4 packet into an IPv6 packet. The IPv6 packet is transported over the IPv6 network to the Border Router (BR), which then translates the IPv6 packet to IPv4 and sends it into the public domain.

As multiple CEs can share a single public IPv4 address, MAP-T must rely on an algorithm (A+P algorithm running on the CEs and BR) to ensure that each CE is assigned a unique port-range on a shared IPv4 public address. In this way, each CE can be uniquely identified at the BR by a combination of the shared IPv4 public address and unique port-range. A set of CEs and BR that share a common set of MAP algorithm rules constitutes a MAP domain. Figure 80 shows a network-level view of Map-T.

**Figure 80 MAP-T Network Level View**



MAP-T offers the following advantages mainly as a result of its stateless BR operation:

- **Improved Scaling**

State maintenance is decentralized, which enables better scaling.

- **Simplified Redundancy**

There are no sessions synchronized between redundant BRs and this translates to simplified redundancy.

- **Reduced Logging**

As there are no NAT resources in the BR that require logging, only configuration changes in the BR are logged, which reduces the volume of logging data.

- **Simpler Communication**

MAP-T simplifies user-to-user communication.

- **Higher Throughput**

MAP-T offers higher throughput than a stateful solution, with less processing required in the BR.

Mapping of address and port (MAP) is a generic function, regardless of the underlying transport mechanism (MAP-T or MAP-E) used. Each MAP CE is assigned as follows:

- **A shared public IPv4 address with a unique port-range on the shared IPv4 address**

Although a shared IPv4 address is used in most cases, the CE is sometimes assigned a unique IPv4 address or even an IPv4 prefix. This information is used for stateful NAT44 at the CE.

- **An IPv6 prefix (IA-PD)**

A “subnet” from the IPv6 prefix is allocated to the CE as a MAP prefix. The MAP prefix is used to encode public IPv4 information and identify the CE in a MAP domain. The remainder of the IA-PD is used on the LAN side of the CE.

- **An IPv6 address (IA-NA)**

The IPv6 address is independent of MAP and is a regular IPv6 address on the WAN side. The address is used for native end-to-end IPv6 communication (it can participate in forming routing adjacencies and other tasks).

The CE and BR perform the following functions in the MAP-T domain:

- **CE Upstream Direction (IPv4 → IPv6)**

- perform stateful NAT44 function (private → public)
- translate the public IPv4 address and port into an assigned IPv6 MAP source address
- send the IPv6 packet with encoded IPv4 information towards the BR

- **BR Upstream Direction (IPv6 → IPv4)**

- perform an anti-spoof check on the received IPv6 packet to ensure that it is coming from a trusted source (CE)

Anti-spoofing is achieved by checking the source IPv6 MAP address against the configured MAP rules and making sure that the correct public IPv4 address and port-range of the CE are encoded in the CE's source IPv6 MAP address.

- translate the IPv6 packet into an IPv4 packet and forward it into the public domain

- **BR Downstream Direction (IPv6<--IPv4)**

- translate the IPv4 packet into an IPv6 packet according to MAP rules

The IPv4 destination address of the received packet is translated into an IPv6 MAP address of the CE.

- send the IPv6 packet towards the CE

- **CE Downstream Direction (IPv4 <-- IPv6)**

- perform the anti-spoofing function using the destination IPv6 address to verify that the packet is destined for the CE

MAP rules are used to verify that the public IPv4 address and the port-range of the CE is encoded in the IPv6 destination IP address of the received packet (IPv6 MAP address of the CE).

- translate the IPv6 packet into an IPv4 packet
- perform the NAT44 function (public → private)
- forward the packet into the private IPv4 network

Each device (CE and BR) is also responsible for fragmentation handling and ICMP error reporting (MTU too small, TTL expired, and so on).

## 7.21.1 MAP-T Rules

MAP-T rules control the address translation in a MAP-T domain. The mapping rules can be delivered to the devices in the MAP domain using RADIUS or DHCP, or be statically provisioned.

The MAP-T rules are:

- **Basic Mapping Rule (BMR)**

The BMR is used to translate the public IPv4 address and port-range assigned to the CE into the IPv6 MAP address. It is composed of the following parameters:

- rule IPv6 prefix (including prefix length)
- rule IPv4 prefix (including prefix length)

- rule Embedded Address bits (EA-bits) define the portion of the IA-PD that encodes the IPv4 suffix and port-range
- rule Port Parameters (optional)
- Forwarding Mapping Rule (FMR)

The FMR is used for forwarding within the MAP domain. FMRs are instantiated in the BR so that the BR can forward traffic to the CEs. FMRs can also be instantiated in CEs to forward traffic directly between CEs, effectively bypassing BR. The FMR is composed of the same set of parameters as the BMR:

  - rule IPv6 prefix (including prefix length)
  - rule IPv4 prefix (including prefix length)
  - rule Embedded Address (EA) bits that define the portion of the IA-PD that encodes the IPv4 suffix and port-range
  - rule Port Parameters (optional)
- Default Mapping Rule (DMR)

The DMR is used to forward traffic outside the MAP domain. This rule contains the IPv6 prefix of the BR in MAP-T and it is used as the default route.

## 7.21.2 A+P Mapping Algorithm

The public IPv4 address and the port-range information of the CE is encoded in its assigned IPv6 delegated prefix (IA-PD). The BMR holds the key to decode this information from the IA-PD of the CE. The BMR identifies the portion of bits of the IA-PD that contain the suffix of the IPv4 address and the port-set ID (PSID). These bits are called the EA bits. The PSID represents the port-range assigned to the CE.

The public IPv4 address of the CE is constructed by concatenating the IPv4 prefix carried in the BMR and the suffix, which is extracted from the EA bits within the IA-PD. The port-range is identified by the remaining EA bits (PSID portion). The EA bits uniquely identify the CE within the IPv6 network in a given MAP domain.

The *psid-offset* value must be set to a value greater than 0. It represents ports that are omitted from the mapping (for example, well-known ports).

An IPv4 address and port on the private side of the CE must be statefully translated to a public IPv4 address, and the port within the assigned port must be set on the public side of the CE. This ensures that the BR, based on the same MAP rules, can extrapolate the IPv4 source of the packet for verification (anti-spoofing) purposes in the upstream direction, and conversely, to determine the destination IPv6 MAP address (CE address) in the downstream direction (based on the destination IPv4+port).

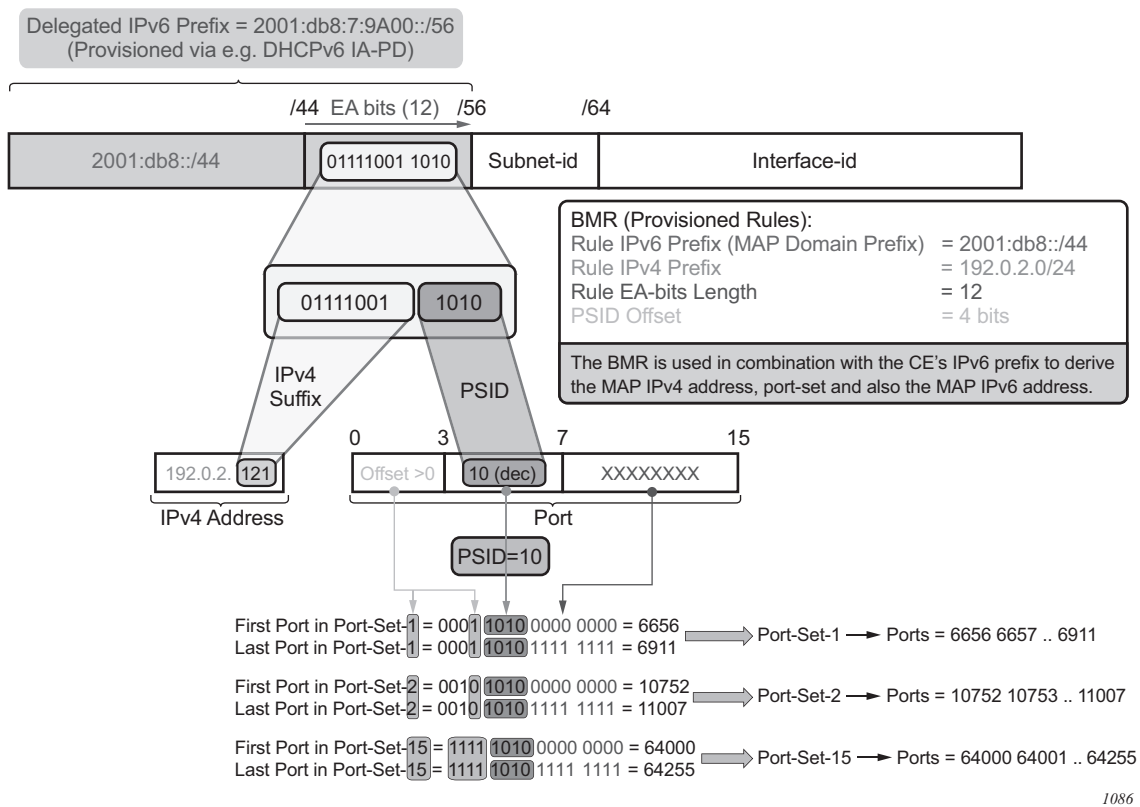


The IPv6 MAP address is constructed by setting the subnet-id in the delegated IPv6 prefix to 0. In this way, the subnet-id of 0 is reserved for MAP function. The remaining subnets can be delegated on the LAN side of the CE.

The interface-id is set to the IPv4 public address and PSID. This is described in RFC 7599, §6.

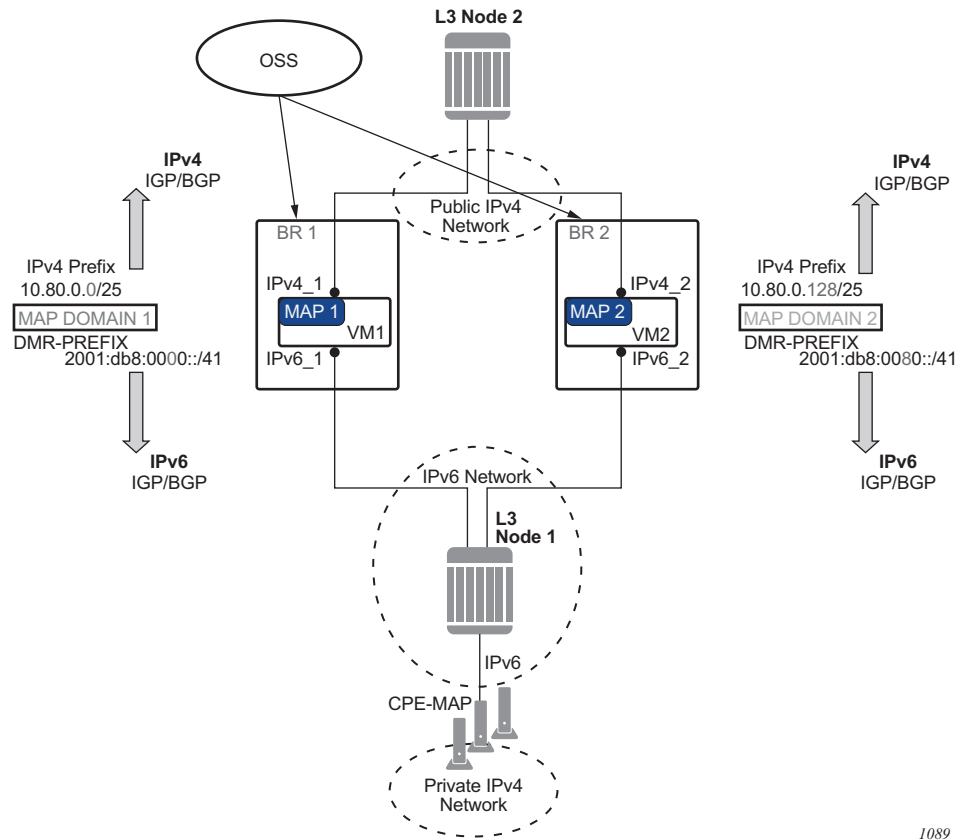
In this way, the IPv4 and IPv6 addresses of the CE are defined and easily converted to each other based on the BMR and the port information in the packet. [Figure 81](#) shows the A+P mapping algorithm.

Figure 81     A+P Mapping



### 7.21.3 Routing Considerations

[Figure 82](#) shows a MAP-T deployment scenario.

**Figure 82** MAP-T Deployment Scenario

1089

The routes related to MAP-T are:

- IPv4 prefixes from the MAP-rules — These routes are advertised in the upstream direction.
- DMR — This is the BR prefix for a specific domain. This route is advertised in the downstream direction.

Routes related to MAP-T are advertised through IPv4 and IPv6 routing protocols. MAP-T routes in the VSR are owned by “protocol nat” with a metric of 50. This can be used to configure an export routing policy when advertising MAP-T routes in IGP or BGP.

Multiple MAP-T domains can be supported in the same routing context.



**Note:** IPv6 IA-PD end-user prefixes are carved out of the IPv6 rule prefix. Aside from MAP-T, IA-PD is used for native IPv6 end-to-end traffic outside of MAP-T. Although the IPv6 rule prefix is not marked as a NAT route in the routing table, it is nonetheless advertised in the upstream direction.

### 7.21.4 Forwarding Considerations in the BR

In the upstream direction, when the BR receives an IPv6 packet destined for the BR prefix, a source-based IPv6 address lookup (anti-spoofing) is performed to verify that the packet is sent by the credible CE.

In the downstream direction, a destination-based IPv4 lookup is performed. This leads to the MAP-T rule entry, which provides the information necessary to derive the IPv6 address of the destination CE.

The MAP-T forwarding function in the VSR is also responsible for:

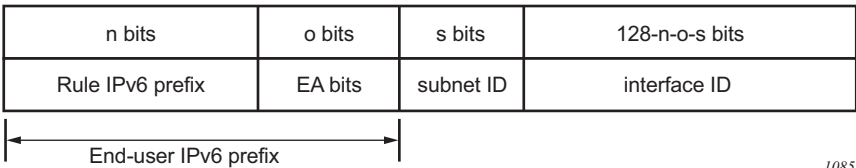
- address conversion between IPv4 and IPv6 based on the BMR rule
- header translation between IPv4 and IPv6, as described in RFC 6145

In address-sharing scenarios, address translation is performed for TCP/UDP and a subset of ICMP traffic; everything else is dropped. In contrast, 1:1 and prefix-sharing scenarios are protocol agnostic.

#### 7.21.4.1 IPv6 Addresses

An IPv6 address of the MAP-T node is constructed according to RFC 7597, §5.2 and RFC 7599, §6. [Figure 83](#) shows the IPv6 address of the MAP-T node.

**Figure 83** IPv6 Address Construction



1085

The subnet ID for a MAP node (CE) is set to 0. [Figure 84](#) shows the node interface (PSID is left-padded with zeros to create a 16-bit field and the IPv4 address is the public IPv4 address assigned to the CE).

**Figure 84     Node Interface**

|         |                           |         |
|---------|---------------------------|---------|
| 16 bits | 128-n-o-s bits<br>32 bits | 16 bits |
| 0       | IPv4 address              | PSID    |

1091

This constructed IPv6 address represents the source IPv6 address of traffic sent from the CE to BR (upstream direction), and the destination IPv6 address in the opposite direction (downstream traffic sent from the BR to the CE).

The source IPv6 address in the downstream direction is a combination of the BR IPv6 prefix and the source IPv4 address (per RFC 7599, §5.1) received in the original packet.

The destination IPv6 address in the upstream direction is a combination of the BR IPv6 prefix and the IPv4 destination address (RFC 7599, §5.1) in the original packet.

**7.21.4.2     1:1 Translations and IPv4 Prefix Translations**

1:1 translations refer to the case in which each CE is assigned a distinct public IPv4 address; that is, there is no public IPv4 address sharing between the CEs. In this case, the PSID field is 0 and the sum of lengths for the IPv4 rule prefix and EA bits is 32. In other words, all the EA bits represent the IPv4 suffix. The public IPv4 address of the CE is created by concatenating the Rule IPv4 Prefix and the EA bits.

IPv4 Prefix translations refer to the case where an IPv4 prefix is assigned to a CE. In this case, the PSID field is 0 and the sum of the lengths for IPv4 rule prefix and EA bits is less than 32.

In both preceding cases, the translations are protocol agnostic; all protocols, not just TCP/UDP or ICMP, will be translated.

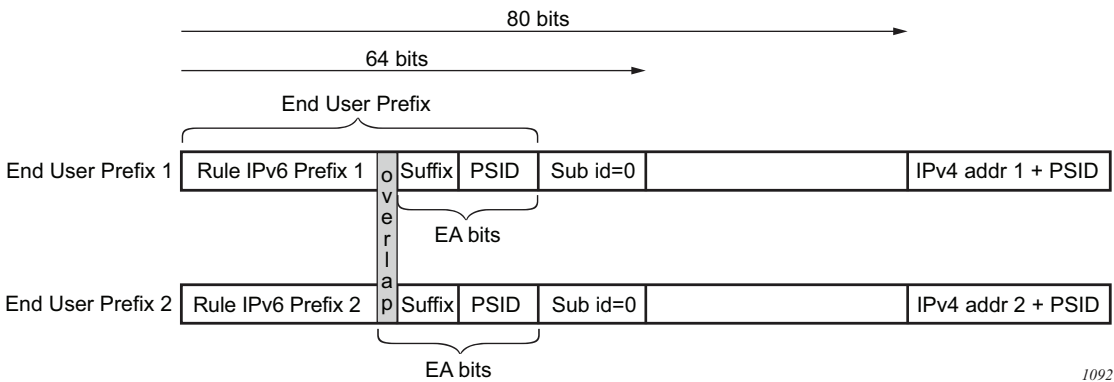
**7.21.4.3     Hub-And-Spoke Topology**

The BR supports hub-and-spoke topology, which means that the BR facilitates communication between MAP-T CEs.

### 7.21.4.4 Rule Prefix Overlap

Rule prefix overlap is not supported because it can cause lookup ambiguity. [Figure 85](#) shows a rule prefix overlap example.

**Figure 85** IPv6 Rule Prefix Overlap



In the case where rule IPv6 prefix 1 is a subset of rule IPv6 prefix 2, the overlapping bits between the EA-bits in end user prefix 2 and the overlapping bits in rule prefix 1 (represented by the shaded sections in [Figure 85](#)) could render end-user prefixes 1 and 2 indistinguishable (everything else being the same) when anti-spoof lookup is performed in the upstream direction. This could result in an incorrect anti-spoofing lookup.

A similar logic can be applied to overlapping IPv4 prefixes in the downstream direction, where the longest prefix match will always lead to the same CE, while the shortest match (leading to a different CE) will not be evaluated.

### 7.21.5 BMR Rules Implementation Example

This section examines an example MAP-T deployment with three MAP rules. The deployment assumes the following:

- There are about 12,000 private IPv4 addresses that need to be translated via MAP-T.
- Each such address should have approximately 4000 ports available per CE. Therefore, the IP address sharing ratio is 16:1; that is, 16 CEs share the same public IP address.
- The public IPv4 addresses that are available to the operator for this translation are from three /24 subnets (10.11.11.0/24, 10.12.12.0/24 and 10.13.13.0/24).

- All users (or CEs) are assigned a /60 IA-PD.

The 12,000 private IPv4 addresses (CEs) in a 16:1 sharing scenario can be covered using three /24 subnets as follows:

$$(3 * 2^8 * 16 = 12,288)$$

The IPv4 rule prefix and EA bits length per rule in this scenario are:

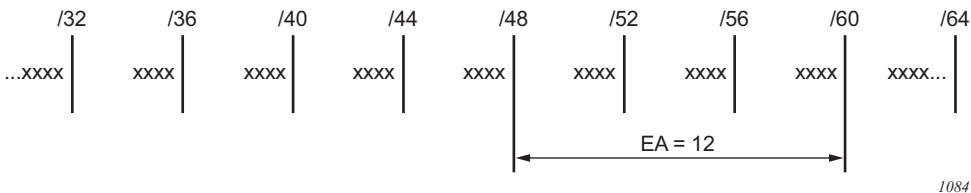
- 10.11.11.0/24    EA length: 12 bits (8 bits for the IPv4 suffix and 4 bits for PSID)
- 10.12.12.0/24    EA length: 12 bits (8 bits for the IPv4 suffix and 4 bits for PSID)
- 10.13.13.0/24    EA length: 12 bits (8 bits for the IPv4 suffix and 4 bits for PSID)

The first 6 bits of the 16 bit port-range are set to 000000 and are reserved for *psid-offset* (ports 0-1023 are reserved); therefore, the user-allocated port space will be calculated as follows:

$$4000 - 64 = 4032 \text{ ports}$$

The IPv6 rule prefix is the next parameter in the MAP rule. [Figure 86](#) shows the relevant bits in the IPv6 address: only bits /32 to /64 are considered; the irrelevant bits of the IPv6 addresses are ignored in this example.

**Figure 86      Determining the Rule IPv6 Prefix**



The following three rules are created in this example:

- Rule 1 will cover subnet 1
- Rule 2 will cover subnet 2
- Rule 3 will cover subnet 3

In each of the three cases, the EA bits extend from the PD length (/60) to the IPv6 rule prefix length (/48).

The IPv6 rule prefix length is determined for each of the three rules. However, the IPv6 rule prefixes must not overlap, see section [7.21.4.4](#) for more information. Non-overlapping IPv6 rule prefixes ensure that each CE is assigned a unique IA-PD. [Table 48](#) describes the rules.

**Table 48** IPv6 Rule Prefixes

|                  | Rule 1              | Rule 1              | Rule 1              |
|------------------|---------------------|---------------------|---------------------|
| IPv6 rule prefix | 2001:db8:0000::/48- | 2001:db8:0001::/48- | 2001:db8:0002::/48- |
| IPv4 rule prefix | 10.11.11.0/24       | 10.12.12.0/24       | 10.13.13.0/24       |
| EA bits          | 12                  | 12                  | 12                  |
| Paid-Offset      | 6                   | 6                   | 6                   |

The final step is to ensure that the DHCPv6 server hands out proper end-user prefixes (IA-PD), and the rules are also delegated.

In this example, each /48 IPv6 rule prefix supports 4,000 MAP-T CEs, where each CE can further delegate 15 IPv6 “subnets” on the LAN side and each CE is allocated about 4,000 ports to use in stateful NAT44.



**Note:** The VSR-BR supports only IPv6 rule prefixes of the same length within a given domain. To accommodate a different prefix length assignment for IA-PD (for example /56), create another domain with a different IPv6 rule prefix (/44 instead of /48).

## 7.21.6 ICMP

The following ICMPv4 messages are supported in MAP-T on the VSR; other types of ICMP messages are not supported:

- ICMP Query messages — These messages contain an identifier field in the ICMP header, which is referred to as the “query identifier” or “query-id” and it is used in MAP-T in the same way as the L4 ports are used in TCP or UDP. ICMP Echo Req/Rep (PING) and traceroute are examples that rely on ICMP Query messages.
- ICMP Error messages — These messages contain the embedded original datagram that triggers the ICMP error message. The ICMP error messages do not contain the **query-id** field.

The ICMP Query messages and ICMP Error messages are supported regardless of whether they are just passing through a VSR (transit messages), or are terminated or generated in or from a VSR.

The NAT-related ICMPv4 behavior is described in RFC 5508. The following NAT messages are supported in the MAP-T VSR (RFC 5508, §7, Requirement 10a):

- ICMPv4 Error Message: Destination Unreachable Message (Type 3)
- ICMPv4 Error Message: Time Exceeded Message (Type 11)
- ICMPv4 Query Message: Echo and Echo Reply Messages (Type 8 and Type 0)

## 7.21.7 Fragmentation

The IPv6 header of the IPv4-translated packet in MAP-T can be up to 28 bytes larger than the IPv4 header (40-byte IPv6 header plus 8-byte fragmentation header versus 20-byte IPv4 header). In the case where the IPv4-to-IPv6 translated packet is larger than the IPv6 MTU, the original IPv4 packet will be fragmented so that the size of the translated IPv6 packet is within IPv6 MTU. IPv6 packets will never be fragmented, although they may contain the fragmentation header that carries fragmentation information related to the original IPv4 packet/fragment.

The IPv6 MTU in the VSR is configurable for each MAP-T domain. The L2 header is excluded from the IPv6 MTU.

### 7.21.7.1 Fragmentation in the Downstream Direction

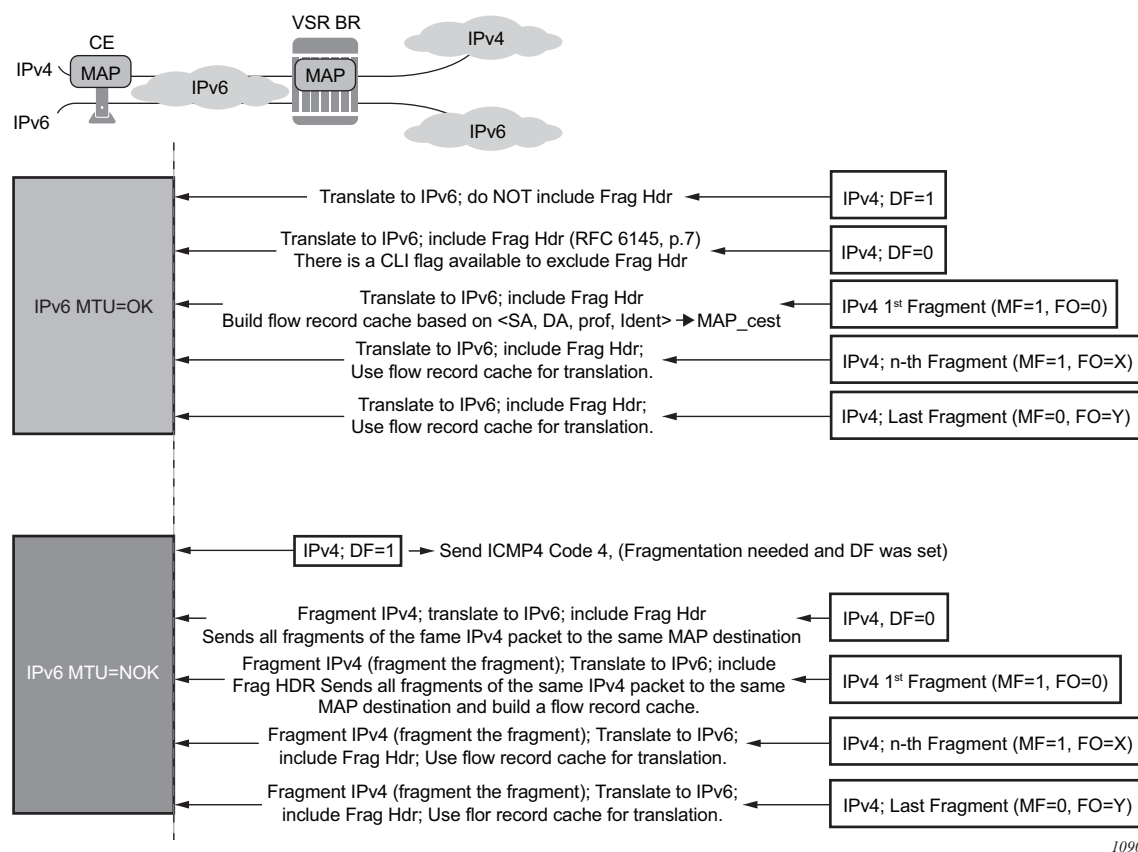
All fragments of the same IPv4 packet are translated and sent towards the same CE. As the second and consecutive fragments do not contain any port information, the translation is performed based on the *<SA, DA, Prot, Ident>* cached flow records extracted from the IPv4 header.

Note that the VSR may further fragment an IPv4 fragment that it has received in order to fit it within the IPv6 MTU.

[Figure 87](#) shows downstream fragmentation scenarios.



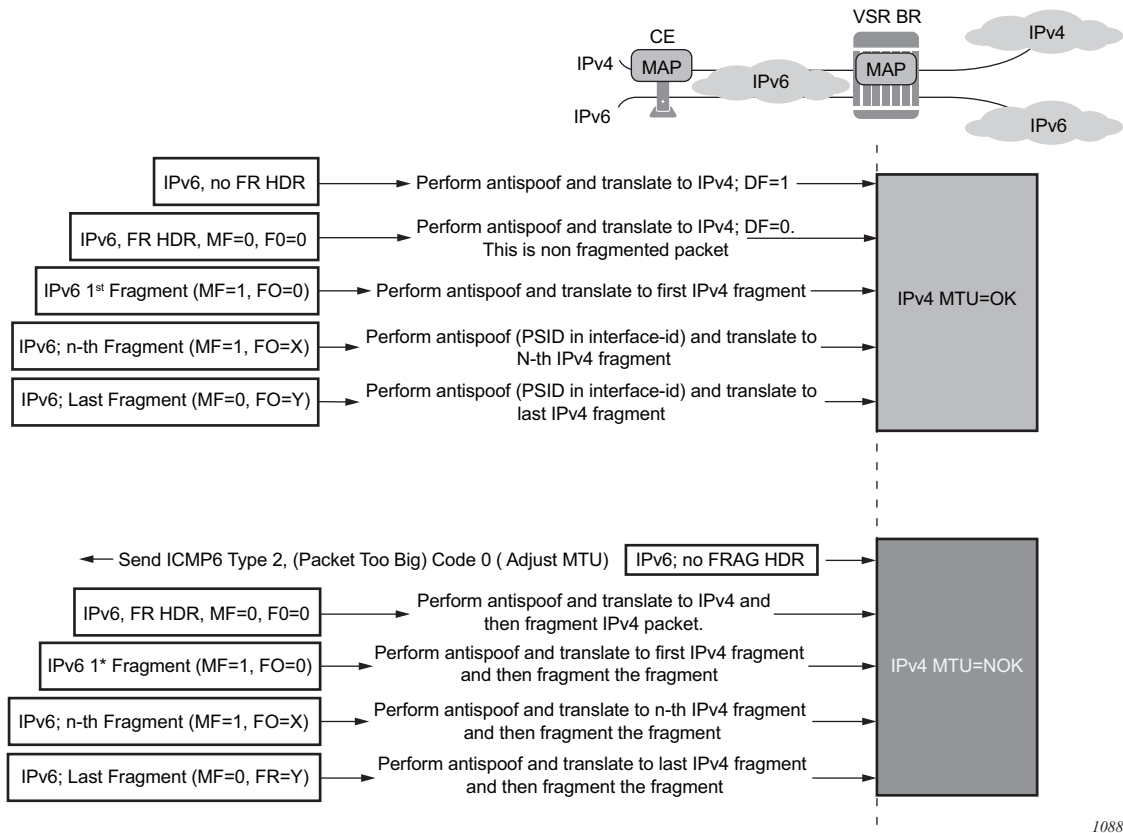
**Figure 87** Fragmentation in the Downstream Direction



1090

### 7.21.7.2 Fragmentation in the Upstream Direction

In the upstream direction, the received IPv6 fragments are artifacts of the IPv4 packets being fragmented on the CP side, before they are translated into IPv6. No flow caching is performed in the upstream direction. The BR performs an anti-spoof for each fragment and if the anti-spoof is successful, the fragment is translated to IPv4. [Figure 88](#) shows the upstream fragmentation scenario.

**Figure 88**      **Fragmentation in the Upstream Direction**

1088

### 7.21.7.3 Fragmentation Statistics

Fragmentation statistics can be cleared using the **clear nat map frag-stats** command. The following fragmentation statistics are available:

- **Rx Resolved Frags**

This counter shows fragments that were resolved and never buffered; for example:

- first fragments (MF=1, FO=0), which are always resolved by definition
- non-first fragments with matching flow records

- **Rx Unresolved Frags**

This counter shows the number of packets that were queued in the system since the last clear command was invoked. For example, packets with out-of-order fragments without a matching flow record (missing 1st fragment) can be eventually resolved and forwarded, or discarded (for example, due to timeout).

- **Tx Frags**

This counter shows the fragments that were transmitted (**Rx Resolved** and **Rx Unresolved** that were eventually resolved) out of fragmentation logic within the VSR. There is no guarantee that the fragments will be transmitted out of the system as they may be dropped on egress because of congestion or restrictions imposed by the configured filter.

- **Dropped Frags**

This counter represents the fragments that are dropped due to fragmentation issues such as timeout, buffer full, and so on.

- **Buffers in Use**

This counter represents the amount of buffered fragments expressed as a percentage of the maximum buffer space that can be used for fragmentation.

- **Max Buffers**

This is a non-cumulative counter that represents the maximum number of buffers allocated since the last **clear** command. The counter captures the highest value of the **buffers-in-use** counter since the last **clear** command. The unit of this counter is the percentage of the total buffer space that can be used by fragmentation.

- **Created Flows**

This is a cumulative counter that represents the total number of flow records since the last **clear** command was invoked. It only counts the first fragment. It represents the number of fragmented packets that were processed by the system since the last **clear** command. This counter does not indicate the number of flows (packets whose fragments were transmitted fully) that were actually transmitted.

- **Flows in Use**

The counter gives an approximation of the number of flow records currently in use and the number of fragmented packets being processed at the time the counter was invoked, as a percentage.

- **Max Flows**

A non-cumulative counter that represents the maximum number of flow records reached since the last **clear** command. The counter shows the highest value of the **flows-in-use** counter since the last **clear** command, as a percentage.

- **Flow Collisions**

This counter represents the number of overlapping first fragments. For example, in the case where a flow record already exists and another first fragment for the flow is received.

- **Exceeded Max Timeouts**

This counter shows the number of fragments that have timed out since the last clear command. The represented fragments are:

- Rx unresolved (buffered) fragments that have timed out due to a missing first fragment
- deleted flow-records because they have not received all fragments within the timeout period
- **Exceeded Max Flows**  
This counter represents the number of times that the flows in the system has exceeded the maximum supported value.
- **Exceeded Max Buffers**  
This counter represents the number of times that the buffers in the system has exceeded the maximum supported value.
- **Exceeded Max Buffers Per Flow**  
This counter represents the number of times that the fragment counter per flow has exceeded its limit.

## 7.21.8 Maximum Segment Size (MSS) Adjust

The MSS Adjust feature is used to prevent fragmentation of TCP traffic. The TCP synchronize/start (SYN) packets are intercepted and their MSS value inspected to ensure that it conforms with the configured MSS value. If the inspected value is greater than the value configured in the VSR BR, the MSS value in the packet is lowered to match the configured value before the TCP SYN packet is forwarded.

As the end nodes governing the MSS value are IPv4 nodes, this feature is supported for IPv4 packets only.

An MSS adjust is performed in both the upstream and downstream directions.

## 7.21.9 Statistics Collection

The VSR BR maintains a count of the forwarded and dropped packets/octets per MAP-T-domain per direction. The statistics are collected on ingress (upstream v6 and downstream v4) and stored in 64-bit counters

## 7.21.10 Logging

As with any NAT operation where the identity of the user is hidden behind the NAT identity, logging of the NAT translation information is required. In the MAP-T domain, NAT logging is based on configuration changes because the user identity can be derived from the configured rules.

A system can have a large number of rules and each configured MAP rule generates a separate log. As a result, the amount of logs generated can be substantial. Logging is explicitly enabled using a log event.

A NAT log contains information about the following:

- MAP type (map-t)
- map-domain name
- map-rule name
- v6 rule-prefix
- v4 rule-prefix
- EA bits
- psid-offset bits
- associated routing context for the MAP-T rule
- timestamp

A MAP rule log is generated when both of the following conditions are met:

- a MAP rule is activated and deactivated in the system (administratively **shutdown/no shutdown**, corresponding MAP domain is associated/dissociated from the routing context, corresponding MAP domain is **shutdown/no shutdown**, and so on)
- event **tmnxNatMapRuleChange (id=2036)** has been enabled in event-control

Example:

```
551 2016/04/22 14:56:35.44 UTC MINOR: NAT #2036 vprn220 NAT MAP
"map-type=map-t map-domain=domain-name-1 rule-name=rule-name-1 rule-
prefix=2001:db8::/44 ipv4-prefix=192.168.10.0/24 ea-length=12 psid-
offset=6 enabled router=vprn220 at 2016/04/22 14:56:35"
```

## 7.21.11 Licensing

A valid MAP-T license is required to enable the MAP-T functionality in the VSR BR. A MAP-T domain can only be instantiated with the appropriate license, which enables the following CLI command:

```
configure
service
 vprn <id> customer <cust-id> create
 map-domain <domain-name>
```

## 7.21.12 Configuration

The MAP-T configuration consists of defining MAP-T parameters within a template. The MAP-T domain is then instantiated by applying (referencing) this template within a routing (router or VPRN) context.

### Defining a MAP Domain Template

```
configure
service
 nat
 map-domain <domain-name> create
 [no] shutdown
 dmr-prefix <ipv6-prefix>
 tcp-mss-adjust <segment-size>
 mtu <mtu-size>
 ip-fragmentation
 [no] v6-frag-header
 mapping-rule <rule-name>
 [no] shutdown
 rule-prefix <ipv6-prefix>
 ipv4-prefix <ipv4-prefix>
 ea-length <ea-bits-length>
 psid-offset <psid-offset-len>
 :
 mapping-rule <rule-name>
 [no] shutdown
 rule-prefix <ipv6-prefix>
 ipv4-prefix <ipv4-prefix>
 ea-length <ea-bits-length>
 psid-offset <psid-offset-len>
 :
 up to 256 rules per domain
```

### MAP-T Domain Instantiation

```
configure
service vprn <id> | router
 nat
```

```
map-t
 map-domain <domain-name>
```

## MAP Domain Example Template

The following example shows the MAP domain template for the BMRs defined [BMR Rules Implementation Example](#).

```
configure
service
 nat
 map-domain domain_1 create
 no shutdown
 dmr-prefix 2001:db8:0100::/64
 mapping-rule rule_1
 no shutdown
 rule-prefix 2001:db8:0000::/48
 ipv4-prefix 10.11.11.0/24
 ea-length 12
 psid-offset 6
 mapping-rule rule_2
 no shutdown
 rule-prefix 2001:db8:0001::/48
 ipv4-prefix 10.12.12.0/24
 ea-length 12
 psid-offset 6
 mapping-rule rule_3
 no shutdown
 rule-prefix 2001:db8:0002::/48
 ipv4-prefix 10.13.13.0/24
 ea-length 12
 psid-offset 6
```

## MAP-T Domain Instantiation Example

The following example shows the MAP-T domain instantiation for the BMRs defined in [BMR Rules Implementation Example](#).

```
configure
service
 vprn 10
 nat
 map-t
 map-domain domain_1
```

### 7.21.12.1 Modifying MAP-T Parameters When the MAP-T Domain is Active

You can add new rules to an existing MAP-T domain while the MAP-T domain is instantiated and forwarding traffic. However, each rule must be in the **shutdown** state before any of its parameters are modified.

A MAP-T domain must be in the **shutdown** state to modify the *dmr-prefix* parameter. The remaining parameters (**tcp-mss-adjust**, **mtu**, **ip-fragmentation**) can be modified while the domain is active.

A MAP domain does not have to be in a **shutdown** state when rule modification is in progress.

### 7.21.13 Inter-Chassis Redundancy

MAP natively provides multi-chassis redundancy through the use of the anycast BR prefix that is advertised from multiple nodes.

As there is no state maintenance in the MAP-T BR, any BR node can process traffic for the same domain at all times. The only traffic interruption during the switch-over is for the fragmented traffic in the downstream direction being handled at the time of switchover (the flow record cache is not synchronized between the nodes).



## 7.22 Configuring NAT

This section provides information to configure NAT using the command line interface.

### 7.22.1 ISA Redundancy

The 7750 SR supports ISA redundancy to provide reliable NAT even when an MDA fails. The **active-mds-limit** command allows an operator to specify how many MDAs will be active in a given NAT group. Any number of MDAs configured above the active-mds-limit will be spare MDAs; they take over the NAT function if one of the current active MDAs fail.

A sample configuration is as follows:

```
configure
 isa
 nat-group 1 create
 active-mds-limit 1
 mda 1/2
 mda 2/2
 no shutdown
 exit
 exit
exit
```

Show commands are available to display the actual state of a nat-group and its corresponding MDAs:

```
show isa nat-group 1
=====
ISA NAT Group 1
=====
Admin state : inService Operational state : inService
Active MDA limit : 1 Reserved sessions : 0
High Watermark (%) : (Not Specified) Low Watermark (%) : (Not Specified)
Last Mgmt Change : 01/11/2010 15:05:36
=====
ISA NAT Group 1 members
=====
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio

1 1 active 1/2 0 0 0 N 0

No. of members: 1
=====
```

A maximum of four nat-groups can be configured. This gives the operator the ability to differentiate between different traffic types. Normal traffic could be routed to nat-group one, where a limited number of MDA without spare MDAs are available, while high priority traffic could make use of nat-group two, where several active MDAs and a spare MDA are configured. A maximum of six MDAs per nat-group can be configured.

A nat-group cannot become active (no shutdown) if the number of configured MDAs is lower than the active-mda-limit.

A given MDA can be configured in several nat-groups but it can only be active in a single nat-group at any moment in time. Spare MDAs can be shared in several nat-groups, but a spare can only become active in one nat-group at a time. Changing the active-mda-limit, adding or removing MDAs can only be done when the nat-group is shutdown.

Nat-groups that share spare MDAs must be configured with the same list of MDAs. It is possible to remove/add spare MDAs to a nat-group while the nat-group is admin enabled.

```
Configure
 isa
 nat-group 1 create
 active-mda-limit 1
 mda 1/2
 mda 2/2
 mda 3/1
 no shutdown
 exit
 nat-group 2 create
 active-mda-limit 1
 mda 1/2
 mda 2/2
 mda 3/1
 no shutdown
 exit
 exit
exit
```

Through show commands, it is possible to display an overview of all the nat-groups and MDAs.

```
show isa nat-group
=====
ISA NAT Group Summary
=====
```

| Mda | Group 1 | Group 2 |
|-----|---------|---------|
| 1/1 | active  | busy    |
| 2/2 | busy    | active  |
| 3/1 | standby | standby |

```
=====
```

If an MDA fails, the spare (if available) will take over. All active sessions will be lost, but new incoming sessions will make use of the spare MDA.

In case of an MDA failure in a nat-group without any spare MDA, all traffic towards that MDA will be black-holed.

For L2-aware NAT, the operator has the possibility to clear all the subscribers on the affected MDA (clear nat isa), terminating all the subscriber leases. New incoming subscribers will make use of the MDAs that are still available in the nat-group.

## 7.22.2 NAT Layer 2-Aware Configurations

The following sections provide NAT Layer 2-Aware configurations.

```
#-----
echo "Card Configuration"
#-----
 card 1
 card-type iom3-xp
 mda 1
 mda-type m60-10/100eth-tx
 exit
 mda 2
 mda-type isa-bb
 exit
 exit
 card 2
 card-type iom3-xp
 mda 1
 mda-type m60-10/100eth-tx
 exit
 mda 2
 mda-type isa-bb
 exit
 exit

#-----
echo "ISA Configuration"
#-----
 isa
 nat-group 1 create
 description "1 active + 1 spare"
 active-mds-limit 1
 mda 1/2
 mda 2/2
 no shutdown
 exit
 exit

#-----
echo "Router (Network Side) Configuration"
#-----
 router
 ...
```

```

#-----
echo "NAT (Network Side) Configuration"
#-----
 nat
 outside
 pool "pool1" nat-group 1 type l2-aware create
 address-range 10.81.0.0 10.81.0.200 create
 exit
 no shutdown
 exit
 exit
exit
#-----
echo "Service Configuration"
#-----
 service
 customer 1 create
 description "Default customer"
 exit
 ...
 vprn 100 customer 1 create
 ...
 nat
 outside
 pool "pool2" nat-group 1 type l2-aware create
 address-range 10.0.0.0 10.0.0.200 create
 exit
 no shutdown
 exit
 exit
 exit
 exit

 vprn 101 customer 1 create
 ...
 nat
 inside
 l2-aware
 # Hosts in this service with IP addresses in these ranges
 # will be subject to l2-aware NAT.
 address 10.0.0.1/29
 address 10.1.0.1/29
 exit
 exit
 exit
 exit
 ...
 nat
 nat-policy "l2-aware-nat-policy1" create
 pool "pool1" router Base
 exit
 nat-policy "l2-aware-nat-policy2" create
 pool "pool2" router 100
 exit
 exit
 ...
 exit
#-----
echo "Subscriber-mgmt Configuration"

```

```
#-----
subscriber-mgmt
Subscribers using these sub-profiles will be subject to l2-aware NAT.
The configured nat-policies will determine which IP pool will be used.
sub-profile "l2-aware-profile1" create
 nat-policy "l2-aware-nat-policy1"
exit
sub-profile "l2-aware-profile2" create
 nat-policy "l2-aware-nat-policy2"
exit
...
exit
```

## 7.22.3 Large Scale NAT Configuration

The following sections provide Large Scale NAT configuration examples.

```
configure
#-----
echo "Card Configuration"
#-----
card 3
 card-type iom3-xp
 mda 1
 mda-type isa-bb
 exit
 mda 2
 mda-type isa-bb
 exit
exit
#-----
echo "ISA Configuration"
#-----
isa
 nat-group 1 create
 active-mds-limit 2
 mda 3/1
 mda 3/2
 no shutdown
 exit
exit
#-----
echo "Filter Configuration"
#-----
filter
 ip-filter 123 create
 entry 10 create
 match
 src-ip 10.0.0.1/8
 exit
 action nat
 exit
exit
exit
#-----
```

```
echo "NAT (Declarations) Configuration"
#-----
 service
 nat
 nat-policy "ls-outPolicy" create
 exit
 exit
 exit
#-----
echo "Service Configuration"
#-----
 service
 customer 1 create
 description "Default customer"
 exit
 vprn 500 customer 1 create
 interface "ip-192.168.113.1" create
 exit
 nat
 outside
 pool "nat1-pool" nat-group 1 type large-scale create
 port-reservation ports 200
 address-range 10.81.0.0 10.81.6.0 create
 exit
 no shutdown
 exit
 exit
 exit
 exit
 vprn 550 customer 1 create
 interface "ip-192.168.13.1" create
 exit
 exit
 nat
 nat-policy "ls-outPolicy" create
 pool "nat1-pool" router 500
 timeouts
 udp hrs 5
 udp-initial min 4
 exit
 exit
 exit
 vprn 500 customer 1 create
 router-id 10.21.1.2
 route-distinguisher 500:10
 vrf-target export target:500:1 import target:500:1
 interface "ip-192.168.113.1" create
 address 192.168.113.1/24
 static-arp 192.168.113.5 2001:db8:01:01:00:01
 sap 1/1/1:200 create
 exit
 exit
 no shutdown
 exit
 vprn 550 customer 1 create
 router-id 10.21.1.2
 route-distinguisher 550:10
 vrf-target export target:550:1 import target:550:1
 interface "ip-192.168.13.1" create
```

```
 address 192.168.13.1/8
 sap 1/2/1:900 create
 ingress
 filter ip 123
 exit
 exit
 exit
nat
 inside
 nat-policy "ls-outPolicy"
 exit
exit
no shutdown
exit
exit
exit all
```

## 7.22.4 NAT Configuration Examples

The following output displays example configurations.

VPRN service example:

```
configure service vprn 100 nat
 inside
 nat-policy "priv-nat-policy"
 destination-prefix 0.0.0.0/0
 dual-stack-lite
 subscriber-prefix-length 128
 address 2001:db8:470:1F00:FFFF:190
 tunnel-mtu 1500
 exit
 no shutdown
 exit
 redundancy
 no peer
 no steering-route
 exit
 subscriber-identification
 shutdown
 no attribute
 no description
 no radius-proxy-server
 exit
 l2-aware
 exit
exit
outside
 no mtu
exit
```

Router NAT example:

```
configure router nat
```

```
outside
 no mtu
 pool "privpool" nat-group 3 type large-scale create
 no description
 port-reservation blocks 128
 port-forwarding-range 1023
 redundancy
 no export
 no monitor
 exit
 subscriber-limit 65535
 no watermarks
 mode auto
 address-range 10.0.0.5 10.0.0.6 create
 no description
 no drain
 exit
 no shutdown
 exit
 pool "pubpool" nat-group 1 type large-scale create
 no description
 port-reservation blocks 1
 port-forwarding-range 1023
 redundancy
 no export
 no monitor
 exit
 subscriber-limit 65535
 no watermarks
 mode auto
 address-range 192.168.8.241 192.168.8.247 create
 no description
 no drain
 exit
 no shutdown
 exit
exit
```

### Service NAT example:

```
configure service nat
 nat-policy "priv-nat-policy" create
 alg
 ftp
 rtsp
 sip
 exit
 block-limit 4
 no destination-nat
 no description
 filtering endpoint-independent
 pool "privpool" router Base
 no ipfix-export-policy
 port-limits
 forwarding 64
 no reserved
 no watermarks
 exit
```



```
priority-sessions
exit
session-limits
 max 65535
 no reserved
 no watermarks
exit
timeouts
 icmp-query min 1
 sip min 2
 no subscriber-retention
 tcp-established hrs 2 min 4
 tcp-syn sec 15
 no tcp-time-wait
 tcp-transitory min 4
 udp min 5
 udp-initial sec 15
 udp-dns sec 15
exit
no tcp-mss-adjust
no udp-inbound-refresh
exit
nat-policy "pub-nat-policy" create
 alg
 ftp
 no rtsp
 no sip
 exit
 block-limit 1
 no destination-nat
 no description
 filtering endpoint-independent
 pool "pubpool" router Base
 no ipfix-export-policy
 port-limits
 no forwarding
 no reserved
 no watermarks
 exit
 priority-sessions
 exit
 session-limits
 max 65535
 no reserved
 no watermarks
 exit
 timeouts
 icmp-query min 1
 sip min 2
 no subscriber-retention
 tcp-established hrs 2 min 4
 tcp-syn sec 15
 no tcp-time-wait
 tcp-transitory min 4
 udp min 5
 udp-initial sec 15
 udp-dns sec 15
 exit
 no tcp-mss-adjust
```

```
no udp-inbound-refresh
exit
```

## 7.23 Configuring VSR-NAT

This section provides information about the VSR-NAT functionality, including licensing requirements, statistics collection, and examples of **show** command output.

### 7.23.1 VSR-NAT Licensing

Appropriate licensing is required to enable the VSR-NAT functionality in the system. However, no further licensing enforcement is performed based on resource utilization, such as the consumed bandwidth or the number of NAT bindings.

The following NAT-related functionality is enabled through licensing:

- LSN (LSN44, DS-Lite, and NAT64)
- L2-Aware NAT
- UPnP
- Geo-redundancy

You can use the CLI or MIB on VSR-NAT to get more information about the number of LSN bindings and LSN bandwidth.

[Table 49](#) describes the licenses required to unlock the VSR-NAT functionality.

**Table 49 NAT Licenses Required to Unlock NAT Functionality**

| NAT License Title | Functionality Enabled                                                                                                                                                                                             | License Purchased                                                                                                                                                                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LSN               | LSN Pool <ul style="list-style-type: none"><li>• <b>configure router nat outside pool <i>name</i> type large-scale</b></li><li>• <b>configure service nat outside pool <i>name</i> type large-scale</b></li></ul> | <p>The following two scaling licenses are required:</p> <ul style="list-style-type: none"><li>• license for the number of LSN bindings</li><li>• license for consumed bandwidth</li></ul> <p>You must purchase both licenses to enable the LSN functionality.</p> |

**Table 49 NAT Licenses Required to Unlock NAT Functionality (Continued)**

| NAT License Title | Functionality Enabled                                                                                                                                                                                              | License Purchased                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2AWARE           | L2Aware Pool <ul style="list-style-type: none"> <li>• <b>configure router nat outside pool</b> <i>name type l2-aware</i></li> <li>• <b>configure service nat outside pool</b> <i>name type l2-aware</i></li> </ul> | Purchase the L2-Aware license to enable the functionality. The LSN scaling license is not required.<br><b>Note:</b> The L2-Aware NAT functionality can only be used with the VBNG. |
| UPnP              | UPnP commands <ul style="list-style-type: none"> <li>• <b>configure subscriber-mgmt sub-profile</b> <i>sub-prof-name upnp-policy upnp-pol-name</i></li> </ul>                                                      | Purchase the UPnP license to enable the functionality.<br><b>Note:</b> The UPnP functionality can only be used with the L2-Aware NAT.                                              |
| GEO REDUNDANCY    | Geo-redundancy Pool <ul style="list-style-type: none"> <li>• <b>configure router nat outside pool</b> <i>redundancy</i></li> <li>• <b>configure service nat outside pool</b> <i>redundancy</i></li> </ul>          | Purchase the Geo Redundancy license to enable the functionality.                                                                                                                   |

## 7.23.2 Statistics Collection For LSN Bindings

A NAT subscriber is an internal entity whose true identity is hidden outside the network. The NAT subscriber is represented by a binding that is a set of stateful mappings between the internal and external representations of the subscriber. From the licensing perspective, the terms “NAT bindings” and “NAT subscribers” can be used interchangeably.

VSR-NAT collects the number of LSN subscribers for licensing purposes; the L2-Aware NAT subscribers are excluded from this count. An LSN subscriber is defined as follows:

- Large Scale NAT44 (or CGN): the subscriber is an internal IPv4 address.
- DS-Lite: the subscriber is identified by the CPE IPv6 address (B4 element) or an IPv6 prefix. The selection of the address or prefix as the representation of a DS-Lite subscriber is configuration-dependent.
- NAT64: the subscriber is an IPv6 address.

The number of LSN subscribers (LSN44, DS-Lite, and NAT64) in VSR-NAT is sampled every hour on the hour (for example, at 00:00 am, 01:00 am, 02:00 am, and so on). Each sample is a snapshot of the number of subscribers at the time that the statistics are collected.

The CLI can be used to view the following information:

- 24 samples (one per hour) in the current day
- Maximum value for each of the last 7 days
- Average value for each of the last 7 days
- Maximum value since the system booted

For the list of CLI commands available for use, see [VSR-NAT Show Command Examples](#).

### 7.23.3 Statistics Collection For LSN Bandwidth

The measurement of LSN bandwidth includes translated packets and octets in the upstream and downstream direction. Packets that are rejected for any reason and traffic carrying logging information are both excluded from the statistics.

LSN bandwidth statistics for VSR-NAT are collected every 10 minutes. The bandwidth is derived as a difference in octet count between the two consecutive collection intervals, divided by a 10 minute interval. There is no bandwidth differentiation per LSN type (LSN44, DS-Lite, and NAT64) or per direction. Aggregate bandwidth values per node are maintained in kb/s units. L2-Aware NAT and WLAN GW statistics are not included in the statistics collection.

The CLI can be used to view the following LSN bandwidth information:

- 144 bandwidth values for the current day (bandwidth statistics are collected every 10 minutes)
- Maximum bandwidth value for each of the last 7 days
- Average bandwidth value for each of the last 7 days
- Maximum bandwidth value since the system booted

For the list of CLI commands available for use, see section [7.23.5 VSR-NAT Show Command Examples](#).

### 7.23.4 Statistics Collection and HA

The LSN and subscriber statistics are synchronized between DP-VMs, where DP-VM redundancy is deployed.

## 7.23.5 VSR-NAT Show Command Examples

The following CLI commands are available for use:

- `show system license-statistics 24-hours application nat`
- `show system license-statistics week application nat`
- `show system license-statistics peak application nat`

The following output shows examples of NAT statistics.

Weekly display example:

```
*A:Dut-A>show system license-statistics week application nat
=====
week license statistics for nat
=====
index time average peak

LSN subscribers
1 2016/02/01 00:00:00 370 456
2 2016/01/31 00:00:00 375 512
3 2016/01/30 00:00:00 374 510
4 2016/01/29 00:00:00 373 478
5 2016/01/28 00:00:00 360 450
6 2016/01/27 00:00:00 370 496
7 2016/01/26 00:00:00 373 503
LSN bandwidth
1 2016/02/01 00:00:00 12472623 12472623
2 2016/01/31 00:00:00 12472623 12472623
3 2016/01/30 00:00:00 12472623 12472623
4 2016/01/29 00:00:00 12472623 12472623
5 2016/01/28 00:00:00 12472623 12472623
6 2016/01/27 00:00:00 12472623 12472623
7 2016/01/26 00:00:00 12472623 12472623

No. of license statistics entries: 14
=====
```

24-hour display example:

```
*A:Dut-A# show system license-statistics 24-hours application nat
=====
24 hours license statistics for nat
=====
index time value

LSN subscribers
1 2016/06/29 19:00:00 512
2 2016/06/29 20:00:00 512
LSN bandwidth
1 2016/06/29 18:10:00 0
2 2016/06/29 18:20:00 0
3 2016/06/29 18:30:00 0
4 2016/06/29 18:40:00 2996286
```

```

5 2016/06/29 18:50:00 12472524
6 2016/06/29 19:00:00 12472424
7 2016/06/29 19:10:00 12471020
8 2016/06/29 19:20:00 12471980
9 2016/06/29 19:30:00 12471566
10 2016/06/29 19:40:00 12471881
11 2016/06/29 19:50:00 12472116
12 2016/06/29 20:00:00 12472623

No. of license statistics entries: 14
=====

```

#### Peak display example:

```

=====
*A:Dut-A# show system license-statistics peak application nat
=====
peak license statistics for nat
=====
 time peak

LSN subscribers 2016/06/29 19:00:00 512
LSN bandwidth 2016/06/29 20:00:00 12472623

No. of license statistics entries: 2
=====

```

[Table 50](#) describes the NAT statistics output fields.

**Table 50 NAT Statistics Output Fields**

| Label   | Description                                                                                                                                                                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index   | The entry number of the displayed value.<br>A weekly display contains 7 entries, one for each of the last 7 days.<br>A 24-hour display can contain up to 24 values for NAT subscribers (statistics are collected hourly) and 144 values for NAT bandwidth (statistics are collected every 10 minutes). |
| Time    | The timestamp of the statistics collection.<br>The bandwidth is averaged in 10 minute intervals. Consequently, bandwidth value at a specific time represents the average bandwidth for the last 10 minute period.                                                                                      |
| Value   | The value for the number of NAT subscribers at a specific time, or the average bandwidth in kb/s for the last 10 minute period.                                                                                                                                                                        |
| Average | In the weekly display, the average daily value for the number of NAT subscribers or the NAT bandwidth.                                                                                                                                                                                                 |
| Peak    | In the weekly display, the daily peak value for the number of NAT subscribers or the NAT bandwidth.                                                                                                                                                                                                    |

## 7.24 VSR Scaling Profiles on BB-ISA

### 7.24.1 Scaling Profiles on the VSR

To meet flexible scaling requirements in common compute platforms, operators can use the CLI to select VSR-NAT scaling profiles that correspond to the amount of memory allocated in the VM.

The following scaling profiles have predefined upper scaling limits and are available for VSR-NAT and IPv6 FW:

- profile-1, with lower scale (default)
- profile-2, with higher scale

Scaling profiles are applied under the following CLI hierarchy:

**CLI Syntax:**

```
configure
 isa
 nat-group id [create]
 scaling-profile {profile-1 | profile-2}
```

### 7.24.2 Scale Profile Modification

A scaling profile can be changed only when the NAT group is in a **shutdown** state. After the scaling profile is changed and the NAT group is activated (**no shutdown**), the system tries to allocate necessary memory. If successful, the vISA transitions in-service; if unsuccessful (for example, if there is not enough memory in the system), the NAT group remains in the shutdown state.

Without sufficient resources to accommodate the required scaling profile, the vMDA where the vISA resides transitions into a failed state, followed by logs describing the failure:

```
33 2018/05/28 09:36:30.484 UTC MAJOR: CHASSIS #2001 Base
Mda 1/1
"Class MDA Module : failed, reason: Insufficient memory
to boot"

36 2018/09/18 14:13:02.426 UTC MAJOR: CHASSIS #2001 Base
Mda 1/1
"Class MDA Module : failed, reason: Insufficient mgmt
cores to boot"
```



---

## 7.25 Network Address Translation Command Reference

### 7.25.1 Command Hierarchies

- [ISA Configuration Commands](#)
- [NAT Service Configuration Commands](#)
  - [NAT Outside Commands](#)
  - [IPFIX Commands](#)
  - [UPnP Commands](#)
  - [ISA RADIUS Policy Commands](#)
  - [NAT Syslog Commands](#)
  - [VPRN Commands](#)
- [NAT Subscriber Management Commands](#)
  - [NAT Subscriber Management BRG Commands](#)
- [NAT Router Configuration Commands](#)
- [NAT DNAT Commands](#)
- [NAT MAP Domain Configuration Commands](#)
- [TCP MSS Adjustment Commands](#)
- [NAT MAP-T Configuration Commands](#)
- [Residential Firewall Subscriber Management Commands](#)
- [Residential Firewall Domain Commands](#)
- [Residential Firewall Commands](#)
- [Show Commands](#)
- [Clear Commands](#)
- [Tools Commands](#)
- [Filter Commands](#)

#### 7.25.1.1 ISA Configuration Commands

```
config
— isa
 — nat-group nat-group-id [create]
 — no nat-group nat-group-id
```

- **active-mda-limit** *number*
- **no active-mda-limit**
- **description** *description-string*
- **no description**
- **failed-mda-limit** *number*
- **no failed-mda-limit**
- **[no] mda** *mda-id*
- **radius-accounting-policy** *nat-accounting-policy*
- **no radius-accounting-policy**
- **redundancy** {**active-active** | **active-standby** | **l2aware-bypass**}
- **no redundancy**
- **scaling-profile** {**profile-1** | **profile-2**}
- **session-limits**
  - **reserved** *num-sessions*
  - **no reserved**
  - **watermarks** **high** *percentage* **low** *percentage*
  - **no watermarks**
- **[no] shutdown**
- **[no] suppress-lsn-events**
- **[no] suppress-lsn-sub-blks-free**

### 7.25.1.2 NAT Service Configuration Commands

- ```
configure
  — service
    — nat
      — deterministic-script
        — location remote-url
        — no location
      — nat-policy nat-policy-name [create]
      — no nat-policy nat-policy-name
      — alg
        — [no] ftp
        — [no] pptp
        — [no] rtsp
        — [no] sip
      — block-limit [1..40]
      — no block-limit
      — description description-string
      — no description
      — filtering filtering-mode
      — no filtering
      — ipfix-export-policy policy-name
      — no ipfix-export-policy
      — syslog-port-policy policy-name
      — pool nat-pool-name service-name service-name
      — pool nat-pool-name router router-instance
      — no pool
      — port-limits
        — forwarding limit
        — no forwarding
```

- **reserved** *num-ports*
- **no reserved**
- **watermarks** *high percentage-high low percentage-low*
- **no watermarks**
- [no] **priority-sessions**
 - [no] **fc** *fc-name*
- [no] **reset-unknown-tcp**
- **session-limits**
 - **max** *num-sessions*
 - **no max**
 - **reserved** *num-sessions*
 - **no reserved**
 - **watermarks** *high percentage-high low percentage-low*
 - **no watermarks**
- **tcp-mss-adjust** *segment-size*
- **no tcp-mss-adjust**
- [no] **timeouts**
 - **icmp-query** [*min minutes*] [*sec seconds*]
 - **no icmp-query**
 - **sip** [*hrs hours*] [*min minutes*] [*sec seconds*]
 - **no sip**
 - **subscriber-retention** [*hrs hours*] [*min minutes*]
 - **no subscriber-retention**
 - **tcp-established** [*hrs hours*] [*min minutes*] [*sec seconds*]
 - **no tcp-established**
 - **tcp-rst** [*min minutes*] [*sec sec*]
 - **no tcp-rst**
 - **tcp-syn** [*hrs hours*] [*min minutes*] [*sec seconds*]
 - **no tcp-syn**
 - **tcp-time-wait** [*min minutes*] [*sec seconds*]
 - **no tcp-time-wait**
 - **tcp-transitory** [*hrs hours*] [*min minutes*] [*sec seconds*]
 - **no tcp-transitory**
 - **udp** [*hrs hours*] [*min minutes*] [*sec seconds*]
 - **no udp**
 - **udp-dns** [*hrs hours*] [*min minutes*] [*sec seconds*]
 - **no udp-dns**
 - **udp-initial** [*min minutes*] [*sec seconds*]
 - **no udp-initial**
- [no] **udp-inbound-refresh**
- **pcp-server-policy** *name* [*create*]
- **no pcp-server-policy** *name*
 - **description** *description-string*
 - **no description**
 - **lifetime** *minimum* [60..86399] *maximum* [61..86400]
 - **no lifetime**
 - **max-description-size** *size*
 - **no max-description-size**
 - [no] **opcode**
 - [no] **announce**
 - [no] **get**
 - [no] **map**
 - [no] **option**
 - [no] **description**

- [no] **next**
- [no] **port-reservation**
- [no] **prefer-failure**
- [no] **third-party**
- **version** *minimum* *minimum* *maximum* *maximum*
- **no version**
- **port-forwarding**
 - **l2-aware** **subscriber** *sub-ident-string* **ip** *ip-address* **protocol** {**tcp** | **udp**} [**port** *port*] [**outside-ip** *ip-address*] [**outside-port** *port*] [**nat-policy** *policy-name*] [**member** *member-id*] [**port-range-start** *port*]
 - **no l2-aware** **subscriber** *sub-ident-string* **ip** *ip-address* **protocol** {**tcp** | **udp**} **port** *port*
 - **lsn** **router** *router-instance* [**b4** *ipv6-address*] [**aftr** *ipv6-address*] **ip** *ip-address* **protocol** {**tcp** | **udp**} [**port** *port*] [**outside-ip** *ipv4-address*] [**outside-port** *port*] [**nat-policy** *nat-policy-name*]
 - **no lsn** **router** *router-instance* [**b4** *ipv6-address*] **ip** *ip-address* **protocol** {**tcp** | **udp**} **port** *port* [**nat-policy** *nat-policy-name*]

7.25.1.2.1 NAT Outside Commands

- ```

configure
 — service
 — epipe
 — nat-outside nat-group-id [create]
 — no nat-outside nat-group-id
 — [no] shutdown

```

#### 7.25.1.2.2 IPFIX Commands

- ```

configure
  — service
    — ipfix
      — ipfix-export-policy policy-name [create]
      — no ipfix-export-policy policy-name
      — collector router router-instance ip ip-address [create]
      — no collector router router-instance ip ip-address
        — mtu mtu
        — no mtu
        — [no] shutdown
        — source-address ip-address
        — no source-address
        — template-refresh-timeout [hrs hours] [min minutes] [sec seconds] [days days] [
          — no template-refresh-timeout
      — description description-string
      — no description
      — template-format {format1 | format2}
      — no template-format

```

7.25.1.2.3 UPnP Commands

```
configure
  — service
    — upnp
      — upnp-policy policy-name [create]
      — no upnp-policy policy-name
        — description description-string
        — no description
        — http-listening-port http-listening-port
        — no http-listening-port
        — mapping-limit limit
        — no mapping-limit
        — [no] strict-mode

configure
  — subscriber-mgmt
    — sub-profile subscriber-profile-name [create]
    — no sub-profile subscriber-profile-name
      — upnp-policy policy-name
      — no upnp-policy
```

7.25.1.2.4 ISA RADIUS Policy Commands

```
configure
  — aaa
    — isa-radius-policy name [create]
    — no isa-radius-policy name
      — [no] acct-include-attributes
        — [no] acct-delay-time
        — [no] acct-trigger-reason
        — [no] called-station-id
        — [no] calling-station-id
        — [no] circuit-id
        — [no] dhcp-options
        — [no] dhcp-vendor-class-id
        — [no] dhcp6-options
        — [no] frame-counters
        — [no] framed-ip-addr
        — [no] framed-ip-netmask
        — [no] framed-ipv6-prefix
        — [no] hardware-timestamp
        — [no] inside-service-id
        — [no] ipv6-address
        — [no] mac-address
        — [no] multi-session-id
        — [no] nas-identifier
        — [no] nas-port-id
        — [no] nas-port-type
        — [no] nat-subscriber-string
        — [no] octet-counters
```

```

— [no] outside-ip
— [no] outside-service-id
— [no] port-range-block
— [no] release-reason
— [no] remote-id
— [no] session-time
— [no] subscriber-data
— [no] subscriber-id
— [no] ue-creation-type
— [no] user-name
— [no] wifi-rssi
— [no] wifi-ssid-vlan
— acct-update-triggers
— [no] address-state
— [no] auth-include-attributes
  — [no] called-station-id
  — [no] calling-station-id
  — [no] circuit-id
  — [no] dhcp-options
  — [no] dhcp-vendor-class-id
  — [no] dhcp6-options
  — [no] framed-ip-addr
  — [no] ipv6-address
  — [no] mac-address
  — [no] nas-identifier
  — [no] nas-port-id
  — [no] nas-port-type
  — [no] remote-id
  — [no] wifi-ssid-vlan
— description description-string
— no description
— nas-ip-address-origin {isa-ip | system-ip}
— no nas-ip-address-origin
— password password [hash | hash2]
— no password
— periodic-update interval hours [rate-limit rate]
— periodic-update
— servers
  — access-algorithm {direct | round-robin | hash-based}
  — no access-algorithm
  — retry count
  — no retry
  — router router-instance
  — router service-name service-name
  — no router
  — server server-index [create]
  — no server server-index
    — accounting [port udp-port]
    — no accounting
    — authentication [port udp-port]
    — no authentication
    — coa [port udp-port]
    — no coa
    — ip-address ip-address

```

- **no ip-address**
- **secret** *secret-key* | **hash-key** [*hash* | *hash2*]
- **no secret**
- **[no] shutdown**
- **source-address-range** *start-ip-address*
- **no source-address-range**
- **timeout** [*sec seconds*] [*min minutes*]
- **no timeout**
- **user-name-format** *user-name-format* [**mac-format** *mac-format*]
- **no user-name-format**

7.25.1.2.5 NAT Syslog Commands

- ```

config
 — service
 — nat
 — syslog
 — syslog-export-policy name [create]
 — no syslog-export-policy name
 — collector router router-name ip ip-address [create]
 — collector service-name service-name ip ip-address [create]
 — no collector router router-name ip ip-address
 — no collector service-name service-name ip ip-address
 — destination-port [destination-port]
 — ipv4-source-address ip-address
 — no ipv4-source-address
 — [no] shutdown
 — description description-string
 — no description
 — facility syslog-facility
 — [no] include
 — [no] destination-ip
 — [no] foreign-ip
 — [no] foreign-port
 — [no] nat-policy-name
 — [no] sub-id
 — log-prefix prefix-text
 — max-tx-delay deciseconds
 — no max-tx-delay
 — mtu mtu-size
 — rate-limit packets-per-second
 — no rate-limit
 — severity-level syslog-level

```

### 7.25.1.2.6 VPRN Commands

- ```

config
  — service
    — vprn service-id customer cust-id create

```

- [no] **nat**
 - **inside**
 - **classic-lsn-max-subscriber-limit** *max*
 - **no classic-lsn-max-subscriber-limit**
 - **destination-prefix** *ip-prefix/length* [**nat-policy** *nat-policy-name*]
 - **no destination-prefix** *ip-prefix/length*
 - **deterministic**
 - **prefix** *ip-prefix/length* **subscriber-type** *nat-sub-type* **nat-policy** *nat-policy-name* [**create**]
 - **prefix** *ip-prefix/length* **subscriber-type** *nat-sub-type*
 - **no prefix** *ip-prefix/length* **subscriber-type** *nat-sub-type*
 - **map start** *lsn-sub-address* **end** *lsn-sub-address* **to** *outside-ip-address*
 - **no map start** *lsn-sub-address* **end** *lsn-sub-address*
 - [no] **shutdown**
 - **downstream-ip-filter** *filter-id*
 - **no downstream-ip-filter**
 - **dslite-max-subscriber-limit** *max*
 - **no dslite-max-subscriber-limit**
 - **dual-stack-lite**
 - [no] **address** *ipv6-address*
 - **ip-fragmentation** {**disabled** | **fragment-ipv6** | **fragment-ipv6-unless-ipv4-df-set**}
 - **no ip-fragmentation**
 - [no] **reassembly**
 - **tunnel-mtu** *mtu-bytes*
 - **no tunnel-mtu**
 - [no] **shutdown**
 - **subscriber-prefix-length** *prefix-length*
 - **no subscriber-prefix-length**
 - **l2-aware**
 - [no] **address** *ip-address/mask*
 - **nat-policy** *nat-policy-name*
 - **no nat-policy**
 - [no] **nat64**
 - [no] **drop-zero-ipv4-checksum**
 - [no] **ignore-tos**
 - [no] **insert-ipv6-fragment-header**
 - **ip-fragmentation** {**disabled** | **fragment-ipv6** | **fragment-ipv6-unless-ipv4-df-set**}
 - **no ip-fragmentation**
 - **ipv6-mtu** *ipv6-mtu*
 - **no ipv6-mtu**
 - **prefix** *ipv6-prefix/prefix-length*
 - **no prefix**
 - **set-tos** [0..255]
 - **no set-tos**
 - [no] **shutdown**
 - **subscriber-prefix-length** *prefix-length*
 - **no subscriber-prefix-length**
 - **redundancy**
 - **peer** *ip-address*
 - **no peer**

- **peer6** *ip-address*
- **no peer6**
- **steering-route** *ip-prefix/length*
- **no steering-route**
- **outside**
 - **downstream-ip-filter** *filter-id*
 - **no downstream-ip-filter**
 - **downstream-ipv6-filter** *filter-id*
 - **no downstream-ipv6-filter**
 - **mtu** *value*
 - **no mtu**
 - **pool** *nat-pool-name nat-group nat-group-id type pool-type*
[**applications** *applications*] [**create**]
 - **no pool** *nat-pool-name*
 - **address-range** *start-ip-address end-ip-address* [**create**]
 - **no address-range** *start-ip-address end-ip-address*
 - **description** *description-string*
 - **no description**
 - **[no] drain**
 - **description** *description-string*
 - **no description**
 - **deterministic**
 - **port-reservation** *num-ports*
 - **no port-reservation**
 - **[no] external-assignment**
 - **mode** {*auto | napt | one-to-one*}
 - **no mode**
 - **[no] port-forwarding-dyn-block-reservation**
 - **port-forwarding-range** *range-end*
 - **no port-forwarding-range**
 - **port-reservation blocks** *num-blocks*
 - **port-reservation ports** *num-ports*
 - **no port-reservation**
 - **redundancy**
 - **export** *ip-prefix/length*
 - **no export**
 - **follow** *router router-instance pool name*
 - **no follow**
 - **monitor** *ip-prefix/length*
 - **no monitor**
 - **[no] shutdown**
 - **subscriber-limit** *limit*
 - **no subscriber-limit**
 - **watermarks** *high percentage-high low percentage-low*
 - **no watermarks**
 - **upstream-ip-filter** *filter-id*
 - **no upstream-ip-filter**
 - **upstream-ipv6-filter** *filter-id*
 - **no upstream-ipv6-filter**
- **mss-adjust-group** *nat-group-id segment-size segment-size*
- **no mss-adjust-group**
- **mtrace2**
 - **[no] shutdown**
 - **udp-port** *udp-port-number*

7.25.1.3 NAT Subscriber Management Commands

```

configure
  — subscriber-mgmt
    — sub-profile subscriber-profile-name [create]
    — no sub-profile subscriber-profile-name
      — nat-policy policy-name
      — no nat-policy
      — nat-prefix-list name
      — no nat-prefix-list

```

7.25.1.3.1 NAT Subscriber Management BRG Commands

```

configure
  — subscriber-mgmt
    — vrgw
      — brg
        — brg-profile profile-name [create]
        — no brg-profile profile-name
          — connectivity-verification [count nr-of-attempts] [timeout
            timeout-seconds] [retry-time retry-seconds]
          — no connectivity-verification
          — description description-string
          — no description
          — dhcp-pool
            — lease-time [days days] [hrs hrs] [min min] [sec sec]
            — lease-time seconds
            — no lease-time
            — options
              — custom-option option-number address [ip-
                address...(upto 4 max)]
              — custom-option option-number hex hex-string
              — custom-option option-number string ascii-string
              — no custom-option option-number
            — subnet ip-prefix/prefix-length start ip-address end ip-
              address
          — hold-time [days days] [hrs hrs] [min min] [sec sec]
          — hold-time seconds
          — no hold-time
          — initial-hold-time seconds
          — no initial-hold-time
          — [no] radius-proxy-server router router-instance name server-
            name
          — radius-server-policy policy-name
          — no radius-server-policy
          — sla-profile-string string
          — no sla-profile-string
          — sub-profile-string string
          — no sub-profile-string

```

7.25.1.4 NAT Router Configuration Commands

```

config
  — router
    — [no] nat
      — inside
        — classic-lsn-max-subscriber-limit max
        — no classic-lsn-max-subscriber-limit
        — destination-prefix ip-prefix/length [nat-policy nat-policy-name]
        — no destination-prefix ip-prefix/length
        — deterministic
          — prefix prefix/ip-prefix-length subscriber-type nat-sub-type nat-policy nat-policy-name [create]
          — prefix ip-prefix/ip-prefix-length subscriber-type nat-sub-type
          — no prefix ip-prefix/ip-prefix-length subscriber-type nat-sub-type
            — map start lsn-sub-address end lsn-sub-address to outside-ip-address
            — no map start lsn-sub-address end lsn-sub-address
            — [no] shutdown
        — dslite-max-subscriber-limit max
        — no dslite-max-subscriber-limit
        — dual-stack-lite
          — [no] address ipv6-address
            — ip-fragmentation {disabled | fragment-ipv6 | fragment-ipv6-unless-ipv4-df-set}
            — no ip-fragmentation
            — tunnel-mtu mtu-bytes
            — no tunnel-mtu
          — [no] shutdown
          — subscriber-prefix-length prefix-length
          — no subscriber-prefix-length
        — l2-aware
          — [no] address ip-address/mask
        — nat-policy nat-policy-name
        — no nat-policy
        — [no] nat64
          — [no] drop-zero-ipv4-checksum
          — [no] ignore-tos
          — [no] insert-ipv6-fragment-header
          — ip-fragmentation {disabled | fragment-ipv6 | fragment-ipv6-unless-ipv4-df-set}
          — no ip-fragmentation
          — ipv6-mtu ipv6-mtu
          — no ipv6-mtu
          — prefix ipv6-prefix/prefix-length
          — no prefix
          — set-tos [0..255]
          — no set-tos
          — [no] shutdown
          — subscriber-prefix-length prefix-length
          — no subscriber-prefix-length
        — redundancy

```

-
- **peer** *ip-address*
 - **no peer**
 - **peer6** *ip-address*
 - **no peer6**
 - **steering-route** *ip-prefix/length*
 - **no steering-route**
 - **subscriber-identification**
 - **attribute** [*vendor vendor-id*] **attribute-type** *attribute-type*
 - **no attribute**
 - **description** *description-string*
 - **no description**
 - **[no] drop-unidentified-traffic**
 - **radius-proxy-server** **router** *router-instance* **name** *server-name*
 - **no radius-proxy-server**
 - **[no] shutdown**
 - **outside**
 - **downstream-ip-filter** *filter-id*
 - **no downstream-ip-filter**
 - **downstream-ipv6-filter** *filter-id*
 - **no downstream-ipv6-filter**
 - **mtu** *mtu-size*
 - **no mtu**
 - **pool** *nat-pool-name* **nat-group** *nat-group-id* **type** *pool-type*
[**applications** *applications*] [**create**]
 - **no pool** *nat-pool-name*
 - **address-range** *start-ip-address end-ip-address* [**create**]
 - **no address-range** *start-ip-address end-ip-address*
 - **description** *description-string*
 - **no description**
 - **[no] drain**
 - **description** *description-string*
 - **[no] external-assignment**
 - **no description**
 - **mode** {*auto | napt | one-to-one*}
 - **no mode**
 - **[no] port-forwarding-dyn-block-reservation**
 - **port-forwarding-range** *range-end*
 - **no port-forwarding-range**
 - **port-reservation** **blocks** *num-blocks*
 - **port-reservation** **ports** *num-ports*
 - **no port-reservation**
 - **redundancy**
 - **export** *ip-prefix/length*
 - **no export**
 - **follow** **router** *router-instance* **pool** *name*
 - **no follow**
 - **monitor** *ip-prefix/length*
 - **no monitor**
 - **[no] shutdown**
 - **subscriber-limit** *limit*
 - **no subscriber-limit**
 - **watermarks** **high** *percentage-high* **low** *percentage-low*
 - **no watermarks**
 - **upstream-ipv6-filter** *filter-id*

- **no upstream-ipv6-filter**

7.25.1.5 NAT DNAT Commands

```

configure
  — service
    — nat
      — nat-classifier classifier-name [create]
      — no nat-classifier classifier-name
        — default-action {dnat | forward} [ip-address ip-address]
        — default-dnat-ip-address ip-address
        — no default-dnat-ip-address
        — description description-string
        — no description
        — entry entry-id [create]
        — no entry entry-id
          — action {dnat | forward} [ip-address ip-address]
          — no action
          — description description-string
          — no description
          — match protocol ip-protocol
          — no match
            — dst-port-range start port-number end port-number
            — no dst-port-range
      — nat-policy nat-policy-name [create]
      — no nat-policy nat-policy-name
        — [no] dnat
          — dnat-only router router-instance nat-group nat-group-id
          — no dnat-only
          — nat-classifier classifier-name
          — no nat-classifier
      — nat-prefix-list name [create] [application application-choice]
      — no nat-prefix-list name
        — prefix ip-prefix/length [nat-policy nat-policy-name]
        — no prefix ip-prefix/length

```

```

configure
  — router
    — nat
      — inside
        — classic-lsn-max-subscriber-limit max
        — no classic-lsn-max-subscriber-limit
        — dnat-only
          — source-prefix-list prefix-list-name
          — no source-prefix-list

```

7.25.1.6 NAT Admin Configuration Commands

```
admin
  — nat
    — save-deterministic-script
```

7.25.1.7 NAT MAP Domain Configuration Commands

```
config
  — service
    — nat
      — entry domain-name create
      — no action
```

7.25.1.8 TCP MSS Adjustment Commands

```
config
  — filter
    — ip-filter
      — entry
        — action
          — tcp-mss-adjust
    — filter
      — ipv6-filter
        — entry
          — action
            — tcp-mss-adjust

config
  — service
    — vprn
      — mss-adjust-group nat-group-id segment-size segment-size
      — [no] mss-adjust-group

config
  — service
    — nat
      — nat-policy
        — tcp-mss-adjust segment-size
        — no tcp-mss-adjust
```

7.25.1.9 NAT MAP-T Configuration Commands



Note: The MAP-T CLI commands listed in this section apply to the Nokia Virtualized Service Router (VSR) only.

```

config
  — service
    — nat
      — map-domain domain-name [create]
      — no map-domain domain-name
        — dmr-prefix dmr-prefix
        — no dmr-prefix
        — [no] ip-fragmentation
          — [no] v6-frag-header
        — mapping-rule map-rule-name
        — no mapping-rule map-rule-name
          — description description-string
          — no description
          — ea-length ea-bits-length
          — no ea-length
          — ipv4-prefix ipv4-prefix
          — no ipv4-prefix
          — psid-offset psid-offset-length
          — no psid-offset
          — rule-prefix rule-prefix
          — no rule-prefix
          — [no] shutdown
        — mtu mtu-size
        — no mtu
        — [no] shutdown
        — tcp-mss-adjust segment-size
        — no tcp-mss-adjust

```

7.25.1.10 Residential Firewall Subscriber Management Commands

```

config
  — subscriber-mgmt
    — sub-profile subscriber-profile-name
      — firewall-policy policy-name
      — no firewall-policy

```

7.25.1.11 Residential Firewall Domain Commands

```

config

```

```

— router
  — firewall
    — domain domain-name [nat-group nat-group-id] [create]
    — no domain domain-name
      — prefix prefix/prefix-length [create]
      — no prefix prefix/prefix-length
        — description description-string
        — no description
      — [no] shutdown

config
  — service
    — vprn service-id
      — firewall
        — domain domain-name [nat-group nat-group-id] [create]
        — no domain domain-name
          — prefix prefix/prefix-length [create]
          — no prefix prefix/prefix-length
            — description description-string
            — no description
          — [no] shutdown

```

7.25.1.12 Residential Firewall Commands

```

config
  — service
    — nat
      — firewall-policy name [create]
      — no firewall-policy name
        — alg
          — [no] ftp
          — [no] rtsp
          — [no] sip
        — description description-string
        — no description
        — domain router router-name name domain-name
        — no domain
        — filtering filtering-mode
        — no filtering
        — port-limits
          — forwarding limit
          — no forwarding
        — [no] priority-sessions
          — [no] fc fc-name
        — session-limits
          — max num-sessions
          — no max
          — reserved num-sessions
          — no reserved
          — watermarks high percentage-high low percentage-low

```


- **no watermarks**
- **tcp-mss-adjust** *segment-size*
- **no tcp-mss-adjust**
- **[no] timeouts**
 - **icmp6-query** [*min minutes*] [**sec seconds**]
 - **no icmp6-query**
 - **sip** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no sip**
 - **tcp-established** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no tcp-established**
 - **tcp-rst** [*min minutes*] [**sec sec**]
 - **no tcp-rst**
 - **tcp-syn** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no tcp-syn**
 - **tcp-time-wait** [*min minutes*] [**sec seconds**]
 - **no tcp-time-wait**
 - **tcp-transitory** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no tcp-transitory**
 - **udp** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no udp**
 - **udp-dns** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no udp-dns**
 - **udp-initial** [*min minutes*] [**sec seconds**]
 - **no udp-initial**
 - **unknown-protocol** [*hrs hours*] [*min minutes*] [**sec seconds**]
 - **no unknown-protocol**
- **[no] udp-inbound-refresh**
- **unknown-protocols**
 - **[no] protocol** {*number* | **any**}

7.25.1.13 Tools Commands

- tools
 - dump
 - nat
 - perform
 - nat
 - **recover-l2aw-bypass** *mda*

7.25.1.14 Show Commands

- show
 - **aaa**
 - **nat-accounting-policy**
 - **nat-accounting-policy** *policy-name*
 - **nat-accounting-policy** *policy-name* **associations**
 - **nat-accounting-policy**
 - **isa**

```

— nat-group
— nat-group nat-group-id [associations]
— nat-group nat-group-id mda mda-id l2-aware-bypass
— nat-group nat-group-id statistics mda mda-id [non-zero-value-only]
— nat-group nat-group-id member [1..255]
— nat-group nat-group-id member[1..255] reassembly-statistics [non-zero-value-only]
— nat-group nat-group-id member [1..255] statistics [non-zero-value-only]
— nat-group [nat-group-id] members
— service
  — nat
    — firewall-hosts [subscriber sub-ident] [ip ipv6-address/prefix-length] [mac
      ieee-address] [firewall-policy policy-name] [router router-instance]
    — firewall-policy [policy-name [associations]]
    — l2-aware-hosts [outside-router router-instance] [outside-ip outside-ip-
      address] [inside-ip-prefix ip-prefix/mask] [vas-filter vas-filter-name]
    — l2-aware-subscribers subscriber sub-ident
    — l2-aware-subscribers [nat-policy nat-policy-name] [nat-group nat-group-id]
      [member [1..255]] [outside-router router-instance] [outside-ip outside-ip-
      address] [firewall-policy policy-name]
    — map
      — frag-stats
      — map-domain
      — map-domain domain-name
      — map-domain domain-name mapping-rule rule-name
      — map-domain domain-name statistics
    — nat-policy
    — nat-policy nat-policy-name
    — nat-policy nat-policy-name associations
    — nat-policy nat-policy-name statistics
    — pcp-server-policy
    — pcp-server-policy name
    — port-forwarding-entries
      — classic-lsn-sub [router router-instance] [ip ip-address]
      — dslite-lsn-sub [router router-instance] [b4 b4-address]
      — l2-aware-sub [subscriber sub-ident-string]
      — nat64-lsn-sub [router router-instance] [ip ipv6-address]
    — nat
      — syslog
        — syslog-export-policy name associations
        — syslog-export-policy name
        — syslog-export-policy
    — upnp
      — upnp-policy policy-name
      — upnp-policy policy-name statistics
      — upnp-policy
  show
    — router
      — firewall
        — domain [domain-name]
        — summary
      — nat

```

- **l2-aware-blocks** **[outside-ip-prefix** *ip-prefix/length* **]** **[outside-port** *[1..65535]* **]** **[pool** *pool-name* **]**
- **lsn-blocks** **[inside-router** *router-instance* **]** **[inside-ip** *ip-address* **]** **[outside-ip-prefix** *ip-prefix/length* **]** **[outside-port** *[0..65535]* **]** **[pool** *pool-name* **]**
- **pool** *pool-name*
- **pool**
- **subscriber-identification**
- **summary**

7.25.1.15 Clear Commands

- ```
clear
 — nat
 — classic-lsn-sub router router-instance ip-prefix ip-prefix/length
 — classic-lsn-sub router router-instance ip-prefix ip-prefix/length subscriber-string
 — dslite-lsn-sub router router-instance b4-address-prefix ipv6-prefix
 — isa
 — nat-group nat-group-id member [1..255] l2-aware-subscribers
 — nat-group nat-group-id statistics mda mda-id
 — nat-group nat-group-id member [1..255] resource-peak-values
 — nat-group nat-group-id member [1..255] statistics
 — l2-aware-sub sub-ident-string
 — map
 — statistics
 — frag-stats
 — map-domain domain-name
 — upnp-mappings subscriber sub-ident-string protocol {tcp | udp} outside-port port-number
 — upnp-mappings subscriber sub-ident-string
 — upnp-policy-statistics policy-name
 — subscriber-mgmt
 — brg
 — gateway brg-id brg-ident
 — gateway brg-id brg-ident idle-bindings [binding ieee-address]
 — gateway all-gateways
 — gateway brg-id brg-ident all-hosts
 — gateway brg-id brg-ident host ieee-address
```

### 7.25.1.16 Tools Commands

- ```
tools
  — dump
    — deterministic-mapping outside-ip ipv4-address router router-instance outside-port [0..65535]
    — nat
      — histogram router router-instance pool pool-name bucket-size [1..65536] num-buckets [2..50]
    — isa
```

- **performance** *mda mda-id last time-span time-unit*
- **resources** *mda mda-id*
- **resources** *nat-group nat-group-id member [1..255]*
- **resources** *redundancy-utilization*
- **sessions** *[nat-group nat-group-id] [mda mda-id] [protocol {gre | icmp | icmp6 | tcp | udp | unknown}] [inside-ip ip-prefix[/ip-prefix-length]] [inside-router router-instance] [inside-port port-number] [outside-ip ipv4-address] [outside-port port-number] [foreign-ip ip-address] [foreign-port port-number] [dslite-address ipv6-address] [wlan-gw-ue ieee-address] [next-index index] [upnp] [member member-id] [nat-policy policy-name] [dest-ip ip-address] [firewall-policy policy-name] [address-type addr-type] [l2-aware-subscriber sub-ident]*
- **perform**
 - **nat**
 - **port-forwarding-action**
 - **l2-aware** *create subscriber sub-ident-string ip ip-address protocol {tcp | udp} [port port] lifetime lifetime [outside-ip ip-address] [outside-port port] [nat-policy policy-name]*
 - **l2-aware** *delete subscriber sub-ident-string ip ip-address protocol {tcp | udp} port port [nat-policy policy-name]*
 - **l2-aware** *modify subscriber sub-ident-string ip ip-address protocol {tcp | udp} port port lifetime lifetime [nat-policy policy-name]*
 - **lsn** *create router router-instance [b4 ipv6-address] [aftr ipv6-address] [ip ip-address] protocol {tcp | udp} port port lifetime lifetime [outside-ip ipv4-address] [outside-port port] [nat-policy nat-policy-name]*
 - **lsn** *delete router router-instance [b4 ipv6-address] ip ip-address protocol {tcp | udp} port port [nat-policy nat-policy-name]*
 - **lsn** *modify router router-instance [b4 ipv6-address] ip ip-address protocol {tcp | udp} port port lifetime lifetime [nat-policy nat-policy-name]*
 - **recover-l2aw-bypass** *mda*

7.25.1.17 Filter Commands

- ```
configure
 — filter
 — ip-filter filter-id
 — entry entry-id
 — action [secondary] nat [nat-policy nat-policy-name]
 — no action [secondary]
 — ipv6-filter filter-id
 — entry entry-id
 — action [secondary] nat nat-type nat-type [nat-policy nat-policy-name]
 — no action [secondary]
```

## 7.25.2 Command Descriptions

- [Generic Commands](#)
- [ISA Configuration Commands](#)
- [NAT Configuration Commands](#)
- [NAT Service Configuration Commands](#)
- [IPFlow Information Export Protocol Commands](#)
- [AAA Policy Commands](#)
- [NAT Subscriber Management Commands](#)
- [NAT Subscriber Management BRG Commands](#)
- [NAT DNAT Commands](#)
- [NAT MAP-T Commands](#)
- [NAT Filter Commands](#)
- [Residential Firewall Commands](#)
- [NAT Show Commands](#)
- [MAP-T Show Commands](#)
- [NAT Clear Commands](#)
- [MAP-T Clear Commands](#)
- [NAT Tools Commands](#)

### 7.25.2.1 Generic Commands

description

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>description</b> <i>description-string</i><br><b>no description</b>                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Context</b> | config>aaa>isa-radius-plcy>servers>server<br>config>isa>nat-group><br>config>router>firewall>domain>prefix<br>config>router>nat>inside>subscriber-id<br>config>router>nat>outside>pool<br>config>router>nat>outside>pool>address-range<br>config>service>ipfix>ipfix-export-policy<br>config>service>nat>firewall-policy<br>config>service>nat>map-domain>mapping-rule<br>config>service>nat>nat-classifier<br>config>service>nat>nat-classifier>entry |

```

config>service>nat>nat-policy
config>service>nat>pcp-server-policy
config>service>upnp>upnp-policy
config>service>vprn>firewall>domain>prefix
config>service>vprn>nat>outside>pool>address-range
config>service>vprn>nat>outside>pool
config>subscr-mgmt>vrgw>brg>brg-profile

```

**Description** This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

**Parameters** *string* — The description character string. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

## shutdown

**Syntax** **[no] shutdown**

**Context**

```

config>aaa>isa-radius-plcy>servers>server
config>isa>nat-group
config>router>firewall>domain
config>router>nat>inside>deterministic>prefix
config>router>nat>inside>dual-stack-lite
config>router>nat>inside>nat64
config>router>nat>inside>redundancy>subscriber-identification
config>router>nat>inside>subscriber-id
config>router>nat>outside>pool
config>router>nat>outside>pool>address-range
config>router>nat>outside>pool>redundancy
config>service>ipfix>ipfix-export-policy>collector
config>service>vprn>mtrace2
config>service>vprn>nat>inside>nat64
config>service>vprn>nat>outside>pool
config>service>vprn>nat>outside>pool>address-range
config>service>vprn>nat>outside>pool>redundancy

```

**Description** This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

### 7.25.2.2 ISA Configuration Commands

#### nat-group

|             |                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------|
| Syntax      | <b>nat-group</b> <i>nat-group-id</i> [ <b>create</b> ]<br><b>no nat-group</b> <i>nat-group-id</i> |
| Context     | config>isa                                                                                        |
| Description | This command configures an ISA NAT group.                                                         |

#### active-mda-limit

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>active-mda-limit</b> <i>number</i><br><b>no active-mda-limit</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Context     | config>isa>nat-group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Description | <p>This command configures the number of active ISAs in active-standby ISA redundancy model for NAT. The active ISAs are automatically selected by the system and any the remaining ISA beyond the number of active limit will automatically assume the standby role. An ISA in the standby mode is idle until the failure of an active ISA occurs. Standby ISA can accept traffic from exactly one failed active ISA. Multiple standby ISAs can be configured in the system to protect against multiple simultaneous failures.</p> <p>Once the active ISA fails, the standby ISA will start forwarding traffic. NAT translations from the failed ISA will have to be re-initiated by the clients and consequently setup on the newly active ISA.</p> <p>In order for this command to take effect, the intra-chassis redundancy mode must be set to active-standby (<b>config&gt;isa&gt;nat-group&gt;redundancy active-standby</b>).</p> |
| Default     | no active-mda-limit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Parameters  | <i>number</i> — Specifies the active MDA limit.<br><b>Values</b> 1 to 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

#### failed-mda-limit

|             |                                                                                 |
|-------------|---------------------------------------------------------------------------------|
| Syntax      | <b>failed-mda-limit</b> <i>number</i><br><b>no failed-mda-limit</b>             |
| Context     | config>isa>nat-group                                                            |
| Description | This command configures the maximum number of supported simultaneously failures |

in active-active intra-chassis NAT redundancy model. Traffic from the failed ISAs is distributed over the remaining ISA in the system. Memory resources are reserved in every ISA to accommodate new mappings from the failed ISA. However, bandwidth is not reserved and each ISA operates at max speed in all conditions (with failure or without the failure).

NAT translations are not preserved across switchovers and consequently they will have to be re-initiated by the clients.

In order for this command to take effect, the intra-chassis redundancy mode must be set to active-active (**config>isa>nat-group>redundancy active-active**).

|            |                                                                                                                                  |
|------------|----------------------------------------------------------------------------------------------------------------------------------|
| Default    | no failed-mda-limit                                                                                                              |
| Parameters | <i>number</i> — Specifies the number of simultaneous ISA failures supported in active-active intra-chassis NAT redundancy model. |
| Values     | 1 to 2                                                                                                                           |

mda

|             |                                                                     |
|-------------|---------------------------------------------------------------------|
| Syntax      | [no] <b>mda</b> <i>mda-id</i>                                       |
| Context     | config>isa>nat-group                                                |
| Description | This command configures an ISA NAT group MDA.                       |
| Parameters  | <i>mda-id</i> — Specifies the MDA ID in the <i>slot/mda</i> format. |
| Values      | slot: 1 to 10<br>mda: 1 to 2                                        |

radius-accounting-policy

|             |                                                                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>radius-accounting-policy</b> <i>nat-accounting-policy</i><br><b>no radius-accounting-policy</b>                                                                                                |
| Context     | config>isa>nat-group                                                                                                                                                                              |
| Description | This command specifies the RADIUS accounting policy to use for each MDA in this ISA group.<br><br>The <b>no</b> form of the command removes the policy ID from the configuration.                 |
| Default     | no radius-accounting-policy                                                                                                                                                                       |
| Parameters  | <i>nat-accounting-policy</i> — Reference to the nat-accounting-policy which defines:<br>Source IP addresses that will be assigned to BB-ISA cards.<br>Parameters related to RADIUS server itself. |



List of RADIUS attributes that will be included in accounting messages.

## redundancy

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>redundancy {active-active   active-standby   l2aware-bypass}</b><br><b>no redundancy</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>isa>nat-group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | This command configures intra-chassis redundancy mode for NAT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Default</b>     | redundancy active-standby                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <p><b>active-active</b> — Specifies the mode in which all MS-ISAs in a NAT group are active. If one or two MS-ISAs in the system fail, the remaining active MS-ISA accepts the load from the failed MS-ISAs.</p> <p><b>active-standby</b> — Specifies the mode in which one or more MS-ISAs in the NAT group are in standby mode. While in standby -mode, MS-ISAs do not process traffic. Only when the active MS-ISA fails, traffic is diverted to the standby MS-ISA which at this point becomes active.</p> <p><b>l2-aware-bypass</b> — Specifies that when an ISA MDA fails, NAT re-routes its traffic based on the regular destination address lookup. This resiliency mode is applicable only to L2-Aware NAT. Once MS-ISA fails, its traffic is routed via regular routing (destination based lookup). The assumption is that traffic will be sent to an external NAT device that serves as a backup NAT device.</p> |

## scaling-profile

|                    |                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>scaling-profile {profile-1   profile-2}</b>                                                                                             |
| <b>Context</b>     | config>isa>nat-group                                                                                                                       |
| <b>Description</b> | This command enables configured scaling profiles for a NAT group in VSR.                                                                   |
| <b>Default</b>     | profile-1                                                                                                                                  |
| <b>Parameters</b>  | <p><b>profile-1</b> — Activates scaling profile 1 (lower scale).</p> <p><b>profile-2</b> — Activates scaling profile 2 (higher scale).</p> |

## session-limits

|                |                                                       |
|----------------|-------------------------------------------------------|
| <b>Syntax</b>  | <b>session-limits</b>                                 |
| <b>Context</b> | config>isa>nat-group<br>config>service>nat>nat-policy |

---

config>service>nat>firewall-policy

**Description** This command enters the context to configure the ISA NAT group or residential firewall session limits.

## reserved

**Syntax** **reserved** *num-sessions*  
**no reserved**

**Context** config>isa>nat-group>session-limits

**Description** This command configures the number of sessions per block that will be reserved for prioritized sessions.

**Default** no reserved

**Parameters** *num-sessions* — Specifies the number of sessions reserved for prioritized sessions.  
**Values** 0 to 6291456

## reserved

**Syntax** **reserved** *num-sessions*  
**no reserved**

**Context** config>service>nat>firewall-policy>session-limits  
config>service>nat>nat-policy>session-limits

**Description** This command configures the number of sessions per block that will be reserved for prioritized sessions.

**Default** no reserved

**Parameters** *num-sessions* — Specifies the number of sessions reserved for prioritized sessions.  
**Values** 0 to 65534

## watermarks

**Syntax** **watermarks** *high percentage low percentage*  
**no watermarks**

**Context** config>isa>nat-group>session-limits  
config>service>nat

**Description** This command configures the ISA NAT group watermarks.

---

|                   |                                                                                                                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | no watermarks                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b> | <b>high <i>percentage</i></b> — Specifies the high watermark of the number of sessions for each MDA in this NAT ISA group.<br><b>Values</b> 1 to 100<br><b>low <i>percentage</i></b> — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA group.<br><b>Values</b> 0 to 99 |

## suppress-lsn-events

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] suppress-lsn-events</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | configure>isa>nat-group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command suppresses the generation of Large Scale NAT (LSN) events when RADIUS accounting is enabled.</p> <p>By default, only one logging facility for tracking subscribers in LSN44, DS-lite, and NAT64 can be enabled at the time: either the SR OS event logging facility or the RADIUS logging facility. SR OS event logs can be sent to multiple destinations, such as the console session, a telnet or SSH session, memory logs, file destinations, SNMP trap groups, and syslog destinations.</p> <p>If RADIUS logging is enabled, the NAT logs are sent to the RADIUS destination and the NAT logs are suppressed in the SR OS event logging facility, for example, NAT logs are not sent to the syslog server.</p> <p>If RADIUS logging is disabled, the NAT logs are sent to the SR OS event logging facility; for example, syslog, assuming that the events are enabled via the event-control command (<b>config&gt; log&gt;event-control nat event generate</b>).</p> <p>By explicitly disabling this command (<b>no suppress-lsn-events</b>), the NAT logs can be sent to both logging facilities simultaneously, the SR OS event logging facility, and the RADIUS logging facility.</p> |
| <b>Default</b>     | suppress-lsn-events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## suppress-lsn-sub-blks-free

|                |                                        |
|----------------|----------------------------------------|
| <b>Syntax</b>  | <b>[no] suppress-lsn-sub-blks-free</b> |
| <b>Context</b> | configure>isa>nat-group                |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <p>This command suppresses the <code>tmnxNatLsnSubBlksFree</code> summary notification and use the <code>tmnxNatPIBlockAllocationLsn</code> notifications. When the SR OS node is in a state of excessive logging, the queue associated with the transmission of logs on the MS-ISA can become congested. This event further delays the generation of logs, and with this, further allocations and deallocations of NAT resources (port-blocks) will be stalled until the queue is relieved of congestion. For example, an excessive logging state in the system can be caused by issuing a command to clear a large number of NAT subscribers where a large number of resources (port-blocks) are released at once.</p> <p>The <b>suppress-lsn-sub-blks-free</b> command enables the generation of individual logs carried in event-id 2012 for every released port block regardless of the state of the transmission queue (whether congested or not). If NAT subscribers have a large number of allocated port blocks (this could be hundreds of port blocks per subscriber), generating individual logs per port-block release contributes to the congestion.</p> <p>To alleviate transmission queue congestion, this behavior can be changed by disabling this command (<b>no suppress-lsn-sub-blks-free</b>). This causes the suppression of logs related to the release of individual port blocks of a NAT subscriber when the transmission queue is congested. As a result, only a summarized release log via event-id 2021 for the subscriber is generated. The purpose of this new log is to inform the operator in a single message that all ports blocks for the subscriber are released. For example, the log message for LSN will be “LSN subscriber all blocks freed”. The benefit of such summarization (or log aggregation) is to alleviate the congestion of the transmission queue and consequently accelerate resource releases. An effect is the decreased granularity of information.</p> <p>If summarization is enabled (<b>no suppress-lsn-sub-blks-free</b>) while there is no logging congestion in the system, the port block releases continue to be logged individually via the event-id 2012 (assuming that this is enabled in the event control), except for the last port block of the subscriber. When the last port block is released, the log with event-id 2021 is generated indicating that all port blocks for the subscriber are now released without carrying the specific information about this last port block that is released.</p> |
| Default     | no suppress-lsn-sub-blks-free                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### 7.25.2.3 NAT Configuration Commands

nat

|             |                                                             |
|-------------|-------------------------------------------------------------|
| Syntax      | [no] nat                                                    |
| Context     | config>service>vprn<br>config>router                        |
| Description | This command configures, creates or deletes a NAT instance. |

## deterministic-script

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>deterministic-script</b>                                         |
| <b>Context</b>     | config>service>nat                                                  |
| <b>Description</b> | This command configures the script generated for deterministic NAT. |

## location

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>location</b> <i>remote-url</i><br><b>no location</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | config>service>nat>deterministic-script                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | This command configures the remote location where the Python script will be exported. The Python script is then used off-line to perform reverse query. If this command is configured, the Python script generation is triggered by any modification of the deterministic NAT configuration. The new script reflects the change in mappings caused by configuration change. However, the script must be manually exported to the outside location with the <b>admin nat save-deterministic-nat</b> command. The script cannot be stored locally on the system. |

The script allows two forms of queries:

- Forward – input is NAT inside parameters, output is NAT outside parameters.
- Backward – input is NAT outside parameters, output is NAT inside parameters.

Forward Query:

```
user@external-server:/home/ftp/pub/det-nat-script$./det-nat.py -f -s 10 -
a 10.0.5.10
```

output:

```
subscriber has public ip address 198.51.100.1 from service 0 and is using ports [132
4 - 1353]
```

Reverse Query:

```
user@external-server:/home/ftp/pub/det-nat-script$./det-nat.py -b -s 0 -
a 198.51.100.1 -p 3020
```

output:

```
subscriber has private ip address 10.0.5.66 from service 10
```

|                |             |
|----------------|-------------|
| <b>Default</b> | no location |
|----------------|-------------|

---

**Parameters**    *remote-url* — A remote location where the script is stored:  
                  [[ftp:// | tftp://]<login>:<pswd>@ <remote-locn>/] [<file-path>]  
                  Maximum length is 180 characters.

## inside

**Syntax**        **inside**

**Context**        config>service>vprn>nat  
                  config>router>nat

**Description**    This command enters the “inside” context to configure the inside NAT instance.

## outside

**Syntax**        **outside**

**Context**        config>service>vprn>nat  
                  config>router>nat

**Description**    This command enters the “outside” context to configure the outside NAT instance.

## downstream-ip-filter

**Syntax**        **downstream-ip-filter** *filter-id*  
                  **no downstream-ip-filter**

**Context**        config>service>vprn>nat>inside

**Description**    This command assigns an IPv4 filter policy to the downstream NAT interface. This filter is applied to downstream traffic after the NAT function is applied but before it enters the inside VPRN instance.

                  The **no** form of the command removes the filter from the configuration.

**Default**        no downstream-ip-filter

**Parameters**    *filter-id* — Specifies an existing IPv4 filter policy. Values can be expressed either as a decimal integer or as an ASCII string of up to 64 characters.

**Values**        1 to 65535, or ASCII string of up to 64 characters

## downstream-ip-filter

**Syntax**        **downstream-ip-filter** *filter-id*

|                    |                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <b>no downstream-ip-filter</b>                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>router>nat>outside<br>config>service>vprn>nat>outside                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | This command specifies a filter to apply to the downstream traffic after routing in the outside virtual router instance and before the NAT function; it is useful for traffic that bypasses the egress filters applied in the inside virtual router instance, such as DSLite traffic.<br><br>The <b>no</b> form of the command removes the filter from the configuration. |
| <b>Default</b>     | no downstream-ip-filter                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>filter-id</i> — Specifies a filter up to 64 characters.                                                                                                                                                                                                                                                                                                                |

## downstream-ipv6-filter

|                    |                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>downstream-ipv6-filter</b> <i>filter-id</i><br><b>no downstream-ipv6-filter</b>                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>router>nat>outside<br>config>service>vprn>nat>outside                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | This command configures the ipv6-filter for downstream traffic. This filter is applied to downstream traffic after it leaves the outside virtual router instance but before the NAT function is applied. This is useful for shared v6 filters that apply to all v6 DSM hosts.<br><br>The <b>no</b> form of the command removes the filter from the configuration. |
| <b>Default</b>     | no downstream-ipv6-filter                                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>filter-id</i> — specifies an IPv6 filter up to 64 characters in length                                                                                                                                                                                                                                                                                         |

## mtu

|                    |                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mtu</b> <i>value</i><br><b>no mtu</b>                                                                                                                                                                                                                      |
| <b>Context</b>     | config>service>vprn>nat>outside                                                                                                                                                                                                                               |
| <b>Description</b> | This command configures the Maximum Transmission Unit (MTU) for downstream traffic flowing through this router (as outside NAT router). The system fragments IP datagrams exceeding the MTU.<br><br>The <b>no</b> form of the command reverts to the default. |
| <b>Default</b>     | no mtu                                                                                                                                                                                                                                                        |

**Parameters**     *value* — Specifies the MTU for downstream traffic.

**Values**        512 to 9000

## destination-prefix

**Syntax**        **destination-prefix** *ip-prefix/length* [**nat-policy***policy-name*]  
**no destination-prefix** *ip-prefix/length*

**Context**        config>service>vprn>nat>inside  
config>router>nat>inside

**Description**    This command configures a destination prefix. An (internal) static route is created for this prefix. All traffic that hits this route will be subject to NAT. The system will not allow a destination-prefix to be configured if the configured **nat-policy** refers to an IP pool that resides in the same service (as this would result in a routing loop).

**Parameters**    *ip-prefix* — Specifies the IP prefix; host bits must be zero (0).

**Values**        a.b.c.d

*length* — Specifies the prefix length.

**Values**        0 to 32

*policy-name* — Specifies the **nat-policy** name associated with the destination prefix.

## deterministic

**Syntax**        **deterministic**

**Context**        config>service>vprn>nat>inside  
config>router>nat>inside

**Description**    This command enables the context to configure deterministic NAT.

## classic-lsn-max-subscriber-limit

**Syntax**        **classic-lsn-max-subscriber-limit** *max*  
**no classic-lsn-max-subscriber-limit**

**Context**        config>service>vprn>nat>inside>deterministic  
config>router>nat>inside>deterministic

**Description**    This command affects ingress hashing of the subscribers for deterministic NAT. It will also affect hashing of the subscribers for non-deterministic NAT if the both types of NAT are configured simultaneously. The hashing will ensure that traffic load is distributed over multiple MS-ISAs in the system. For deterministic LSN44, (32 – n) bits of the source IP address will be considered for hashing, where  $2^n = \text{classic-lsn-max-subscriber-limit}$ .



The scope of this command is the inside routing instance. This command must match the largest subscriber limit of all pools that are referenced by nat-policies configured within the corresponding inside routing instance.

This parameter must be configured before any prefix is configured and can be modified only if there are no prefixes configured under the deterministic NAT CLI hierarchy.

If non-deterministic NAT is not used simultaneously with deterministic NAT within a routing context, then hashing for non-deterministic NAT will be performed based on the subscriber.

|            |                                                                                                                                                                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default    | no classic-lsn-max-subscriber-limit                                                                                                                                                                                                                                     |
| Parameters | <i>max</i> — The power of 2 ( $2^n$ ) number that must match the largest subscriber limit number in a deterministic pool referenced from this inside routing instance. The range for this command is the same as the subscriber-limit command under the pool hierarchy. |

dslite-max-subscriber-limit

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>dslite-max-subscriber-limit</b> <i>max</i><br><b>no dslite-max-subscriber-limit</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Context     | config>service>vprn>nat>inside<br>config>router>nat>inside>dslite<br>config>router>nat>inside>deterministic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Description | <p>This command sets the value for the number of high order bits of the source IPv6 address that will be considered as DS-Lite subscriber. The remaining bits of the source IPv6 address will be masked off, effectively aggregation all IPv6 source addresses under the configured prefix length into a single DS-Lite subscriber. Source IPv4 addresses/ports of the traffic carried within the DS-Lite subscriber will be translated into a single outside IPv4 address and the corresponding deterministic port-block (port-blocks can be extended).</p> <p>The range of values for subscriber-prefix-length in non-deterministic DS-Lite is limited from 32 to 64 (a prefix will be considered as a DS-Lite subscriber) or it can be set to a value of 128 (the source IPv6 address is considered as a DS-Lite subscriber).</p> <p>In cases where deterministic DS-Lite is enabled in a giver inside routing context, the range of values of the subscriber-prefix-length depends on the value of dslite-max-subscriber-limit parameter as follows:</p> <p><b>subscriber-prefix-length – n = [32..64,128]</b></p> <p><b>where n = log2(dslite-max-subscriber-limit)</b></p> <p>[or in an alternate form: dslite-max-subscriber-limit = <math>2^n</math>.]</p> |

In other words the largest prefix length for the deterministic DS-lite subscriber will be  $32+n$ , where  $n = \log_2(\text{dslite-max-subscriber-limit})$ . The subscriber prefix length can extend up to 64 bits. Beyond 64 bits for the subscriber prefix length, there only one value is allowed: 128. In the case  $n$  must be 0, which means that the mapping between B4 elements (or IPv6 address) and the IPv4 outside addresses is in 1:1 ratio (no sharing of outside IPv4 addresses).

This parameter can be changed only when there are no deterministic prefixes configured in the same routing context.

**Default** 128

**Parameters** *max* — In non-deterministic DS-Lite this value can be 32 to 64, 128, assuming that the deterministic DS-Lite is not concurrently enabled in the same inside routing context. In case that deterministic DS-Lite is enabled, this value can be within the range  $[(32+n)..64, 128]$  where  $n = \log_2(\text{dslite-max-subscriber-limit})$ . The value of 128 is allowed only when  $n=0$  (each subscriber is mapped to a single outside IPv4 IP address).

## prefix

**Syntax** **prefix** *ip-prefix/length* **subscriber-type** *nat-sub-type* **nat-policy** *nat-policy-name* [**create**]  
**prefix** *p-prefix/length* **subscriber-type** *nat-sub-type*  
**no prefix** *ip-prefix/length* **subscriber-type** *nat-sub-type*

**Context** config>service>vprn>nat>inside>deterministic  
 config>router>nat>inside>deterministic

**Description** This command is applicable only to deterministic NAT (LSN44 or DS-Lite). It configures prefixes on the inside and their association with outside deterministic pools via the nat-policy. Subscribers within the prefix will be deterministically mapped to outside IP addresses and corresponding port-ranges in the associated pool.

Multiple prefixes within an inside routing instance can be defined and they can reference different nat-policies (and therefore outside pools and routing instances). Moreover, prefixes from multiple routing instances can share the same deterministic pool.

Non-deterministic NAT can be used simultaneously with deterministic NAT within the same inside routing instance. However, they cannot share the same pool.

Prefixes can be added/removed under the condition that the associated deterministic pool is in a **no shutdown** mode.

Removing a prefix or modifying the map statement under it requires that the prefix be in a 'shutdown' mode.

The subscribers under the prefix are mapped deterministically into the outside IPv4 addresses and port ranges. The subscribers in LSN44 are the IPv4 addresses under the configured prefix, while in DS-Lite the subscribers are IPv6 source addresses that fall under the configured prefix OR IPv6 sub-prefixes whose length is determined by the DS-Lite subscriber-prefix-length command.

**Parameters** *ip-prefix/length* — A prefix on the inside encompassing subscribers that will be deterministically mapped to an outside IP address and port block in the corresponding pool.

**Values**

|                      |                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------|
| <ip-prefix/ip-pref*> | <ipv4-prefix>/<ipv4-prefix-length><br><ipv6-prefix>/<ipv6-prefix-length>                                             |
| <ipv4-prefix>        | a.b.c.d (host bits must be 0)                                                                                        |
| <ipv4-prefix-length> | [0 to 32]                                                                                                            |
| <ipv6-prefix>        | x:x:x:x:x:x:x (eight 16-bit pieces)<br>x:x:x:x:x:d.d.d.d<br>x - [0 to FFFF]H<br>d - [0 to 255]D                      |
| <ipv6-prefix-length> | [0 to 128]                                                                                                           |
| <nat-sub-type>       | classic-lsn-sub, dslite-lsn-sub                                                                                      |
| <nat-policy-name>    | Reference to a nat-policy that points to an outside pool and outside routing instance up to 32 characters in length. |

**create** — Keyword used to create the particular prefix instance.

## map

**Syntax** **map start** *lsn-sub-address* **end** *lsn-sub-address* **to** *outside-ip-address*  
**no map start** *lsn-sub-address* **end** *lsn-sub-address*

**Context** config>service>vprn>nat>inside>deterministic>prefix  
config>router>nat>inside>deterministic>prefix

**Description** This command is applicable to prefixes in deterministic NAT (LSN44 and DS-Lite). Its purpose is to split the number of subscribers within the configured prefix over available sequence of outside IP addresses.

There are several rules guiding the usage of the map statement:

- If the number of subscribers per configured prefix is greater than the subscriber-limit per outside IP parameter ( $2^n$ ), then the lowest n bits of the map start *<inside-addr-start>* must be set to 0.

Subscriber in LSN44 is equals to an inside IPv4 address, while in DS-Lite, the subscriber can be an IPv6 address or IPv6 prefix. If the **subscriber-prefix-length** command is set to 128, then the subscriber in DS-Lite is an IPv6 address. Otherwise it will be an IPv6 prefix with length in the range [32 to 64] as set by the **subscriber-prefix-length** command.

- If the number of subscribers per configured prefix is equal or less than the subscriber-limit per outside IP parameter ( $2^n$ ), then only one map command for this prefix is allowed. In this case there is no restriction on the lower n bits of the map start *lsn-sub-address*. The range of the inside IP addresses in such map statement represents the prefix itself.
- *outside-ip-address* in the map statements must be unique amongst all map statements referencing the same pool. In other words, two map statements cannot reference the same *outside-ip-address* in a pool.

To modify map statements, the corresponding prefix must be in a shutdown mode.

Map statements can be configured automatically by the system, as soon as the prefix is enabled (no shutdown state) or they can be configured manually by the operator while the prefix is disabled.

The following is an example of the map statement for the LSN44 case:

- The subscriber-limit in the pool is 128
- The pool has an address range 192.168.0.1 - 192.168.0.10
- The prefix is 10.0.0.0/24
- The map statement is configured as:  
**map start 10.0.0.0 end 10.0.0.255 to 192.168.0.1**

Since each outside IP address can accommodate only 128 hosts, the subscribers (IPv4 addresses in LSN44) from the 10.0.0.0/24 prefix will be split and mapped into two outside IP addresses

**10.0.0.0 – 10.0.0.127 (10.0.0.0/25) - 192.168.0.1**

**10.0.0.128 – 10.0.0.255 (10.0.0.128/25) - 192.168.0.2**

The first IP address range will be mapped to the 'to' address in the map statement => 192.168.0.1. The second IP address range will be mapped into the next consecutive IP address in the pool assuming that this IP address is free. In this case this consecutive address (192.168.0.2) would not be shown in the map statement.

For Deterministic DS-Lite, the example would be:

- The subscriber-limit in the pool is 128
- The pool has an address range 192.168.0.1 - 192.168.0.10
- The prefix is 2001:db8::/56
- The subscriber-prefix-length = 64
- The map statement is configured as:

### **map start 2001:db8::/64 end 2001:db8::FF:0:0:0/64 to 192.168.0.1**

There are 256 DS-Lite subscribers within the 2001:db8::/56 prefix. Each subscriber will be a /64 IPv6 prefix as dictated by the subscriber-prefix-length command.

Since each outside IP address can accommodate only 128 hosts, the subscribers from the 2001:db8::/56 prefix will be split and mapped into two outside IP addresses

**2001:db8:: – 2001:db8:0:7F:: (2001:db8::/57) - 192.168.0.1**

**2001:db8:0:80:: – 2001:db8:0:FF::(2001:db8:0:FF::/57) - 192.168.0.2**

The first IP prefix range will be mapped to the 'to' address in the map statement => 192.168.0.1. The second IP prefix range will be mapped into the next consecutive IP address in the pool assuming that this IP address is free. In this case this consecutive address (192.168.0.2) would not be shown in the map statement.

**Default** By default, the system will automatically divide the prefix and create the map statements when the prefix command is enabled (no shutdown). However, this automatic map provisioning can be overruled by manual configuration.

**Parameters** *inside-ip-start* — Start IPv4/v6 address or IPv6 prefix on the inside.

*inside-ip-end* — End IPv4/v6 address or IPv6 prefix on the inside. The number of subscribers (range of inside IPv4 addresses in LSN44 or IPv6 addresses or prefixes in DS-Lite) in the map statement does not have to be a power of 2. Rather it has to be a multiple of a power of two  $m * 2^n$ , where  $m$  is the number of consecutive outside IP addresses to which the subscribers are mapped and the  $2^n$  is the subscriber-limit per outside IP.

*outside-ip-start* — The first outside IPv4 address in the pool to which the subscribers are mapped. In case that the number of subscribers in the map statement is larger than the subscriber-limit for the *outside-ip address*, the consecutive outside IP addresses will be used for additional mappings. Those additional (consecutive) outside IP addresses are not shown in the map statement (only the first address is shown in the map statement).

## dual-stack-lite

**Syntax** **dual-stack-lite**

**Context** config>service>vprn>nat>inside  
config>router>nat>inside

**Description** This command enables the context to configure Dual Stack Lite parameters.

## address

**Syntax** [no] address *ipv6-address*

|             |                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------|
| Context     | config>router>nat>inside>dual-stack-lite<br>config>service>vprn>nat>inside>dual-stack-lite                      |
| Description | This command configures the IP address of the NAT redundancy peer in the realm of this virtual router instance. |

subscriber-prefix-length

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>subscriber-prefix-length</b> <i>prefix-length</i><br><b>no subscriber-prefix-length</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Context     | config>router>nat>inside>dual-stack-lite                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Description | This command sets the value for the number of high order bits of the source IPv6 address that will be considered as DS-Lite subscriber. The remaining bits of the source IPv6 address will be masked off, effectively aggregation all IPv6 source addresses under the configured prefix length into a single DS-Lite subscriber. Source IPv4 addresses/ports of the traffic carried within the DS-Lite subscriber will be translated into a single outside IPv4 address and the corresponding deterministic port-block (port-blocks can be extended). |

The range of values for subscriber-prefix-length in non-deterministic DS-Lite is limited from 32 to 64 (a prefix will be considered as a DS-Lite subscriber) or it can be set to a value of 128 (the source IPv6 address is considered as a DS-Lite subscriber).

In cases where deterministic DS-Lite is enabled in a giver inside routing context, the range of values of the **subscriber-prefix-length** depends on the value of *dslite-max-subscriber-limit* parameter as follows:

**subscriber-prefix-length – n = [32..64,128]**

**where n = log2(dslite-max-subscriber-limit)**

[or in an alternate form: dslite-max-subscriber-limit = 2^n.]

In other words the largest prefix length for the deterministic DS-lite subscriber will be 32+n, where n = log2(dslite-max-subscriber-limit). The subscriber prefix length can extend up to 64 bits. Beyond 64 bits for the subscriber prefix length, there only one value is allowed: 128. In the case n must be 0, which means that the mapping between B4 elements (or IPv6 address) and the IPv4 outside addresses is in 1:1 ratio (no sharing of outside IPv4 addresses).

This parameter can be changed only when there are no deterministic prefixes configured in the same routing context.

The **no** form of the command reverts to the default.

|         |     |
|---------|-----|
| Default | 128 |
|---------|-----|

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>prefix-length</i> — In non-deterministic DS-Lite this value can be [32..64,128], assuming that the deterministic DS-Lite is not concurrently enabled in the same inside routing context. In case that deterministic DS-Lite is enabled, this value can be within the range [(32+n)..64,128] where $n = \log_2(\text{dslite-max-subscriber-limit})$ . The value of 128 is allowed only when $n=0$ (each subscriber is mapped to a single outside IPv4 IP address). |
| <b>Values</b>     | 32 to 64                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## ip-fragmentation

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-fragmentation {disabled   fragment-ipv6   fragment-ipv6-unless-ipv4-df-set}<br/>no ip-fragmentation</b>                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>router>nat>inside>dslite>address<br>config>router>nat>inside>nat64<br>config>service>vprn>nat>inside>nat64<br>config>service>vprn>nat>inside>dslite>address                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command configures downstream IPv6 fragmentation behavior in DS-lite and NAT64. IPv6 fragmentation is performed in the ISA. IPv4 fragmentation is not affected by this command. If desired, downstream IPv4 packet can be fragmented in the carrier IOM before the packet reaches ISA (and the NAT function). The IPv4 fragmentation in the downstream direction can be set by the <b>config&gt;router/vprn&gt;nat&gt;outside&gt;mtu</b> command |

### DS-Lite IPv6 Fragmentation in Downstream Direction (IPv4 to IPv6)

In case that the length of the received IPv4 packet is larger than the configured tunnel-mtu value while fragmentation is allowed, the resulting IPv6 packet will be fragmented (IPv4 is tunneled within IPv6). The maximum size of the of the fragmented IPv6 packet will be 48bytes larger than the configured tunnel-mtu value. This is due to the size of the tunneling IPv6 header: 40bytes basic IPv6 header + 8 bytes of extended fragmentation IPv6 header.

In case that fragmentation is not allowed while the IPv4 packet size is larger than configured tunnel-mtu size, the IPv4 packet will be dropped and an ICMPv4 Datagram Too Big message will be generated towards the source. The advertised mtu size in that ICMP message will be set to configured tunnel-mtu value.

### NAT64 IPv6 Fragmentation in Downstream Direction (IPv4to IPv6)

In contrast to DS-lite, NAT64 transport is not based on tunneling. Instead, IP headers are translated between IPv4 and IPv6. Consequently, NAT64 fragmentation operates based on the ipv6-mtu, as opposed to tunnel-mtu in DS-lite which represents the size of the tunnel payload (IPv4 packet).

In case that the length of the translated IPv6 packet exceeds the size of the configured ipv6-mtu value while fragmentation is allowed, the resulting IPv6 packet will be fragmented. The maximum size of the of the fragmented IPv6 packet will be the configured ipv6-mtu value.

In case that fragmentation is not allowed while the translated IPv6 packet size is larger than configured ipv6-mtu size, the IPv4 packet (that is supposed to be translated into IPv6) will be dropped and an ICMPv4 Datagram Too Big message will be generated towards the source. The advertised mtu size in that ICMP message will be set to the ipv6-mtu value minus 28bytes. The 28bytes comes from the size of the IPv6 overhead of the translated packet (20bytes difference between the IP header sizes ? 40bytes in IPv6 vs 20bytes in IPv4; 8 bytes for extended IPv6 fragmentation header).

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | disabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b> | <b>disabled</b> — IPv6 Fragmentation is disabled. In case that the packet size is larger than what is set by the mtu value (tunnel-mtu or ipv6-mtu) the IPv4 packet will be dropped and ICMPv4 Datagram Too Big messages will be sent back to the source.<br><b>fragment-ipv6</b> — IPv6 fragmentation will be performed in all cases, regardless of the DF bit setting in the tunneled/translated IPv4 packet.<br><b>fragment-ipv6-unless-ipv4-df-set</b> — IPv6 Fragmentation will be performed only in cases when DF bit in tunneled/translated IPv4 packet is cleared. |

## reassemble

|                    |                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] reassemble                                                                                                                                                                                       |
| <b>Context</b>     | config>router>nat>inside>dual-stack-lit>address                                                                                                                                                       |
| <b>Description</b> | This command enables reassembly of fragmented frames for DS-lite. Reassembly is enabled in the upstream direction per AFTR address.<br><br>The <b>no</b> form of the command disables the reassembly. |

## tunnel-mtu

|                    |                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tunnel-mtu</b> <i>mtu-bytes</i><br><b>no tunnel-mtu</b>                                                                                      |
| <b>Context</b>     | config>router>nat>inside>dual-stack-lit>address<br>config>service>vprn>nat>inside>dual-stack-lite                                               |
| <b>Description</b> | This command sets the size of the payload in IPv6 packet in downstream DS-lite direction. The payload is, in essence, the tunneled IPv4 packet. |

## l2-aware

|                |                          |
|----------------|--------------------------|
| <b>Syntax</b>  | <b>l2-aware</b>          |
| <b>Context</b> | config>router>nat>inside |



**Description** This command enters the “l2-aware” context for configuration specific to Layer 2-aware NAT.

address

**Syntax** [no] address ip-address/mask

**Context** config>router>nat>inside

**Description** This command configures the IP address and mask of the subnet.

The **no** form of the command removes the IP address and prefix length from the configuration.

**Default** none

**Parameters** ip-address/mask — Specifies the IP address and mask of the subnet.

**Values**

|             |          |
|-------------|----------|
| ip-address: | a.b.c.d  |
| mask:       | 16 to 32 |

nat64

**Syntax** [no] nat64

**Context** config>service>vprn>inside

**Description** This command enables the context to configure NAT64.

The **no** form of the command disables NAT64.

drop-zero-ipv4-checksum

**Syntax** [no] drop-zero-ipv4-checksum

**Context** config>service>vprn>inside>nat64

**Description** This command specifies if UDP datagrams with zero IPv4 checksum are dropped.

If this command is disabled, the system calculates the IPv6 checksum for each such datagram.

ignore-tos

**Syntax** [no] ignore-tos

---

|                    |                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>service>vprn>inside>nat64                                                                                                                                                                                        |
| <b>Description</b> | <p>This command specifies if the IPv4 Type Of Service (TOS) is ignored and the IPv6 traffic class bits set to zero.</p> <p>If this command is disabled, the system copies the IPv4 TOS into the IPv6 traffic class.</p> |
| <b>Default</b>     | disabled                                                                                                                                                                                                                |

## insert-ipv6-fragment-header

|                    |                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] insert-ipv6-fragment-header                                                                                                                                                                                                            |
| <b>Context</b>     | config>service>vprn>inside>nat64                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command specifies if the system always inserts an IPv6 fragment header, to indicate that the sender allows fragmentation.</p> <p>The <b>no</b> form of the command does not allow the system to insert an IPv6 fragment header.</p> |
| <b>Default</b>     | disabled                                                                                                                                                                                                                                    |

## l2-aware

|                    |                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>l2-aware</b>                                                                             |
| <b>Context</b>     | config>services>vprn>nat>inside                                                             |
| <b>Description</b> | This command enters the “l2-aware” context for configuration specific to Layer 2-aware NAT. |

## address

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] address <i>ip-address/mask</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>services>vprn>nat>inside>l2-aware                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command configures a Layer 2-aware NAT address. This address will act as a local address of the system. Hosts connected to the inside service will be able to ARP for this address. To verify connectivity, a host can also ping the address. This address is typically used as next hop of the default route of a Layer 2-aware host. The given mask defines a Layer 2-aware subnet. The (inside) IP address used by a Layer 2-aware host must match one of the subnets defined here or it will be rejected. |
| <b>Parameters</b>  | <p><i>ip-address</i> — Specifies the IP address in a.b.c.d format.</p> <p><i>mask</i> — Specifies the mask.</p>                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Values</b>      | 16 to 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## nat-policy

|                    |                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-policy</b> <i>nat-policy-name</i><br><b>no nat-policy</b>                                                                                                                       |
| <b>Context</b>     | config>services>vprn>nat>inside<br>config>router>nat>inside                                                                                                                            |
| <b>Description</b> | This command configures the NAT policy that will be used for large-scale NAT in this service.<br><br>The <b>no</b> form of the command removes the policy name from the configuration. |
| <b>Parameters</b>  | <i>nat-policy-name</i> — Specifies the NAT policy name, up to 32 characters.                                                                                                           |

## nat64

|                    |                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] nat64</b>                                                                                                        |
| <b>Context</b>     | config>service>vprn>nat>inside<br>config>router>nat>inside                                                               |
| <b>Description</b> | This command enables the context to configure NAT64 parameters.<br><br>The <b>no</b> form of the command disables NAT64. |

## drop-zero-ipv4-checksum

|                    |                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] drop-zero-ipv4-checksum</b>                                                                                                                                                                                            |
| <b>Context</b>     | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64                                                                                                                                                         |
| <b>Description</b> | This command enables the NAT64 node to drop received UDP datagrams with zero IPv4 checksum. By default, checksum is re-calculated for non-fragmented datagrams.<br><br>The <b>no</b> form of the command disables the command. |
| <b>Default</b>     | disabled                                                                                                                                                                                                                       |

## ignore-tos

|                |                                                                        |
|----------------|------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>[no] ignore-tos</b>                                                 |
| <b>Context</b> | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64 |

---

|                    |                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command specifies whether the IPv4 Type Of Service (TOS) is ignored and the IPv6 traffic class bits set to zero.</p> <p>When disabled, the system copies the IPv4 TOS into the IPv6 traffic class.</p> <p>The <b>no</b> form of the command recognizes the IPv4 Type Of Service (TOS).</p> |
| <b>Default</b>     | disabled                                                                                                                                                                                                                                                                                           |

## insert-ipv6-fragment-header

|                    |                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] insert-ipv6-fragment-header</b>                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64                                                                                                                                                                                                  |
| <b>Description</b> | <p>This command specifies whether the NAT64 node will insert IPv6 fragment header to IPv6 packets for which the DF bit is not set in the corresponding IPv4 packet, and is not already a fragment.</p> <p>The <b>no</b> form of the command disables the insertion.</p> |
| <b>Default</b>     | disabled                                                                                                                                                                                                                                                                |

## ipv6-mtu

|                    |                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipv6-mtu <i>ipv6-mtu</i></b><br><b>no ipv6-mtu</b>                                                                                                                           |
| <b>Context</b>     | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64                                                                                                          |
| <b>Description</b> | <p>This command sets the size of the IPv6 downstream packet in NAT64. This packet is translated from IPv4.</p> <p>The <b>no</b> form of the command reverts to the default.</p> |
| <b>Default</b>     | ipv6-mtu 1520                                                                                                                                                                   |
| <b>Parameters</b>  | <i>ipv6-mtu</i> — Specifies the IPv6 MTU.                                                                                                                                       |
| <b>Values</b>      | 1280 to 9212                                                                                                                                                                    |

## prefix

|               |                                                                    |
|---------------|--------------------------------------------------------------------|
| <b>Syntax</b> | <b>prefix <i>ipv6-prefix/prefix-length</i></b><br><b>no prefix</b> |
|---------------|--------------------------------------------------------------------|

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |              |                                                                                                  |               |                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--------------------------------------------------------------------------------------------------|---------------|------------------------|
| <b>Context</b>     | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64                                                                                                                                                                                                                                                                                                                                                                                                   |              |                                                                                                  |               |                        |
| <b>Description</b> | <p>This command configures the IPv6 prefix used to derive the IPv6 address from the IPv4 address, and is same as the prefix used by DNS64 to generate AAAA record returned for IPv4 endpoint resolution. NAT64 node announces this prefix in routing to attract traffic from IPv6 hosts. If the prefix is not configured, then a well-known prefix, 64:FF9B::/96, is used.</p> <p>The <b>no</b> form of the command removes the prefix from the NAT64 configuration.</p> |              |                                                                                                  |               |                        |
| <b>Parameters</b>  | <i>ipv6-prefix/prefix-length</i> — Specifies the NAT64 destination prefix.                                                                                                                                                                                                                                                                                                                                                                                               |              |                                                                                                  |               |                        |
| <b>Values</b>      | <table> <tr> <td>ipv6-prefix:</td><td> x::x::x::x::x::x (eight 16-bit pieces)<br/> x::x::x::x::d.d.d.d<br/> x - [0..FFFF]H<br/> d - [0..255]D </td></tr> <tr> <td>prefix-length</td><td>32, 40, 48, 56, 64, 96</td></tr> </table>                                                                                                                                                                                                                                        | ipv6-prefix: | x::x::x::x::x::x (eight 16-bit pieces)<br>x::x::x::x::d.d.d.d<br>x - [0..FFFF]H<br>d - [0..255]D | prefix-length | 32, 40, 48, 56, 64, 96 |
| ipv6-prefix:       | x::x::x::x::x::x (eight 16-bit pieces)<br>x::x::x::x::d.d.d.d<br>x - [0..FFFF]H<br>d - [0..255]D                                                                                                                                                                                                                                                                                                                                                                         |              |                                                                                                  |               |                        |
| prefix-length      | 32, 40, 48, 56, 64, 96                                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |                                                                                                  |               |                        |

## set-tos

|                    |                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>set-tos [0..255]</b><br><b>no set-tos</b>                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64                                                                                                                                                                                                           |
| <b>Description</b> | <p>This command specifies the value of the IPv4 Type Of Service (TOS) field. When enabled, the NAT64 node ignores IPv6 traffic-class and sets IPv4 TOS to supplied tos-value in the translated IPv4 packet.</p> <p>The <b>no</b> form of the command reverts to the default.</p> |
| <b>Default</b>     | set-tos 0                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <b>[0..255]</b> — Sets the IPv4 TOS to a fixed value the IPv6 Traffic Class and set the IPv4 TOS to a fixed value and ignores the IPv6 traffic class.                                                                                                                            |

## subscriber-prefix-length

|                    |                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>subscriber-prefix-length <i>prefix-length</i></b><br><b>no subscriber-prefix-length</b>                                  |
| <b>Context</b>     | config>service>vprn>nat>inside>nat64<br>config>router>nat>inside>nat64                                                      |
| <b>Description</b> | This command specifies the IPv6 address prefix length to be used for the NAT64 subscribers in this virtual router instance. |

The no form of the command

**Default** subscriber-prefix-length128

**Parameters** *prefix-length* — Specifies the subscriber identification for Large Scale NAT.

**Values** 32 to 64, 128

redundancy

**Syntax** redundancy

**Context** config>router>nat>inside  
config>service>vprn>nat>inside

**Description** This command enables the context to configure redundancy parameters.

peer

**Syntax** peer *ipv4-address*  
no peer

**Context** config>router>nat>inside>redundancy  
config>service>vprn>nat>inside>redundancy

**Description** This command is used in LSN44 multi-chassis redundancy in conjunction with filters. The configured peer address is an IPv4 address that is configured under an interface on the peering LSN44 node (active or standby). This IPv4 interface address is advertised via routing on the inside in order to attract traffic from the standby to the active LSN44 node.

If configured, the steering-route will be advertised only from the active LSN44 node. Consequently, upstream traffic for LSN44 will be attracted to the active LSN44 node. The nat action in the ipv4-filter on the active LSN44 node will forward traffic to the local MS-ISA where LSN44 function is performed. However, in that case that upstream traffic somehow arrives on the standby LSN44 node, the nat action in the IPv4-filter will forward traffic to the peer address (active LSN44 node).

The no form of the command removes the peer ipv4-address from the configuration.

**Default** none

**Parameters** *ipv4-address* — Specifies the IP address of the NAT redundancy peer.

**Values** ipv4-address:a.b.c.d

peer6

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | peer6 ipv6-address<br>no peer6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Context     | config>router>nat>inside>redundancy<br>config>service>vprn>nat>inside>redundancy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Description | <p>This command is used in NAT64 multi-chassis redundancy in conjunction with filters. The configured peer6 address is an IPv6 address configured under an interface on the peering NAT64 node (active or standby). This IPv6 interface address is advertised via routing on the inside in order to attract traffic from the standby to the active NAT64 node.</p> <p>Under normal circumstances, the NAT64 prefix will be advertised only from the active NAT64 node. Consequently, upstream traffic for NAT64 will be attracted to the active NAT64 node. The nat action in the ipv6-filter on the active NAT64 node will forward traffic to the local MS-ISA where NAT64 function is performed. However, in that case that upstream traffic somehow arrives on the standby NAT64 node, the nat action in the IPv6-filter will forward traffic to the peer6 address (active NAT64 node).</p> <p>The <b>no</b> form of the command removes the peer6 ip-address from the configuration.</p> |
| Default     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Parameters  | ipv6-address — Specifies the IPv6 address of the NAT redundancy peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Values      | <div>ipv6-address:      ipv6-address   - x:x:x:x:x:x:x:x   (eight 16-bit pieces)<br/>                         x:x:x:x:x:x:d.d.d.d<br/>                         x - [0..FFFF]H<br/>                         d - [0..255]D</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

steering-route

|             |                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | steering-route ip-prefix/length<br>no steering-route                                                                                                                                            |
| Context     | config>router>nat>inside>redundancy<br>config>service>vprn>nat>inside>redundancy                                                                                                                |
| Description | <p>This command is optionally used in LSN44 multi-chassis redundancy when filters are used on the inside to send traffic destined for the LSN44 function to MS-ISA, where NAT is performed.</p> |

If configured, the steering-route is advertised only from the active LSN44 node: the purpose is to bring the LSN44 node activity awareness to downstream routers. In this fashion, downstream routers can make a more intelligent decision when forwarding traffic in the upstream direction. Based on the steering-route, traffic can be sent directly towards the active LSN44 node. This route avoids an extra forwarding hop which would ensue in the case without LSN44 activity awareness, where the upstream traffic can be forwarded to the standby LSN44 node and then to the active LSN44 node.

LSN44 node activity (active/standby) is evaluated per isa-group based on monitoring routes advertised on the outside.

The **no** form of the command removes the ip-prefix/length from the configuration.

|            |                                                                                      |
|------------|--------------------------------------------------------------------------------------|
| Default    | none                                                                                 |
| Parameters | <i>ip-prefix/length</i> — Specifies the IP address and length of the steering route. |
| Values     |                                                                                      |
|            | ip-prefix: a.b.c.d                                                                   |
|            | ip-prefix-length: 0 to 32                                                            |

subscriber-identification

|             |                                                                                              |
|-------------|----------------------------------------------------------------------------------------------|
| Syntax      | <b>subscriber-identification</b>                                                             |
| Context     | config>router>nat>inside                                                                     |
| Description | This command enables the context to configure subscriber identification for Large Scale NAT. |

attribute

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>attribute</b> [ <b>vendor</b> <i>vendor-id</i> ] <b>attribute-type</b> <i>attribute-type</i><br><b>no attribute</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Context     | config>router>nat>inside>subscriber-identification<br>config>service>vprn>nat>inside>subscriber-identification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description | <p>This command defines the attribute that will in addition to framed-ip-address (inside IP address) and service-id be used for correlating BNG subscriber with the NAT subscriber.</p> <p>Only a single attribute at the time can be configured. The attribute will be extracted from the BNG accounting start and/or interim-update messages via Radius accounting proxy server. This attribute can be then optionally passed to the Large Scale NAT44 accounting server. User-name attribute (if included) in Large Scale NAT44 accounting messages will be automatically set to the subscriber-id string.</p> |



The attribute parameter can be changed at any given time and the change will be reflected automatically when the next interim-update message from the BNG host is received by the RADIUS accounting proxy.

In case that the BNG accounting message in RADIUS accounting proxy does not contain this attribute, subscriber aware Large Scale NAT44 functionality for this particular subscriber will be disabled.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | attribute vendor "nokia" attribute-type "alc-sub-string"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b> | <b>vendor</b> <i>vendor-id</i> — specifies the RADIUS vendor ID.<br><br><b>Values</b> standard, nokia (6527), 3gpp<br><b>Default</b> nokia<br><br><b>attribute-type</b> <i>attribute-type</i> — Specifies the RADIUS attribute to be used as subscriber identifier<br><br><b>Values</b> <b>alc-sub-string (nokia)</b> — Subscriber-id string (Alc-Subsc-ID-Str) is cached in Large Scale NAT44 application and used to correlate Large Scale NAT44 subscriber to BNG subscriber.<br><b>user-name (stnd)</b> — User-Name standard Radius attribute is cached in Large Scale NAT44 application and is used to correlate Large Scale NAT44 subscriber to BNG subscriber.<br><b>class (stnd)</b> — Class standard Radius attribute is cached in Large Scale NAT44 application and is used to correlate Large Scale NAT44 subscriber to BNG subscriber. Class attribute is initially set and send by Radius server. As such it must be echoed by BNG in all accounting messages.<br><b>station-id (stnd)</b> — Calling-Station-Id Radius attribute is cached in Large Scale NAT44 application and is used to correlate Large Scale NAT44 subscriber to BNG subscriber.<br><b>imsi (3gpp)</b> — International Mobile Subscriber Identification is used in WiFi Offload applications as a SIM card identifier.<br><b>imei (3gpp)</b> — International Mobile Equipment Identification is used in WiFi Offload applications as a physical phone device identifier. |

## drop-unidentified-traffic

|                    |                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] drop-unidentified-traffic</b>                                                                                                                                                                                                |
| <b>Context</b>     | config>router>nat>inside>subscriber-identification<br>config>service>vprn>nat>inside>subscriber-identification                                                                                                                       |
| <b>Description</b> | When this command denies address translation to subscribers that have not been identified via accounting messages sent by BNG and received by Radius accounting proxy. This command has effect only in Subscriber Aware Application. |

---

**Default** no drop-unidentified-traffic

## radius-proxy-server

**Syntax** **radius-proxy-server** *router router-instance name server-name*  
**no radius-proxy-server**

**Context** config>router>nat>inside>subscriber-identification  
config>service>vprn>nat>inside>subscriber-identification

**Description** This command configures RADIUS proxy server parameters. This is a reference to a RADIUS accounting proxy server in Subscriber Aware Large Scale NAT44 application. RADIUS accounting proxy server will cache attributes related to a BNG subscriber as they are received in standard accounting messages (RFC 2866). Radius accounting proxy server can be configured in any routing instance within 7750 SR.

**Default** none

**Parameters** **router** *router-instance* — Specifies the routing instance in which the RADIUS accounting proxy is configured.  
**name** *server-name* — Specifies the name reference to the RADIUS accounting proxy server that is instantiated in 7750 SR.

## mtu

**Syntax** **mtu** *mtu-size*  
**no mtu**

**Context** config>router>nat>outside

**Description** This command configures the MTU for downstream traffic flowing through this router (as outside NAT router). The system fragments IP datagrams exceeding the MTU.

**Default** no mtu

**Parameters** *mtu-size* — Specifies the MTU for downstream traffic.  
**Values** 512 to 9000

## pool

**Syntax** **pool** *nat-pool-name nat-group nat-group-id type pool-type [applications applications]*  
**[create]**  
**no pool** *nat-pool-name*

**Context** config>service>vprn>nat>outside

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | config>router>nat>outside                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | This command creates a NAT pool in the outside routing context. The nat pool defines the parameters that will be used for IP address and port translation within the pool.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <i>nat-pool-name</i> — Specifies the NAT pool name, up to 32 characters.<br><i>nat-group-id</i> — Specifies the NAT group ID.<br><b>Values</b> 1 to 4<br><b>create</b> — This parameter must be specified to create the instance.<br><i>pool-type</i> — Species the pool type, either large-scale or L2-aware.<br><b>Values</b> large-scale, l2-aware, wlan-gw-anchor<br><b>applications</b> <i>applications</i> — This creation-time parameter configures the nat-pool for protocol agnostic operation. The IP addresses are translated in 1:1 fashion regardless of the protocol. No ports are translated for TCP or UDP traffic. Traffic through the pool can be initiated from inside or outside. When nat-pool is configured in agnostic mode, certain parameters in the pool are pre-set and cannot be changed: <ul style="list-style-type: none"><li>• mode one-to-one</li><li>• port-forwarding-range 0</li><li>• port-reservation blocks 1</li><li>• subscriber-limit 1</li><li>• deterministic port-reservation 65536.</li></ul> This pool is used to configure static 1:1 NAT, where the operator have the control of the mapping between the inside and outside IP addresses. The static IP address mapping is using CLI constructs used in deterministic NAT (prefix and map deterministic NAT commands in the inside routing context).<br>ALG for TCP/UDP are supported in protocol agnostic pool.<br><b>Values</b> agnostic |

## address-range

|                    |                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>address-range</b> <i>start-ip-address end-ip-address</i> [ <b>create</b> ]<br><b>no address-range</b> <i>start-ip-address end-ip-address</i>                                                                                                      |
| <b>Context</b>     | config>service>vprn>nat>outside>pool<br>config>router>nat>outside>pool                                                                                                                                                                               |
| <b>Description</b> | This command configures a NAT address range.                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>start-ip-address</i> — Specifies the beginning IP address in a.b.c.d form.<br><i>end-ip-address</i> — Specifies the ending IP address in a.b.c.d. form.<br><b>create</b> — This parameter must be specified to create the address range instance. |

---

## drain

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] drain</b>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>service>vprn>nat>outside>pool>address-range<br>config>router>nat>outside>pool>address-range                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | This command starts or stops draining this NAT address range. When an address-range is being drained, it will not be used to serve new hosts. Existing hosts, however, will still be able to use the address that was assigned to them even if it is being drained. An address-range can only be deleted if the parent pool is shut down or if the range itself is effectively drained (hosts are no longer using the addresses). |

## external-assignment

|                    |                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] external-assignment</b>                                                                                                                                |
| <b>Context</b>     | config>router>nat>outside>pool<br>config>service>vprn>nat>outside>pool                                                                                         |
| <b>Description</b> | This command enables external allocation of L2-Aware NAT outside IP addresses from the pool.<br><br>The <b>no</b> form of the command disables the allocation. |

## mode

|                    |                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mode {auto   napt   one-to-one}</b><br><b>no mode</b>                                                                                |
| <b>Context</b>     | config>router>nat>outside>pool                                                                                                          |
| <b>Description</b> | This command specifies the mode of operation of this NAT address pool.<br><br>The <b>no</b> form of the command reverts to the default. |
| <b>Default</b>     | auto                                                                                                                                    |
| <b>Parameters</b>  | <b>{auto   napt   one-to-one}</b> — Specifies the mode of operation of this NAT pool.                                                   |

## port-forwarding-range

|                |                                                                                  |
|----------------|----------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>port-forwarding-range</b> <i>range-end</i><br><b>no port-forwarding-range</b> |
| <b>Context</b> | config>router>nat>outside>pool<br>config>service>nat>nat-policy                  |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | config>service>nat>firewall-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Description | <p>This command configures the end of the port range available for port forwarding. The start of the range is always equal to one.</p> <p>The number of ports that can be configured is half of the available block =&gt; 64512 : 2 = 32256</p> <p>In combination with port-forwarding-range the formulas are:</p> <p>"max port-reservation blocks" = 65535 - "port-forwarding-range"</p> <p>"max port-reservation ports" = (65535 - "port-forwarding-range") / 2</p> <p>with:</p> <p>the default min value for "port-forwarding-range" = 1023</p> <p>Also, the same applies for max port-forwarding-range if the port-reservation is already configured:</p> <p>"max port-forwarding-range" = 65535 - "port-reservation blocks"</p> <p>"max port-forwarding-range" = 65535 - ("port-reservation ports" * 2)</p> <p>The <b>no</b> form of the command reverts to the default.</p> |
| Default     | port-forwarding-range 1023                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Parameters  | <p><i>range-end</i> — Specifies the end of the port range available for port forwarding.</p> <p><b>Values</b> 1023 to 65535</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

deterministic

|             |                                                          |
|-------------|----------------------------------------------------------|
| Syntax      | deterministic                                            |
| Context     | config>service>vprn>nat>outside>pool                     |
| Description | This command configures deterministic NAT for this pool. |

port-reservation

|         |                                                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax  | <p>port-reservation <i>num-ports</i></p> <p>no port-reservation</p>                                                                            |
| Context | <p>config&gt;router&gt;nat&gt;outside&gt;pool&gt;deterministic</p> <p>config&gt;service&gt;vprn&gt;nat&gt;outside&gt;pool&gt;deterministic</p> |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command is applicable only to deterministic NAT. It configures the number of deterministic ports per subscriber (for example a subscriber is an inside IP address in LSN44 or IPv6 address or prefix in DS-lite). Once this command is enabled, the pool will transition into deterministic mode of operation. This means that the subscribers can use dynamic port-blocks in the pool only as a mean to expand the range of originally assigned deterministic ports. A pool with such property is referred to as deterministic pool. However, deterministic NAT and non-deterministic NAT cannot use the same pool simultaneously.</p> <p>All subscribers in deterministic pool are pre-mapped during the configuration phase to outside IP addresses and deterministic port-blocks. Because of this, the deterministic pool cannot be oversubscribed with subscribers (first-come, first-served).</p> <p>Once the deterministic pool becomes operational (no shutdown) a log is created. The same applies if the pool is disabled (shutdown). As a result of this one-time logging, there will be no additional logging when a subscriber starts using ports from the pre-assigned deterministic port block. This drastically reduces the logging overhead. However, when a deterministic port block is expanded by a dynamic port block, a log will be created on any allocation/de-allocation of the dynamic port block. The logs are also created for static port forwards (including PCP).</p> <p>The number of subscribers per outside IP address (subscriber-limit) multiplied by the number of deterministic ports per subscriber (port-reservation) will determine the port range of an outside IP address that will be dedicated to deterministic mappings. The number of subscribers per outside IP address in deterministic NAT must be power of 2 (<math>2^n</math>). Once the deterministic ports are allocated, the dynamic ports are carved out of the remaining port space of the same outside IP address according to the existing <b>port-reservation</b> command under the same hierarchy,</p> |
| <b>Parameters</b>  | <p><i>num-ports</i> — Specifies the number of ports in a deterministic port block that is allocated and dedicated to a single subscribers during the configuration phase.</p> <p><b>Values</b>      1 to 65536</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

port-reservation

|                    |                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <p><b>port-reservation blocks</b> <i>num-blocks</i><br/><b>port-reservation ports</b> <i>num-ports</i><br/><b>no port-reservation</b></p>                                                                                              |
| <b>Context</b>     | <p>config&gt;service&gt;vprn&gt;nat&gt;outside&gt;pool<br/>config&gt;router&gt;nat&gt;outside&gt;pool</p>                                                                                                                              |
| <b>Description</b> | <p>This command configures the size of the port-block that will be assigned to a host that is served by this pool. The number of ports configured here will be available to UDP, TCP and ICMP (as identifiers).</p>                    |
| <b>Parameters</b>  | <p><b>blocks</b> <i>num-blocks</i> — Specifies the number of port-blocks per IP address. Setting num-blocks to one (1) for large scale NAT will enable 1:1 NAT for IP addresses in this pool.</p> <p><b>Values</b>      1 to 64512</p> |

**ports** *num-ports* — Specifies the number of ports per block.

**Values** 1 to 32256

## mode

|                    |                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mode</b> { <b>auto</b>   <b>napt</b>   <b>one-to-one</b> }<br><b>no mode</b>                                                                                                                                                                                                                         |
| <b>Context</b>     | config>service>vprn>nat>outside>pool                                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command configures the mode of operation of this NAT pool.                                                                                                                                                                                                                                         |
| <b>Default</b>     | mode auto                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <b>napt</b> — Specifies NAPT (Network Address Port Translation)<br><b>auto</b> — The system selects the actual mode based upon other configuration parameters; the actual mode can be NAPT or 1:1 NAT (also known as 'Basic NAT').<br><b>one-to-one</b> — Indicates 1:1 NAT (also known as 'Basic NAT') |

## port-forwarding-dyn-block-reservation

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] <b>port-forwarding-dyn-block-reservation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>service>vprn>nat>outside>pool<br>config>service>router>nat>outside>pool                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command will enable the reservation of the dynamic port blocks when the first port forward for the subscriber is created. The dynamic port block allocation is logged only if the block is being utilized (mapping are created). In other words, dynamic port block reservation due to the port forward creation but without any dynamic mapping, will not be logged.</p> <p>The reserved port block will be released only when the last mapping in the block expires and there is not port forward associated with the subscriber. The de-allocation log (syslog or Radius) will be generated when the dynamic port block is completely released.</p> <p>Dynamic port block reservation can be enabled only if the configured maximum number of subscriber per outside IP address is less or equal then the maximum number of configured port blocks per outside IP address.</p> |
| <b>Default</b>     | no port-forwarding-dyn-block-reservation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## port-forwarding-range

|               |                                                                                  |
|---------------|----------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>port-forwarding-range</b> <i>range-end</i><br><b>no port-forwarding-range</b> |
|---------------|----------------------------------------------------------------------------------|

|             |                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------|
| Context     | config>service>vpn>nat>outside>pool                                                                                            |
| Description | This command specifies the end of the port range available for port forwarding. The start of the range is always equal to one. |
| Default     | port-forwarding-range 1023                                                                                                     |
| Parameters  | <i>range-end</i> — Specifies the port forwarding range end.<br><b>Values</b> 1023 to 65535                                     |

redundancy

|             |                                                                               |
|-------------|-------------------------------------------------------------------------------|
| Syntax      | <b>redundancy</b>                                                             |
| Context     | config>router>nat>outside>pool                                                |
| Description | This command enables the context to configure NAT pool redundancy parameters. |

export

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |         |                   |         |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------|-------------------|---------|
| Syntax            | <b>export</b> <i>ip-prefix/length</i><br><b>no export</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |         |                   |         |
| Context           | config>router>nat>outside>pool>redundancy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |         |                   |         |
| Description       | <p>This command configures the route to export to the peer. While the export prefix is configured and the value of the object <code>tmxNatPILsnRedActive</code> is equal to true, the system exports this prefix in the realm of the virtual router instance associated with this pool; to the NAT redundancy peer, the presence of this prefix is an indication that the Large Scale NAT function in this virtual router instance is active; hence, the export prefix of this system is the monitor prefix of the peer.</p> <p>The export prefix must be different from the monitor prefix.</p> |            |         |                   |         |
| Default           | no export                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |         |                   |         |
| Parameters        | <i>ip-prefix/length</i> — Specifies the IP address and length of the prefix to be exported.<br><b>Values</b><br><table><tr><td>ip-prefix:</td><td>a.b.c.d</td></tr><tr><td>ip-prefix-length:</td><td>0 to 32</td></tr></table>                                                                                                                                                                                                                                                                                                                                                                   | ip-prefix: | a.b.c.d | ip-prefix-length: | 0 to 32 |
| ip-prefix:        | a.b.c.d                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |         |                   |         |
| ip-prefix-length: | 0 to 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |         |                   |         |

follow

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| Syntax | <b>follow router</b> <i>router-instance</i> <b>pool</b> <i>name</i><br><b>no follow</b> |
|--------|-----------------------------------------------------------------------------------------|



---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>service>vprn>nat>outside>pool>redundancy<br>config>router> nat>outside>pool>redundancy                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | This command implicitly enables Pool Fate-Sharing Group (PFSG) which is required in case of multiple NAT policies per inside routing context. A NAT pool configured with this command will not advertise or monitor any route in order to change its (activity) state but instead it will directly follow the state of the lead pool in the PFSG. Once the lead pool changes its (activity) state, all the remaining pools following the lead pool will change their state accordingly. |
| <b>Default</b>     | no follow                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <b>router</b> <i>router-instance</i> — Specifies the routing instance where the lead pool resides.<br><b>Values</b> <router-name>   <service-id><br>router-name    - "Base"<br>service-id    - [1 to 2147483647]<br><b>pool</b> <i>name</i> — The pool whose activity state is being shared up to 32 characters in length.                                                                                                                                                              |

## monitor

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |         |                   |         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------|-------------------|---------|
| <b>Syntax</b>      | <b>monitor</b> <i>ip-prefix/length</i><br><b>no monitor</b>                                                                                                                                                                                                                                                                                                                                                                                                                             |            |         |                   |         |
| <b>Context</b>     | config>router>nat>outside>pool>redundancy                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |         |                   |         |
| <b>Description</b> | <p>This command configures the IP address of the prefix to be monitored.</p> <p>While the monitor prefix is configured, the system monitors the presence of this prefix in the routing table of the virtual router instance associated with this pool; the presence of this prefix is an indication that the NAT redundancy peer is active; the monitor prefix of this system is the export prefix of the peer.</p> <p>The monitor prefix must be different from the export prefix.</p> |            |         |                   |         |
| <b>Default</b>     | no monitor                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |         |                   |         |
| <b>Parameters</b>  | <i>ip-prefix/length</i> — Specifies the peer route to monitor.<br><b>Values</b> <table> <tr> <td>ip-prefix:</td><td>a.b.c.d</td></tr> <tr> <td>ip-prefix-length:</td><td>0 to 32</td></tr> </table>                                                                                                                                                                                                                                                                                     | ip-prefix: | a.b.c.d | ip-prefix-length: | 0 to 32 |
| ip-prefix:         | a.b.c.d                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |         |                   |         |
| ip-prefix-length:  | 0 to 32                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |         |                   |         |

## subscriber-limit

|               |                                                                    |
|---------------|--------------------------------------------------------------------|
| <b>Syntax</b> | <b>subscriber-limit</b> <i>limit</i><br><b>no subscriber-limit</b> |
|---------------|--------------------------------------------------------------------|

---

|                    |                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>service>vprn>nat>outside<br>config>router>nat>outside>pool                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command configures the maximum number of subscribers per outside IP address. In case multiple port blocks per subscriber are used, the block size is typically small; all blocks assigned to a given subscriber belong to the same IP address; the subscriber limit guarantees that any subscriber can get a minimum number of ports. |
| <b>Default</b>     | subscriber-limit 65535                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <i>limit</i> — Specify the maximum number of subscribers per IP address.<br><b>Values</b> 1 to 65535                                                                                                                                                                                                                                       |

## watermarks

|                    |                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>watermarks high percentage-high low percentage-low</b><br><b>no watermarks</b>                                                                                            |
| <b>Context</b>     | config>service>vprn>nat>outside>pool<br>config>router>nat>outside>pool                                                                                                       |
| <b>Description</b> | This command configures the watermarks for this NAT pool.                                                                                                                    |
| <b>Default</b>     | no watermarks                                                                                                                                                                |
| <b>Parameters</b>  | <i>high percentage-high</i> — Specifies the high percentage.<br><b>Values</b> 1 to 100<br><i>low percentage-low</i> — Specifies the low percentage.<br><b>Values</b> 0 to 99 |

## upstream-ip-filter

|                    |                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upstream-ip-filter filter-id</b><br><b>no upstream-ip-filter</b>                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>service>vprn>nat>outside<br>config>router>nat>outside                                                                                                                                                                                                                                                                  |
| <b>Description</b> | This command configures the ip-filter for upstream traffic. This filter is applied to the upstream traffic after the NAT function and before it enters the outside virtual router instance; it is useful for traffic that bypasses the ingress filters applied in the inside virtual router instance, such as DSLite traffic. |
| <b>Default</b>     | no upstream-ip-filter                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>filter-id</i> — Specifies the identifier of an IP filter.                                                                                                                                                                                                                                                                  |

## upstream-ipv6-filter

|                    |                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upstream-ipv6-filter</b> <i>filter-id</i><br><b>no upstream-ipv6-filter</b>                                                                                                                                                                                     |
| <b>Context</b>     | config>router>nat>outside<br>config>service>vprn>nat>outside                                                                                                                                                                                                       |
| <b>Description</b> | This command configures the ipv6-filter for upstream traffic. This filter is applied to the upstream traffic after the NAT function and before it enters the outside virtual router instance. This is useful for shared v6 filters that apply to all v6 DSM hosts. |
| <b>Default</b>     | no upstream-ipv6-filter                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>filter-id</i> — Specifies the identifier of an ipv6-filter.                                                                                                                                                                                                     |

## mss-adjust-group

|                    |                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mss-adjust-group</b> <i>nat-group-id</i> <b>segment-size</b> <i>segment-size</i><br><b>no mss-adjust-group</b>                                                                                                                          |
| <b>Context</b>     | config>router<br>config>service>vprn                                                                                                                                                                                                       |
| <b>Description</b> | This command associates the MSS adjust group consisting of multiple ISAs with the routing context in which the application requiring TCP MSS adjust resides.                                                                               |
| <b>Parameters</b>  | <i>nat-group-id</i> — Specifies the NAT group used for TCP MSS adjust.<br><i>segment-size</i> — Specifies the value to put into the TCP Maximum Segment Size (MSS) option if it is not already present, or if the present value is higher. |

## mtrace2

|                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mtrace2</b>                                                    |
| <b>Context</b>     | config>service>vprn<br>config>router                              |
| <b>Description</b> | This command traces a multicast path from a source to a receiver. |

## udp-port

|                |                                                      |
|----------------|------------------------------------------------------|
| <b>Syntax</b>  | <b>udp-port</b> <i>udp-port-number</i>               |
| <b>Context</b> | config>service>vprn>mtrace2<br>config>router>mtrace2 |

|             |                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | This command specifies the destination and listening port for the mtrace2 command. When set, this command generates mtrace2 packets with the set UDP-port, and also listens on the same port for any incoming mtrace2 packets. |
| Default     | 5000                                                                                                                                                                                                                           |
| Parameters  | <i>udp-port-number</i> — Specifies the UDP port for the test.<br><b>Values</b> 1024 to 49151                                                                                                                                   |

### 7.25.2.4 NAT Service Configuration Commands

#### nat-policy

|             |                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>nat-policy</b> <i>nat-policy-name</i> [create]<br><b>no nat-policy</b> <i>nat-policy-name</i>                                       |
| Context     | config>service>nat                                                                                                                     |
| Description | This command configures a NAT policy.                                                                                                  |
| Parameters  | <i>nat-policy-name</i> — Specifies the NAT policy name, up to 32 characters.<br><b>create</b> — Keyword used to create the NAT policy. |

#### alg

|             |                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------|
| Syntax      | <b>alg</b>                                                                                               |
| Context     | config>service>nat>nat-policy<br>config>service>nat>firewall-policy                                      |
| Description | This command enables the context to configure application layer gateway (ALG) parameters of this policy. |

#### ftp

|             |                                                                                          |
|-------------|------------------------------------------------------------------------------------------|
| Syntax      | [no] <b>ftp</b>                                                                          |
| Context     | config>service>nat>nat-policy>alg<br>config>service>nat>firewall-policy>alg              |
| Description | This command enables FTP ALG.<br><br>The <b>no</b> form of the command disables FTP ALG. |

**Default** ftp

## l2-outside

**Syntax** l2-outside  
no l2-outside

**Context** config>service>nat>nat-policy  
config>service>nat>firewall-policy

**Description** This command configures a NAT policy to be used with a Layer 2 outside service instead of a Layer 3 outside service. This command and the **pool** command are mutually exclusive.

**Default** no l2-outside

## pptp

**Syntax** [no] pptp

**Context** config>service>nat>nat-policy>alg

**Description** This command enables PPTP ALG.

The call-id is captured in the outgoing call management messages and along with the source IP address and the source TCP, is translated by NAT. Once the PPTP call is established, the call-id in the associated GRE packet in the incoming direction (from outside to inside) is correspondingly translated so that it matches the call-id mapping established during the call establishment phase. The call-ids used in the mappings are selected randomly and they try to honor parity (odds/even).

A PPTP session can be initiated only from the inside of NAT.

GRE traffic is allowed through NAT only if the corresponding mapping exists. This mapping is created during the call negotiation phase.

There can be seven calls (GRE tunnels) per control session.

**Default** no pptp

## rtsp

**Syntax** [no] rtsp

**Context** config>service>nat>nat-policy>alg  
config>service>nat>firewall-policy>alg

**Description** This command enables RTSP ALG.

---

The **no** form of the command disables RTSP ALG.

**Default** no rtsp

## sip

**Syntax** [no] sip

**Context** config>service>nat>nat-policy>alg  
config>service>nat>firewall-policy>alg

**Description** This command enables SIP ALG.

The **no** form of the command disables SIP ALG.

**Default** no sip

## block-limit

**Syntax** block-limit [1..40]  
no block-limit

**Context** config>service>nat>nat-policy

**Description** This command configures the maximum number of port blocks per subscriber.

The **no** form of the command reverts to the default.

**Default** block-limit 1

## filtering

**Syntax** filtering *filtering-mode*  
no filtering

**Context** config>service>nat>nat-policy  
config>service>nat>firewall-policy

**Description** This command configures the filtering of the NAT or residential firewall policy.

**Default** filtering endpoint-independent

**Parameters** *filtering-mode* — Specifies the way that inbound traffic is filtered.

**Values** address-and-port-dependent, endpoint-independent

## ipfix-export-policy

|                    |                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipfix-export-policy</b> <i>policy-name</i><br><b>no ipfix-export-policy</b>                                                                         |
| <b>Context</b>     | config>service>nat>nat-policy                                                                                                                          |
| <b>Description</b> | This command configures the IP flow information export policy.<br><br>The <b>no</b> form of the command removes the IP flow information export policy. |
| <b>Default</b>     | no ipfix-export-policy                                                                                                                                 |

## syslog-port-policy

|                    |                                                                                |
|--------------------|--------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>syslog-port-policy</b> <i>policy-name</i><br><b>no syslog-export-policy</b> |
| <b>Context</b>     | config>service>nat>nat-policy                                                  |
| <b>Description</b> |                                                                                |
| <b>Parameters</b>  | <i>policy-name</i> —                                                           |

## pool

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>pool</b> <i>nat-pool-name</i> <b>service-name</b> <i>service-name</i><br><b>pool</b> <i>nat-pool-name</i> <b>router</b> <i>router-instance</i><br><b>no pool</b>                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>service>nat>nat-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | This command configures the NAT pool of this policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <i>nat-pool-name</i> — Specifies the name of the NAT pool, up to 32 characters.<br><i>router-instance</i> — Specifies the router instance the pool belongs to, either by router name or service ID.<br><br><div> <b>Values</b> <div> 1 to 2147483647<br/> <i>svc-name</i> — a string up to 64 characters. </div> </div> <div> <b>Values</b> <div> <i>router-name</i>: “Base”   “management” </div> </div> <div> <b>Default</b> <div> Base </div> </div> <i>service-name</i> — Specifies the name of the service, up to 64 characters. |

---

## port-limits

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>port-limits</b>                                                  |
| <b>Context</b>     | config>service>nat>nat-policy<br>config>service>nat>firewall-policy |
| <b>Description</b> | This command configures the port limits of this policy.             |

## forwarding

|                    |                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>forwarding</b> <i>limit</i><br><b>no forwarding</b>                                                          |
| <b>Context</b>     | config>service>nat>nat-policy>port-limits<br>config>service>nat>firewall-policy>port-limits                     |
| <b>Description</b> | This command configures the maximum number of port forwarding entries.                                          |
| <b>Default</b>     | no forwarding                                                                                                   |
| <b>Parameters</b>  | <i>limit</i> — Specifies the maximum number of port forwarding entries per subscriber.<br><b>Values</b> 1 to 64 |

## reserved

|                    |                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>reserved</b> <i>num-ports</i><br><b>no reserved</b>                                                            |
| <b>Context</b>     | config>service>nat>nat-policy>port-limits                                                                         |
| <b>Description</b> | This command configures the number of ports per block that will be reserved for prioritized sessions.             |
| <b>Default</b>     | no reserved                                                                                                       |
| <b>Parameters</b>  | <i>num-ports</i> — Specifies the number of ports to reserve for prioritized sessions.<br><b>Values</b> 1 to 65534 |

## watermarks

|                |                                                                                          |
|----------------|------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>watermarks</b> <i>high percentage-high low percentage-low</i><br><b>no watermarks</b> |
| <b>Context</b> | config>service>nat>nat-policy>port-limits                                                |



---

|                    |                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command configures the port usage watermarks for the NAT policy.                                                                                                                      |
| <b>Default</b>     | no watermarks                                                                                                                                                                              |
| <b>Parameters</b>  | <i>percentage-high</i> — Specifies the high percentage.<br><div> <b>Values</b> 1 to 100 </div> <i>percentage-low</i> — Specifies the low percentage.<br><div> <b>Values</b> 0 to 99 </div> |

## watermarks

|                    |                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>watermarks high <i>percentage-high</i> low <i>percentage-low</i></b><br><b>no watermarks</b>                                                                                            |
| <b>Context</b>     | config>service>nat>nat-policy>session-limits<br>config>service>nat>firewall-policy>session-limits                                                                                          |
| <b>Description</b> | This command configures the session watermarks for the NAT or residential firewall policy.                                                                                                 |
| <b>Default</b>     | no watermarks                                                                                                                                                                              |
| <b>Parameters</b>  | <i>percentage-high</i> — Specifies the high percentage.<br><div> <b>Values</b> 1 to 100 </div> <i>percentage-low</i> — Specifies the low percentage.<br><div> <b>Values</b> 0 to 99 </div> |

## priority-sessions

|                    |                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] priority-sessions</b>                                                                |
| <b>Context</b>     | config>service>nat>nat-policy<br>config>service>nat>firewall-policy                          |
| <b>Description</b> | This command configures the prioritized sessions of this NAT or residential firewall policy. |

## reset-unknown-tcp

|                    |                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] reset-unknown-tcp</b>                                                                                                                                                                                       |
| <b>Context</b>     | config>service>nat>nat-policy                                                                                                                                                                                       |
| <b>Description</b> | This command specifies what to do when a TCP packet without the SYN flag set is received by the NAT inside for an unknown flow. When this is enabled, the packet will be dropped and a TCP reset will be generated. |

The no form of this command disables sending the reset; the packet will still be dropped.

**Default** no reset-unknown-tcp

## fc

**Syntax** [no] fc *fc-name*

**Context** config>service>nat>nat-policy>priority-sessions  
config>service>nat>firewall-policy>priority-sessions

**Description** This command configures the forwarding classes that have their sessions prioritized.

**Parameters** *fc-name* — Specifies the forwarding class.

**Values** be, l2, af, l1, h2, ef, h1, nc

## max

**Syntax** max *num-sessions*  
no max

**Context** config>service>nat>nat-policy>session-limits  
config>service>nat>firewall-policy>session-limits

**Description** This command configures the session limit of this policy. The session limit is the maximum number of sessions allowed for a subscriber associated with this policy

**Default** max 65535

**Parameters** *num-sessions* — Specifies the session limit.

**Values** 1 to 65535

## tcp-mss-adjust

**Syntax** tcp-mss-adjust *segment-size*  
no tcp-mss-adjust

**Context** config>service>nat>nat-policy  
config>service>nat>firewall-policy

**Description** This command configures the value to adjust the TCP Maximum Segment Size (MSS) option.  
The no form of the command returns the segment size to the default.

**Default** no tcp-mss-adjust

---

|                   |                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>segment-size</i> — specifies the value to put into the TCP Maximum Segment Size (MSS) option if not already present, or if the present value is higher. |
| <b>Values</b>     | 0, 160 to 10240                                                                                                                                            |

## tcp-mss-adjust

|                    |                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-mss-adjust</b>                                                                                                 |
| <b>Context</b>     | config>filter>ip-filter>entry>action<br>config>filter>ipv6-filter>entry>action                                        |
| <b>Description</b> | This command activates the adjustment of the TCP Maximum Segment Size (MSS) option of TCP packets matching the entry. |

## timeouts

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] timeouts</b>                                                |
| <b>Context</b>     | config>service>nat>nat-policy<br>config>service>nat>firewall-policy |
| <b>Description</b> | This command configures session idle timeouts for this policy.      |

## icmp-query

|                    |                                                                                                                                                                                                                                                                                                                                                                                      |               |        |                |   |               |         |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------|----------------|---|---------------|---------|
| <b>Syntax</b>      | <b>icmp-query [min <i>minutes</i>] [sec <i>seconds</i>]</b><br><b>no icmp-query</b>                                                                                                                                                                                                                                                                                                  |               |        |                |   |               |         |
| <b>Context</b>     | config>service>nat>nat-policy>timeouts                                                                                                                                                                                                                                                                                                                                               |               |        |                |   |               |         |
| <b>Description</b> | This command configures the timeout applied to an ICMP query session.                                                                                                                                                                                                                                                                                                                |               |        |                |   |               |         |
| <b>Default</b>     | icmp-query min 1                                                                                                                                                                                                                                                                                                                                                                     |               |        |                |   |               |         |
| <b>Parameters</b>  | <b>min <i>minutes</i></b> — Specifies the timeout, in minutes, applied to an ICMP query session<br><table> <tr> <td><b>Values</b></td><td>1 to 4</td></tr> <tr> <td><b>Default</b></td><td>1</td></tr> </table> <b>sec <i>seconds</i></b> — Specifies the timeout, in seconds, applied to an ICMP query session<br><table> <tr> <td><b>Values</b></td><td>1 to 59</td></tr> </table> | <b>Values</b> | 1 to 4 | <b>Default</b> | 1 | <b>Values</b> | 1 to 59 |
| <b>Values</b>      | 1 to 4                                                                                                                                                                                                                                                                                                                                                                               |               |        |                |   |               |         |
| <b>Default</b>     | 1                                                                                                                                                                                                                                                                                                                                                                                    |               |        |                |   |               |         |
| <b>Values</b>      | 1 to 59                                                                                                                                                                                                                                                                                                                                                                              |               |        |                |   |               |         |

---

## icmp6-query

|                    |                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>icmp6-query</b> [ <i>min minutes</i> ] [ <i>sec seconds</i> ]<br><b>no icmp6-query</b>                                                                                                                                                     |
| <b>Context</b>     | config>service>nat>firewall-policy>timeouts                                                                                                                                                                                                   |
| <b>Description</b> | This command configures the timeout interval for ICMPv6 query mappings.<br><br>The <b>no</b> form of the command reverts the timeout interval to the default of 1 minute.                                                                     |
| <b>Default</b>     | icmp6-query min 1                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <i>minutes</i> — Specifies the number of minutes in the ICMP query mapping timeout interval.<br><b>Values</b> 1 to 4<br><i>seconds</i> — Specifies the number of seconds in the ICMP query mapping timeout interval.<br><b>Values</b> 0 to 59 |

## sip

|                    |                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>sip</b> [ <i>hrs hours</i> ] [ <i>min minutes</i> ] [ <i>sec seconds</i> ]<br><b>no sip</b>                                                                                                                                                                                                   |
| <b>Context</b>     | config>service>nat>nat-policy>timeouts<br>config>service>nat>firewall-policy>timeouts                                                                                                                                                                                                            |
| <b>Description</b> | This command configures the SIP inactive media timeout.                                                                                                                                                                                                                                          |
| <b>Default</b>     | sip min 2                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>hours</i> — Specifies the SIP inactive media timeout, in hours.<br><b>Values</b> 1 to 2<br><i>minutes</i> — Specifies the SIP inactive media timeout, in minutes.<br><b>Values</b> 1 to 59<br><i>seconds</i> — Specifies the SIP inactive media timeout, in seconds.<br><b>Values</b> 1 to 59 |

## subscriber-retention

|                |                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>subscriber-retention</b> [ <i>hrs hours</i> ] [ <i>min minutes</i> ]<br><b>no subscriber-retention</b> |
| <b>Context</b> | config>service>nat>nat-policy>timeouts                                                                    |

---

|                    |                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command specifies the subscriber retention timeout, the time a NAT subscriber and its associated IP address is kept after all hosts and associated port blocks have expired.</p> <p>If a NAT subscriber host appears before the retention timeout has elapsed, it will be given the same outside IP address.</p>                  |
| <b>Default</b>     | no subscriber-retention                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <p><b>hrs</b> <i>hours</i> — Configures the hours a subscriber's IP address is kept after all hosts and port blocks have expired.</p> <p><b>Values</b> 1 to 24</p> <p><b>min</b> <i>minutes</i> — Configures the minutes a subscriber's IP address is kept after all hosts and port blocks have expired.</p> <p><b>Values</b> 1 to 59</p> |

## tcp-rst

|                    |                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <p><b>tcp-rst</b> [<b>min</b> <i>minutes</i>] [<b>sec</b> <i>sec</i>]</p> <p><b>no tcp-rst</b></p>                                                                                                                                                                                                                                                   |
| <b>Context</b>     | <p>config&gt;service&gt;nat&gt;nat-policy&gt;timeouts</p> <p>config&gt;service&gt;nat&gt;firewall-policy&gt;timeouts</p>                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command suspends the use of the outside TCP ports that have been used in translations for TCP connections that are closed via TCP RST. Once this timer expires, the outside ports can be reused for new TCP translations.</p> <p>The <b>no</b> form of the command reverts to the default.</p>                                               |
| <b>Default</b>     | no tcp-rst                                                                                                                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <p><i>minutes</i> — Specifies the timeout, in minutes, after receiving a RST and closing the session before going to the LISTEN state again</p> <p><b>Values</b> 1 to 4</p> <p><i>sec</i> — Specifies the timeout, in seconds, after receiving a RST and closing the session before going to the LISTEN state again</p> <p><b>Values</b> 1 to 59</p> |

## tcp-established

|                |                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <p><b>tcp-established</b> [<b>hrs</b> <i>hours</i>] [<b>min</b> <i>minutes</i>] [<b>sec</b> <i>seconds</i>]</p> <p><b>no tcp-established</b></p> |
| <b>Context</b> | <p>config&gt;service&gt;nat&gt;nat-policy&gt;timeouts</p> <p>config&gt;service&gt;nat&gt;firewall-policy&gt;timeouts</p>                         |

---

|                    |                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command configures the idle timeout applied to a TCP session in the established state.                                                                                                                                                    |
| <b>Default</b>     | tcp-established hrs 2 min 4                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <i>hours</i> — Specifies the timeout hours field.<br><b>Values</b> 1 to 24<br><i>minutes</i> — Specifies the timeout minutes field.<br><b>Values</b> 1 to 59<br><i>seconds</i> — Specifies the timeout seconds field.<br><b>Values</b> 1 to 59 |

## tcp-syn

|                    |                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-syn</b> [ <i>hrs hours</i> ] [ <i>min minutes</i> ] [ <i>sec seconds</i> ]<br><b>no tcp-syn</b>                                                                                                                                         |
| <b>Context</b>     | config>service>nat>nat-policy>timeouts<br>config>service>nat>firewall-policy>timeouts                                                                                                                                                          |
| <b>Description</b> | This command configures the timeout applied to a TCP session in the SYN state.                                                                                                                                                                 |
| <b>Default</b>     | tcp-syn sec 15                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <i>hours</i> — Specifies the timeout hours field.<br><b>Values</b> 1 to 24<br><i>minutes</i> — Specifies the timeout minutes field.<br><b>Values</b> 1 to 59<br><i>seconds</i> — Specifies the timeout seconds field.<br><b>Values</b> 1 to 59 |

## tcp-time-wait

|                    |                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-time-wait</b> [ <i>min minutes</i> ] [ <i>sec seconds</i> ]<br><b>no tcp-time-wait</b> |
| <b>Context</b>     | config>service>nat>nat-policy>timeouts<br>config>service>nat>firewall-policy>timeouts         |
| <b>Description</b> | This command configures the timeout applied to a TCP session in a time-wait state.            |
| <b>Default</b>     | no tcp-time-wait                                                                              |

**Parameters**     *minutes* — Specifies the timeout minutes field.  
                          **Values**        1 to 4  
                          *seconds* — Specifies the timeout seconds field.  
                          **Values**        1 to 59

## tcp-transitory

**Syntax**        **tcp-transitory** [*hrs hours*] [*min minutes*] [*sec seconds*]  
                          **no tcp-transitory**

**Context**        config>service>nat>nat-policy>timeouts  
                          config>service>nat>firewall-policy>timeouts

**Description**    This command configures the idle timeout applied to a TCP session in a transitory state.

**Default**        tcp-transitory min 4

**Parameters**    *hours* — Specifies the timeout hours field.  
                          **Values**        1 to 24  
                          *minutes* — Specifies the timeout minutes field.  
                          **Values**        1 to 59  
                          *seconds* — Specifies the timeout seconds field.  
                          **Values**        1 to 59

## udp

**Syntax**        **udp** [*hrs hours*] [*min minutes*] [*sec seconds*]  
                          **no udp**

**Context**        config>service>nat>nat-policy>timeouts  
                          config>service>nat>firewall-policy>timeouts

**Description**    This command configures the UDP mapping timeout.

**Default**        udp min 5

**Parameters**    *hours* — Specifies the timeout hours field.  
                          **Values**        1 to 24  
                          *minutes* — Specifies the timeout minutes field.  
                          **Values**        1 to 59

*seconds* — Specifies the timeout seconds field.

**Values** 1 to 59

## udp-dns

**Syntax** **udp-dns** [*hrs hours*] [*min minutes*] [*sec seconds*]  
**no udp-dns**

**Context** config>service>nat>nat-policy>timeouts  
config>service>nat>firewall-policy>timeouts

**Description** This command configures the timeout applied to a UDP session with destination port 53.

**Default** udp-dns sec 15

**Parameters** *hours* — Specifies the timeout hours field.

**Values** 1 to 24

*minutes* — Specifies the timeout minutes field.

**Values** 1 to 59

*seconds* — Specifies the timeout seconds field.

**Values** 1 to 59

## udp-initial

**Syntax** **udp-initial** [*min minutes*] [*sec seconds*]  
**no udp-initial**

**Context** config>service>nat>nat-policy>timeouts  
config>service>nat>firewall-policy>timeouts

**Description** This command configures the UDP mapping timeout applied to new sessions.

**Default** udp-initial sec 15

**Parameters** *minutes* — Specifies the timeout minutes field.

**Values** 1 to 59

*seconds* — Specifies the timeout seconds field.

**Values** 1 to 59



## unknown-protocol

|                    |                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>unknown-protocol</b> [ <i>hrs hours</i> ] [ <i>min minutes</i> ] [ <i>sec seconds</i> ]<br><b>no unknown-protocol</b>                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>service>nat>firewall-policy>timeouts                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command configures the timeout interval for unknown protocol mappings.<br><br>The <b>no</b> form of the command reverts the timeout interval to the default of 5 minutes.                                                                                                                                                                                                                    |
| <b>Default</b>     | unknown-protocol min 5                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>hours</i> — Specifies the number of hours in the unknown protocol mapping timeout interval.<br><br><b>Values</b> 0 to 24<br><i>minutes</i> — Specifies the number of minutes in the unknown protocol mapping timeout interval.<br><br><b>Values</b> 1 to 59<br><i>seconds</i> — Specifies the number of seconds in the unknown protocol mapping timeout interval.<br><br><b>Values</b> 0 to 59 |

## udp-inbound-refresh

|                    |                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] udp-inbound-refresh</b>                                                                |
| <b>Context</b>     | config>service>nat>nat-policy<br>config>service>nat>firewall-policy                            |
| <b>Description</b> | This command specifies whether or not UDP session timeout will be extended on inbound traffic. |
| <b>Default</b>     | no udp-inbound-refresh                                                                         |

## unknown-protocols

|                    |                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>unknown-protocols</b>                                                                                                                                              |
| <b>Context</b>     | config>service>nat>firewall-policy                                                                                                                                    |
| <b>Description</b> | This command enables the context to configure the treatment of flows of unknown Layer 4 protocols, which are protocols that cannot be natively handled by the system. |

---

## protocol

|                    |                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] protocol</b> { <i>number</i>   <b>any</b> }                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>service>nat>firewall-policy>unknown-protocols                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command configures the protocol numbers that are allowed to create unknown flows.</p> <p>Protocol or IPv6 extension header values that are explicitly supported by SR OS can be configured but will not be treated as unknown protocols.</p> <p>The <b>no</b> form of the command removes the allowance for the specified protocol to create unknown flows.</p> |
| <b>Parameters</b>  | <p><b>any</b> — Specifies that unknown flows can be created by any protocol.</p> <p><i>number</i> — Specifies the IANA number of a protocol that needs to be allowed to create unknown flows.</p> <p><b>Values</b>      0 to 255</p>                                                                                                                                    |

## pcp-server-policy

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>pcp-server-policy</b> <i>name</i> [ <b>create</b> ]<br><b>no pcp-server-policy</b> <i>name</i>                                                 |
| <b>Context</b>     | config>service>nat                                                                                                                                |
| <b>Description</b> | <p>This command configures a PCP server policy name.</p> <p>The <b>no</b> form of the command removes the name from the configuration.</p>        |
| <b>Parameters</b>  | <p><i>name</i> — Specifies a PCP server policy name up to 32 characters.</p> <p><b>create</b> — Keyword used to create the PCP server policy.</p> |

## lifetime

|                    |                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>lifetime</b> <b>minimum</b> <i>minimum</i> <b>maximum</b> <i>maximum</i><br><b>no lifetime</b> |
| <b>Context</b>     | config>service>nat>pcp-server-policy                                                              |
| <b>Description</b> | This command configures the lifetime of explicit mappings made by the PCP servers.                |
| <b>Default</b>     | lifetime minimum 120 maximum 86400                                                                |

---

|                   |                                                                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>minimum</i> — Specifies the minimum lifetime of explicit mappings made by the PCP servers using this PCP policy, in seconds.<br><b>Values</b> 60 to 86399 |
|                   | <i>maximum</i> — Specifies the maximum lifetime of explicit mappings made by the PCP servers using this PCP policy, in seconds.<br><b>Values</b> 61 to 86400 |

## max-description-size

|                    |                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>max-description-size</b> <i>size</i><br><b>no max-description-size</b>                                            |
| <b>Context</b>     | config>service>nat>pcp-server-policy                                                                                 |
| <b>Description</b> | This command specifies the maximum length of mapping descriptions made by the PCP servers using this PCP policy.     |
| <b>Default</b>     | max-description-size 64                                                                                              |
| <b>Parameters</b>  | <i>size</i> — Specifies the maximum length of mapping descriptions made by the PCP servers.<br><b>Values</b> 1 to 64 |

## opcode

|                    |                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] opcode</b>                                                                         |
| <b>Context</b>     | config>service>nat>pcp-server-policy                                                       |
| <b>Description</b> | This command specifies the PCP opcodes supported by the PCP servers using this PCP policy. |

## announce

|                    |                                                                       |
|--------------------|-----------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] announce</b>                                                  |
| <b>Context</b>     | config>service>nat>pcp-server-policy>opcode                           |
| <b>Description</b> | This command enables/disables support for the <b>announce</b> opcode. |
| <b>Default</b>     | no announce                                                           |

---

## get

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] get</b>                                                  |
| <b>Context</b>     | config>service>nat>pcp-server-policy>opcode                      |
| <b>Description</b> | This command enables/disables support for the <b>get</b> opcode. |
| <b>Default</b>     | no get                                                           |

## map

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] map</b>                                                  |
| <b>Context</b>     | config>service>nat>pcp-server-policy>opcode                      |
| <b>Description</b> | This command enables/disables support for the <b>map</b> opcode. |
| <b>Default</b>     | no map                                                           |

## option

|                    |                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] option</b>                                                                          |
| <b>Context</b>     | config>service>nat>pcp-server-policy                                                        |
| <b>Description</b> | This command configures the PCP options supported by the PCP servers using this PCP policy. |

## description

|                    |                                                                          |
|--------------------|--------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] description</b>                                                  |
| <b>Context</b>     | config>service>nat>pcp-server-policy>option                              |
| <b>Description</b> | This command enables/disables support for the <b>description</b> option. |
| <b>Default</b>     | no description                                                           |

## next

|                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] next</b>                                                  |
| <b>Context</b>     | config>service>nat>pcp-server-policy>option                       |
| <b>Description</b> | This command enables/disables support for the <b>next</b> option. |

**Default** no next

## port-reservation

**Syntax** [no] **port-reservation**

**Context** config>service>nat>pcp-server-policy>option

**Description** This command enables/disables support for the **port-reservation** option.

**Default** no port-reservation

## prefer-failure

**Syntax** [no] **prefer-failure**

**Context** config>service>nat>pcp-server-policy>option

**Description** This command enables/disables support for the **prefer-failure** option.

**Default** no prefer-failure

## third-party

**Syntax** [no] **third-party**

**Context** config>service>nat>pcp-server-policy>option

**Description** This command enables/disables support for the **third-party** option.

**Default** no third-party

## version

**Syntax** **version** **minimum** *minimum* **maximum** *maximum*  
**no version**

**Context** config>service>nat>pcp-server-policy

**Description** This command configures the accepted protocol version range.

**Default** version minimum 1 maximum 1

|            |                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------|
| Parameters | <i>minimum</i> — Specifies the minimum protocol version supported by the PCP servers using this PCP policy. |
|            | <b>Values</b> 1 to 255                                                                                      |
|            | <i>maximum</i> — Specifies the maximum protocol version supported by the PCP servers using this PCP policy. |
|            | <b>Values</b> 1 to 255                                                                                      |

port-forwarding

|             |                                                                               |
|-------------|-------------------------------------------------------------------------------|
| Syntax      | port-forwarding                                                               |
| Context     | config>service>nat                                                            |
| Description | This command enables the context to configure NAT port forwarding parameters. |

l2-aware

|             |                                                                                                                                                                                                                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>l2-aware subscriber</b> <i>sub-ident-string</i> <b>ip</b> <i>ip-address</i> <b>protocol</b> { <b>tcp</b>   <b>udp</b> } [ <b>port</b> <i>port</i> ] [ <b>outside-ip</b> <i>ip-address</i> ] [ <b>outside-port</b> <i>port</i> ] [ <b>nat-policy</b> <i>policy-name</i> ] [ <b>member</b> <i>member-id</i> ] [ <b>port-range-start</b> <i>port</i> ] |
|             | <b>no l2-aware subscriber</b> <i>sub-ident-string</i> <b>ip</b> <i>ip-address</i> <b>protocol</b> { <b>tcp</b>   <b>udp</b> <b>port</b> <i>port</i> }                                                                                                                                                                                                  |
| Context     | config>service>nat>fwd                                                                                                                                                                                                                                                                                                                                 |
| Description | This command creates NAT static port forwards for L2 aware subscribers. The ESM subscriber must be present in the system before this command is executed.                                                                                                                                                                                              |
|             | The <b>no</b> form of the command deletes NAT static port forwards for L2 aware subscribers.                                                                                                                                                                                                                                                           |
| Default     | none                                                                                                                                                                                                                                                                                                                                                   |
| Parameters  | <b>subscriber</b> <i>sub-ident-string</i> — This mandatory parameter specifies the ESM subscriber for which the SPF is to be created; ESM subscriber must be present in the system before the SPF can be created.                                                                                                                                      |
|             | <b>ip</b> <i>ip-address</i> — This mandatory parameter specifies the source IPv4/IPv6 address for which SPF will be created.                                                                                                                                                                                                                           |
|             | <b>protocol</b> { <b>tcp</b>   <b>udp</b> } — This mandatory parameter specifies the protocol to use, either TCP or UDP.                                                                                                                                                                                                                               |
|             | <b>port</b> <i>port</i> — This optional parameter specifies a source port.                                                                                                                                                                                                                                                                             |
|             | <b>Values</b> 1 to 65535                                                                                                                                                                                                                                                                                                                               |
|             | <b>outside-ip</b> <i>ipv4-address</i> — This mandatory parameter specifies the outside IPv4 address. If the outside IPv4 address is specified, then all other optional parameters become mandatory.                                                                                                                                                    |

**outside-port** *port* — This optional parameter specifies the outside port.

**nat-policy** *policy-name* — If multiple NAT policies are used inside the routing context, then the NAT policy should be specified in the SPF request so the SPF is created in the correct NAT pool. Otherwise, the default NAT policy from the inside routing context will be used.

**member** *member-id* — This optional parameter should not be used by the operator. It is used only if the command is replayed via the **exec** command or at **boot-config**. The *memberId* indicates the identifier of the NAT ISA group member associated with this NAT subscriber.

## Isn

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>Isn router</b> <i>router-instance</i> [ <b>b4</b> <i>ipv6-address</i> ] [ <b>aftr</b> <i>ipv6-address</i> ] <b>ip</b> <i>ip-address</i> <b>protocol</b> { <b>tcp udp</b> } [ <b>port</b> <i>port</i> ] [ <b>outside-ip</b> <i>ipv4-address</i> ] [ <b>outside-port</b> <i>port</i> ] [ <b>nat-policy</b> <i>nat-policy-name</i> ]<br><b>no Isn router</b> <i>router-instance</i> [ <b>b4</b> <i>ipv6-address</i> ] <b>ip</b> <i>ip-address</i> <b>protocol</b> { <b>tcp udp</b> } <b>port</b> <i>port</i> [ <b>nat-policy</b> <i>nat-policy-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>service>nat>fwd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command creates NAT static port forwards for LSN44, Ds-Lite and NAT64. Static port forwards (SPF) are static mappings created so that certain applications on the inside (private side) can be reached from host that are on the outside of the NAT. SPF statically map the subscriber (inside IP address in LSN44, CPE IPv6 address/prefix in DS-Lite and IPv6 prefix in NAT64), inside port and protocol to an outside IPv4 address, port and the same protocol.</p> <p>If only the inside router, the inside IPv4/v6 address/prefix and the protocol are configured as parameters in the SPF request, the remaining fields in the mapping (outside port and outside IPv4 address) will be selected automatically by the node and reported in CLI once the command execution is completed.</p> <p>Specifying the outside IPv4 address in the SPF request, mandates that all other, otherwise optional, parameters be also specified in the request (inside port and outside port). This creates a fully specified SPF request. Fully specified SPF request can be used in multi-chassis NAT redundancy deployments where the SPF is manually replicated between the SR OS nodes. In single chassis NAT deployments, fully specified SPF request is guaranteed to work only in the system with a single MS-ISA in it. Otherwise (multiple MS-ISAs in the system) a conflict may arise where two distinct inside IP addresses that may reside on separate MS-ISAs are requested to be mapped to the same outside IPv4 address. This will not be possible since the outside IPv4 address cannot be split across the MS-ISAs (each IP address, inside or outside, is tied to a single MS-ISA).</p> <p>In non-fully specified SPF requests (missing the inside port and/or outside port and the outside IPv4 address within the SPF request), the outside IPv4 address selection will depend on the configuration of the outside port in the SPF request:</p> |

- If the outside port is not specified or is specified from the configured **port-forwarding-range** [1024..port-forwarding-range], then the outside IPv4 address will be the same as the outside IPv4 address in an existing dynamic mapping for the same subscriber. If the subscriber does not exist (no dynamic mappings exist at the time of SPF creation request), then the subscriber will be automatically created and an outside IPv4 address will be assigned. In case that the outside ports are not available from the outside IPv4 address of the corresponding dynamic mapping, then the SPF request will fail. In other words, the dynamic and static mappings (created in this manner) for the same subscriber must use the same outside IPv4 address.
- If the outside port from the well-known port range [0 – 1023] is requested, then the outside IPv4 address does not have to match the outside IPv4 address of an existing dynamic mapping for the same subscriber, but can instead be any outside IPv4 address.

If multiple NAT policies per inside routing context are used, then the NAT policy must be specified in the SPF creation request. This is needed so the SPF be created in the correct pool.

SPFs are disabled by default and they must be explicitly enabled by the **port-limits forwarding** command within the NAT policy.

Configured SPFs, unlike SPFs created via the **tools** commands, are preserved across reboots without having to configure persistency (**config>system>persistence>nat-port-forwarding**) since they are part of the configuration. When the pool is shutdown the SPFs will be deactivated. When the pool is enabled (no shutdown), the SPFs (as created by tools command or via configuration) will be activated.

To avoid possible persistency related conflicts, SPFs can only be created using one method on a given node: either as configuration (the CLI **configure** branch) or using the **tools** command. For example: if a first SPF entry is created via CLI **tools** commands, the node will prevent SPF creation via configuration (the CLI **configure** branch) and vice versa.

The **no** form of the command deletes NAT static port forwards for LSN44, Ds-Lite and NAT64.

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default    | none                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Parameters | <b>router</b> <i>router-instance</i> — This mandatory parameter specifies the inside routing instance; router name or service-id.<br><br><b>Values</b> router-name, service-id<br><br><b>b4</b> <i>ipv6-address</i> — This optional parameter specifies the IPv6 address of the B4 element in DS-Lite.<br><br><b>Values</b> <ipv6-address>      : ipv6-address  - x:x:x:x:x:x:x (eight 16-bit pieces)<br>x:x:x:x:x:d.d.d.d<br>x - [0..FFFF]H<br>d - [0..255]D |



**aftr** *ipv6-address* — This optional parameter specifies IPv6 address of the AFTR element in DS-Lite.

**Values**      <ip-address>            : ipv4-address - a.b.c.d  
                                              ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)  
                                              x:x:x:x:x:x:d.d.d.d  
                                              x - [0..FFFF]H  
                                              d - [0..255]D

**protocol** {**tcp**|**udp**} — This mandatory parameter specifies the protocol to use, either TCP or UDP.

**port** *port* — This optional parameter specifies a source port.

**Values**            1 to 65535

**outside-ip** *ipv4-address* — This mandatory parameter specifies the outside IPv4 address. If the outside IPv4 address is specified, then all other optional parameters become mandatory.

**outside-port** *port* — This optional parameter specifies the outside port.

**nat-policy** *policy-name* — If multiple NAT policies are used inside the routing context, then the NAT policy should be specified in the SPF request so the SPF is created in the correct NAT pool. Otherwise, the default NAT policy from the inside routing context will be used.

### 7.25.2.5 NAT Outside Epipe Commands

#### nat-outside

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-outside</b> <i>nat-group-id</i> [ <b>create</b> ]<br><b>no nat-outside</b> <i>nat-group-id</i>                                                                                                                                                                                                                                                                                                                   |
| <b>Context</b>     | config>service>epipe                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command binds an Epipe to a NAT context running on an ISA-BB, allowing the Epipe to act as the outside service for the NAT or firewall. When <b>nat-outside</b> is enabled, one end of the Epipe is implicitly tied to ISA BB forwarding, leaving one remaining SAP, spoke, or similar available to be configured.</p> <p>The <b>no</b> version of this command removes the Epipe binding to a NAT context.</p> |
| <b>Parameters</b>  | <i>nat-group-id</i> — The NAT group ID where the PPPoE client is applied.                                                                                                                                                                                                                                                                                                                                               |

## shutdown

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                  |
| <b>Context</b>     | config>service>epipe>nat-outside                                                      |
| <b>Description</b> | This command administratively enables or disables the Epipe as a NAT outside service. |
| <b>Default</b>     | shutdown                                                                              |

### 7.25.2.6 IPFlow Information Export Protocol Commands

## ipfix

|                    |                                                                 |
|--------------------|-----------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipfix</b>                                                    |
| <b>Context</b>     | config>service                                                  |
| <b>Description</b> | This command enables the context to configure IPFIX parameters. |

## ipfix-export-policy

|                    |                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipfix-export-policy</b> <i>policy-name</i> [create]<br><b>no ipfix-export-policy</b> <i>policy-name</i>                                                                                                                                                                                                    |
| <b>Context</b>     | config>service>ipfix                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command creates an IPFIX export policy with a set of transport parameters that will be used to transmit IPFIX records generated by an application within 7750 SR node to an external collector node. This policy name can be referenced from each application within 7750 SR that requires flow logging. |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies the name of the policy that can be referenced within an application in 7750 SR node that requires flow logging.<br><b>create</b> — Keyword used to create the policy.                                                                                                          |

## collector

|                |                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>collector router</b> <i>router-instance</i> <b>ip</b> <i>ip-address</i> [create]<br><b>no collector router</b> <i>router-instance</i> <b>ip</b> <i>ip-address</i> |
| <b>Context</b> | config>service>ipfix>export-policy                                                                                                                                   |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command defines an external collector node that will collect IPFIX records sent by 7750 SR node. The IPFIX records will be streamed to the collector node using UDP transport. Traffic is originated from a random ephemeral UDP port to the destination port 4739. Up to two collector nodes can be defined for redundancy purposes.</p> <p>UDP streams are stateless due to the significant volume of transactions. However they do contain 32bit sequence numbers such that packet loss can be identified.</p> <p>Multiple IPFIX records are sent in a single UDP packet. UDP packet transmission is triggered when the packet size containing IPFIX records exceeds the configured MTU value or the internal timer which is set to 250ms, whichever occurs first.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <p><b>router</b> <i>router-instance</i> — Router instance from which the collector node is reachable.</p> <p><b>Values</b></p> <p>&lt;router-name&gt;   &lt;service-id&gt;</p> <p>router-name: "Base"</p> <p>service-id: 1 to 2147483647</p> <p><i>ip ip-address</i> — IPv4 address of the external collector node to which IPFIX records will be sent.</p> <p><b>create</b> — Keyword used to create the collector instance.</p>                                                                                                                                                                                                                                                                                                                                                 |

## mtu

|                    |                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <p><b>mtu</b> <i>mtu</i></p> <p><b>no mtu</b></p>                                                                                                                                                                                                                      |
| <b>Context</b>     | config>service>ipfix>export-policy>collector                                                                                                                                                                                                                           |
| <b>Description</b> | This command sets the MTU size of the UDP packet containing IPFIX records destined for the collector node. Multiple records will be stuffed into a single IP packet until stuffing an additional data record would exceed MTU or the internal timer of 250 ms expires. |
| <b>Default</b>     | mtu 1500                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><i>mtu</i> — Specifies the Maximum Transmission Unit range.</p> <p><b>Values</b> 512 to 9212</p>                                                                                                                                                                    |

## source-address

|               |                                                                                |
|---------------|--------------------------------------------------------------------------------|
| <b>Syntax</b> | <p><b>source-address</b> <i>ip-address</i></p> <p><b>no source-address</b></p> |
|---------------|--------------------------------------------------------------------------------|

|                    |                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>service>ipfix>export-policy>collector                                                                     |
| <b>Description</b> | This command configures the source address from which UDP streams containing IPFIX flow records will be sourced. |
| <b>Default</b>     | no source-address                                                                                                |
| <b>Parameters</b>  | <i>ip-address</i> — Source IPv4 address from which UDP streams are sent.                                         |

template-refresh-timeout

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>template-refresh-timeout</b> [hrs <i>hours</i> ] [min <i>minutes</i> ] [sec <i>seconds</i> ] [days <i>days</i> ]<br><b>no template-refresh-timeout</b>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Context</b>     | config>service>ipfix>export-policy>collector                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | This command configures the time interval in which Template Set messages are sent to the collector node. Template sets is an IPFIX message that defines fields for subsequent IPFIX messages but contains no data of its own. In other words, IPFIX data is not passed as set of TLVs, but instead data is encoded with a scheme defined through the Template Set message.                                                                                                                                                                                                   |
| <b>Default</b>     | template-refresh-timeout min 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <i>hours</i> — Specifies the time interval, in hours, after which IPFIX templates are resent to this collector.<br><b>Values</b> 1 to 24<br><i>minutes</i> — Specifies the time interval, in minutes, after which IPFIX templates are resent to this collector.<br><b>Values</b> 1 to 59<br><i>seconds</i> — Specifies the time interval, in seconds, after which IPFIX templates are resent to this collector.<br><b>Values</b> 1 to 59<br><i>days</i> — Specifies the time interval, in days, after which IPFIX templates are resent to this collector.<br><b>Values</b> 1 |

template-format

|                |                                                                         |
|----------------|-------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>template-format</b> {format1   format2}<br><b>no template-format</b> |
| <b>Context</b> | configure>service>ipfix>ipfix-export-policy                             |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <p>This command selects one of two template formats that contains a set of element IDs and their interpretation in IPFIX NAT flow logging. The difference between the two formats is related to the fields conveying information about the translated source IP addresses and ports (outside IP addresses and ports). Further, format 1 conveys information about the translated source port (post NAT) in the sourceTransportPort information element while format 2 conveys this information in the postNAPTsourceTrasportPort element.</p> <p>Further, format1 conveys information about the translated source port (post NAT) in the information element sourceTransportPort while a new information element postNAPTsourceTrasportPort is introduced in format2 to carry this information.</p> <p>For more information about template formats, see <a href="#">Template Formats</a>. <a href="#">Table 41</a> lists supported information elements and their description for each format.</p> <p>The <b>no</b> form of the command reverts to the default value.</p> |
| Default     | template-format format1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Parameters  | <p><b>format1</b> — Specifies that template format 1 is used by the IPFIX collectors associated with this IPFIX Export policy.</p> <p><b>format2</b> — Specifies that template format 2 is used by the IPFIX collectors associated with this IPFIX Export policy.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

### 7.25.2.7 AAA Policy Commands

#### isa-radius-policy

|             |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>isa-radius-policy</b> <i>name</i> [ <b>create</b> ]<br><b>no isa-radius-policy</b> <i>name</i>                                                                                                                                                                                                                                                                                                                       |
| Context     | config>aaa                                                                                                                                                                                                                                                                                                                                                                                                              |
| Description | <p>This command creates a policy template related to transport of accounting messages from the BB-ISA card to the accounting server. It also defines accounting attributes that will be included in accounting messages. The policy template will be instantiated once it is applied to the BB-ISA cards in the nat-group.</p> <p>The <b>no</b> form of the command removes the policy name from the configuration.</p> |
| Default     | none                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Parameters  | <p><i>name</i> — Specifies the name of the ISA RADIUS policy that can be referenced by a NAT application.</p> <p><b>create</b> — Keyword used to create the policy.</p>                                                                                                                                                                                                                                                 |

## acct-include-attributes

|                    |                                                                                  |
|--------------------|----------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] acct-include-attributes</b>                                              |
| <b>Context</b>     | config>aaa>isa-radius-plcy                                                       |
| <b>Description</b> | This command configures attributes to be included in RADIUS accounting messages. |

## auth-include-attributes

|                    |                                                                                      |
|--------------------|--------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] auth-include-attributes</b>                                                  |
| <b>Context</b>     | config>aaa>isa-radius-plcy                                                           |
| <b>Description</b> | This command configures attributes to be included in RADIUS authentication messages. |

## acct-delay-time

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>[no] acct-delay-time</b>                        |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes |
| <b>Description</b> | This command enables the acct-delay-time.          |
| <b>Default</b>     | no acct-delay-time                                 |

## acct-trigger-reason

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>[no] acct-trigger-reason</b>                    |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes |
| <b>Description</b> | This command enables the acct-trigger-reason.      |
| <b>Default</b>     | no acct-trigger-reason                             |

## called-station-id

|                    |                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] called-station-id</b>                                                                                                       |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes                            |
| <b>Description</b> | This command includes called station id attributes.<br><br>The <b>no</b> form of the command excludes called station id attributes. |

**Default** no called-station-id

## calling-station-id

**Syntax** [no] calling-station-id

**Context** config>aaa>isa-radius-plcy>acct-include-attributes  
config>aaa>isa-radius-plcy>auth-include-attributes

**Description** This command enables the inclusion of the calling-station-id attribute in RADIUS authentication requests and RADIUS accounting messages.

**Default** no calling-station-id

## circuit-id

**Syntax** [no] circuit-id

**Context** config>aaa>isa-radius-plcy>acct-include-attributes  
config>aaa>isa-radius-plcy>auth-include-attributes

**Description** This command enables the generation of the agent-circuit-id for RADIUS.

**Default** no circuit-id

## dhcp-options

**Syntax** [no] dhcp-options

**Context** config>aaa>isa-radius-plcy>acct-include-attributes  
config>aaa>isa-radius-plcy>auth-include-attributes

**Description** This command enables insertion of RADIUS VSA containing all dhcp-options from dhcp-discover (or dhcp-request) message. The VSA contains all dhcp-options in a form of the string. If required (the total length of all dhcp-options exceeds 255B), multiple VSAs are included.

**Default** no dhcp-options

## dhcp-vendor-class-id

**Syntax** [no] dhcp-vendor-class-id

**Context** config>aaa>isa-radius-plcy>acct-include-attributes  
config>aaa>isa-radius-plcy>auth-include-attributes

|                    |                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command includes the “[26-6527-36] Alc-DHCP-Vendor-Class-Id” attribute in RADIUS accounting messages. The content of the DHCP Vendor-Class-Identifier option (60) is mapped in this attribute. |
| <b>Default</b>     | no dhcp-vendor-class-id                                                                                                                                                                             |

dhcp6-options

|                    |                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] dhcp6-options                                                                                                               |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                               |
| <b>Description</b> | If a DHCPv6 stack is active for a UE, this attribute defines if options received in the last DHCPv6 message should be reflected. |
| <b>Default</b>     | no dhcp6-options                                                                                                                 |

dhcp6-options

|                    |                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] dhcp6-options                                                                                                                                        |
| <b>Context</b>     | config>aaa>isa-radius-plcy>auth-include-attributes                                                                                                        |
| <b>Description</b> | If authentication was triggered by DHCPv6, this knob defines if options received in that DHCPv6 message should be reflected in the radius Access-Request. |
| <b>Default</b>     | no dhcp6-options                                                                                                                                          |

ipv6-address

|                    |                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] ipv6-address                                                                                                        |
| <b>Context</b>     | config>aaa>isa-radius-plcy>auth-include-attributes                                                                       |
| <b>Description</b> | This attribute defines if the ipv6 address of the UE is present during authentication if the datatrigger packet is IPv6. |
| <b>Default</b>     | no ipv6-address                                                                                                          |

ipv6-address

|                |                                                    |
|----------------|----------------------------------------------------|
| <b>Syntax</b>  | [no] ipv6-address                                  |
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes |



---

|                    |                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | If an active IA_NA lease exists, this attribute defines if the IA_NA address of the UE is present in accounting. |
|--------------------|------------------------------------------------------------------------------------------------------------------|

|                |                 |
|----------------|-----------------|
| <b>Default</b> | no ipv6-address |
|----------------|-----------------|

## frame-counters

|               |                     |
|---------------|---------------------|
| <b>Syntax</b> | [no] frame-counters |
|---------------|---------------------|

|                |                                                    |
|----------------|----------------------------------------------------|
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes |
|----------------|----------------------------------------------------|

|                    |                                                     |
|--------------------|-----------------------------------------------------|
| <b>Description</b> | This command includes the frame-counters attribute. |
|--------------------|-----------------------------------------------------|

The **no** form of the command excludes frame-counters attribute.

|                |                   |
|----------------|-------------------|
| <b>Default</b> | no frame-counters |
|----------------|-------------------|

## framed-ip-addr

|               |                     |
|---------------|---------------------|
| <b>Syntax</b> | [no] framed-ip-addr |
|---------------|---------------------|

|                |                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------|
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes |
|----------------|----------------------------------------------------------------------------------------------------------|

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Description</b> | This command enables the inclusion of the framed-ip-addr attribute. |
|--------------------|---------------------------------------------------------------------|

The **no** form of the command excludes called framed-ip-addr attributes.

|                |                   |
|----------------|-------------------|
| <b>Default</b> | no framed-ip-addr |
|----------------|-------------------|

## framed-ip-netmask

|               |                        |
|---------------|------------------------|
| <b>Syntax</b> | [no] framed-ip-netmask |
|---------------|------------------------|

|                |                                                    |
|----------------|----------------------------------------------------|
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes |
|----------------|----------------------------------------------------|

|                    |                                                                        |
|--------------------|------------------------------------------------------------------------|
| <b>Description</b> | This command enables the inclusion of the framed-ip-netmask attribute. |
|--------------------|------------------------------------------------------------------------|

The **no** form of the command disables the inclusion.

|                |                      |
|----------------|----------------------|
| <b>Default</b> | no framed-ip-netmask |
|----------------|----------------------|

## framed-ipv6-prefix

|               |                         |
|---------------|-------------------------|
| <b>Syntax</b> | [no] framed-ipv6-prefix |
|---------------|-------------------------|

---

|                    |                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                               |
| <b>Description</b> | If an active SLAAC lease exists, this attribute defines if the SLAAC prefix of the UE is present in accounting.. |
| <b>Default</b>     | no framed-ipv6-prefix                                                                                            |

## hardware-timestamp

|                    |                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] hardware-timestamp                                                                                                                                       |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                            |
| <b>Description</b> | This command enables the inclusion of the hardware timestamp attributes.<br><br>The <b>no</b> form of the command excludes the hardware timestamp attributes. |
| <b>Default</b>     | no hardware-timestamp                                                                                                                                         |

## inside-service-id

|                    |                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] inside-service-id                                                                                                                                          |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                              |
| <b>Description</b> | This command enables the inclusion of the NAT inside service ID attributes.<br><br>The <b>no</b> form of the command excludes NAT inside service ID attributes. |
| <b>Default</b>     | no inside-service-id                                                                                                                                            |

## mac-address

|                    |                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] mac-address                                                                                         |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes |
| <b>Description</b> | This command enables the generation of the client MAC address RADIUS attribute.                          |
| <b>Default</b>     | no mac-address                                                                                           |

## multi-session-id

|               |                       |
|---------------|-----------------------|
| <b>Syntax</b> | [no] multi-session-id |
|---------------|-----------------------|

---

|                    |                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                        |
| <b>Description</b> | This command enables the inclusion of the multi-session-id attributes.<br><br>The <b>no</b> form of the command excludes the multi-session-id attributes. |
| <b>Default</b>     | no multi-session-id                                                                                                                                       |

## nas-identifier

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] nas-identifier</b>                                                                                                                        |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes                                          |
| <b>Description</b> | This command enables the inclusion of the NAS-Identifier attributes.<br><br>The <b>no</b> form of the command excludes NAS-Identifier attributes. |
| <b>Default</b>     | no nas-identifier                                                                                                                                 |

## nas-ip-address-origin

|                    |                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nas-ip-address-origin {isa-ip   system-ip}</b><br><b>no nas-ip-address-origin</b>                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>aaa>isa-radius-plcy                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | This command specifies the RADIUS NAS-IP-Address attribute.<br><br>The <b>no</b> form of the command reverts to the default.                                                                                                                                                                                                                                      |
| <b>Default</b>     | nas-ip-address-origin system-ip                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <b>system-ip</b> — Specifies that the value of the object TIMETRA-VRTR-MIB::vRialpAddress.1.1.1 is used.<br><br><b>isaip</b> — Specifies that a value in the range specified by tmnxRadIsaPlcySrvSrcAddrStart and tmnxRadIsaPlcySrvSrcAddrEnd is used that corresponds to the ISA card that transmits the Access-Request packet or the Accounting-Request packet. |

## nas-port-id

|                |                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>[no] nas-port-id</b>                                                                                  |
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes |

---

|                    |                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command enables the generation of the nas-port-id RADIUS attribute. Optionally, the value of this attribute (the SAP-id) can be prefixed by a fixed string and suffixed by the circuit-id or the remote-id of the client connection. If a suffix is configured, but no corresponding data is available, the suffix used will be 0/0/0/0/0/0. |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                |                |
|----------------|----------------|
| <b>Default</b> | no nas-port-id |
|----------------|----------------|

## nas-port-type

|               |                           |
|---------------|---------------------------|
| <b>Syntax</b> | [no] <b>nas-port-type</b> |
|---------------|---------------------------|

|                |                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------|
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes |
|----------------|----------------------------------------------------------------------------------------------------------|

|                    |                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command enables the generation of the NAS-Port-Type RADIUS attribute.<br><br>The <b>no</b> form of the command disables the generation. |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------|

|                |                  |
|----------------|------------------|
| <b>Default</b> | no nas-port-type |
|----------------|------------------|

## nat-subscriber-string

|               |                                   |
|---------------|-----------------------------------|
| <b>Syntax</b> | [no] <b>nat-subscriber-string</b> |
|---------------|-----------------------------------|

|                |                                                    |
|----------------|----------------------------------------------------|
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes |
|----------------|----------------------------------------------------|

|                    |                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command enables the inclusion of the NAT subscriber string attributes.<br><br>The <b>no</b> form of the command excludes NAT subscriber string attributes. |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                |                          |
|----------------|--------------------------|
| <b>Default</b> | no nat-subscriber-string |
|----------------|--------------------------|

## octet-counters

|               |                            |
|---------------|----------------------------|
| <b>Syntax</b> | [no] <b>octet-counters</b> |
|---------------|----------------------------|

|                |                                                    |
|----------------|----------------------------------------------------|
| <b>Context</b> | config>aaa>isa-radius-plcy>acct-include-attributes |
|----------------|----------------------------------------------------|

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command enables the inclusion of the octet-counters attributes.<br><br>The <b>no</b> form of the command excludes octet-counters attributes. |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|

|                |                   |
|----------------|-------------------|
| <b>Default</b> | no octet-counters |
|----------------|-------------------|

## outside-ip

|                    |                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] outside-ip</b>                                                                                                                    |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                        |
| <b>Description</b> | This command enables the inclusion of the outside IP attributes.<br><br>The <b>no</b> form of the command excludes outside IP attributes. |
| <b>Default</b>     | no outside-ip                                                                                                                             |

## outside-service-id

|                    |                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] outside-service-id</b>                                                                                                                                    |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                                |
| <b>Description</b> | This command enables the inclusion of the NAT outside service ID attributes.<br><br>The <b>no</b> form of the command excludes NAT outside service ID attributes. |
| <b>Default</b>     | no outside-service-id                                                                                                                                             |

## port-range-block

|                    |                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] port-range-block</b>                                                                                                                                  |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                            |
| <b>Description</b> | This command enables the inclusion of the NAT port range block attributes.<br><br>The <b>no</b> form of the command excludes NAT port range block attributes. |
| <b>Default</b>     | no port-range-block                                                                                                                                           |

## release-reason

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] release-reason</b>                                                                                                                        |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                |
| <b>Description</b> | This command enables the inclusion of the release reason attributes.<br><br>The <b>no</b> form of the command excludes release reason attributes. |
| <b>Default</b>     | no release-reason                                                                                                                                 |

---

## remote-id

|                    |                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] remote-id</b>                                                                                                                                                                                                           |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes                                                                                                                        |
| <b>Description</b> | <p>This command enables the sending of remote ID option. The client DHCP Unique Identifier (DUID) is used as the remote ID.</p> <p>The <b>no</b> form of the command disables the sending of remote ID option relay packet.</p> |
| <b>Default</b>     | no remote-id                                                                                                                                                                                                                    |

## wifi-ssid-vlan

|                    |                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] wifi-ssid-vlan</b>                                                                               |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes<br>config>aaa>isa-radius-plcy>auth-include-attributes |
| <b>Description</b> | This command enables including the per-SSID VLAN ID in Alc-Wlan-SSID-VLAN.                               |
| <b>Default</b>     | no wifi-ssid-vlan                                                                                        |

## password

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>password <i>password</i> [hash   hash2]</b><br><b>no password</b>                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>aaa>isa-radius-plcy                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command specifies the password that is used in the RADIUS access requests. It shall be specified as a string of up to 32 characters in length.</p> <p>The <b>no</b> form of the command resets the password to its default of <b>ALU</b> and will be stored using hash/hash2 encryption.</p>                                                                                                            |
| <b>Default</b>     | no password                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <p><i>password</i> — Specifies a password string up to 32 characters.</p> <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified</p> |

**hash2** — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

## periodic-update

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>periodic-update interval hours [rate-limit rate]</b><br><b>no periodic-update</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>aaa>isa-radius-plcy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | This command enables periodic RADIUS logging of currently allocated port blocks for a NAT subscriber (NAT binding).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Default</b>     | no periodic-update (no Interim Update messages are sent)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <p><b>interval hours</b> — Specifies the interval at which RADIUS logging is refreshed. The log generation might delayed past the configured interval value if the message pacing (rate-limit) is enabled or when the number of un-acknowledged (pending) messages in SR OS has reached its upper limit. An increased number of pending Interim Update messages in SR OS is due to lack of adequate responsiveness of the RADIUS server.</p> <p><b>Values</b> 1 to 72</p> <p><b>rate-limit rate</b> — Specifies the pacing of the Interim Update messages related to refreshment of the currently allocated port blocks. By default, when this command is disabled, the messages are sent at a high rate determined by the processing capability of the SR OS. Such a high message rate can exceed the processing power of the logging server which can result in the loss of logging information. To overcome this, the Interim Update messages can be generated in a staggered manner at a configured interval that is accommodating toward the processing capabilities of the logging server.</p> <p><b>Default</b> 1 to 100000 messages per second</p> |

## session-time

|                    |                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] session-time</b>                                                                                                                             |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                                   |
| <b>Description</b> | <p>This command enables the inclusion of the session-time attributes.</p> <p>The <b>no</b> form of the command excludes session-time attributes.</p> |
| <b>Default</b>     | no session-time                                                                                                                                      |

## subscriber-data

|                    |                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] subscriber-data</b>                                                                                                                     |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                              |
| <b>Description</b> | This command enables the inclusion of subscriber data attributes.<br><br>The <b>no</b> form of the command excludes subscriber data attributes. |
| <b>Default</b>     | no subscriber-data                                                                                                                              |

## subscriber-id

|                    |                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] subscriber-id</b>                                                                                |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                       |
| <b>Description</b> | This command specifies that subscriber ID attributes should be included into RADIUS accounting messages. |
| <b>Default</b>     | no subscriber-id                                                                                         |

## ue-creation-type

|                    |                                                               |
|--------------------|---------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] ue-creation-type</b>                                  |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes            |
| <b>Description</b> | This command enables including the Alc-Wlan-Ue-Creation-Type. |
| <b>Default</b>     | no ue-creation-type                                           |

## user-name

|                    |                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] user-name</b>                                                                                                               |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes                                                                                  |
| <b>Description</b> | This command enables the inclusion of user name attributes.<br><br>The <b>no</b> form of the command excludes user name attributes. |
| <b>Default</b>     | no user-name                                                                                                                        |



## wifi-rssi

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>[no] wifi-rssi</b>                              |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-include-attributes |
| <b>Description</b> | This command enables including the Alc-RSSI.       |
| <b>Default</b>     | no wifi-rssi                                       |

## acct-update-triggers

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>acct-update-triggers</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>aaa>isa-radius-plcy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>This command enables the context to enable or disable the sending of triggered interim-updates, with the exception of the following:</p> <ul style="list-style-type: none"> <li>• After an update interval change, an interim update is always sent to indicate the start of the new interval.</li> <li>• Mobility-triggered updates are configured in the (<b>service vprn &lt;svc-id&gt;   router</b>) <b>wlan-gw mobility-triggered-acct</b> context.</li> <li>• NAT port block allocation depends on the inclusion of NAT-related attributes (port-range, outside-service, outside-ip).</li> </ul> |

## address-state

|                    |                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] address-state</b>                                                                                                 |
| <b>Context</b>     | config>aaa>isa-radius-plcy>acct-update-triggers                                                                           |
| <b>Description</b> | If enabled, an interim-update will be sent for a DSM UE whenever a DHCP, SLAAC or DHCPv6 address gets allocated or freed. |
| <b>Default</b>     | no address-state                                                                                                          |

## access-algorithm

|                    |                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>access-algorithm {direct   round-robin   hash-based}</b><br><b>no access-algorithm</b>   |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers                                                          |
| <b>Description</b> | This command configures the algorithm used to access the list of configured RADIUS servers. |

---

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | access-algorithm direct                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b> | <b>direct</b> — Specifies that the first server will be used as primary server for all requests, the second as secondary and so on.<br><b>round-robin</b> — Specifies that the first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.<br><b>hashed-based</b> — Specifies that the selection is based on the hash-based procedures. |

## retry

|                    |                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>retry</b> <i>count</i>                                                                                                                                                                                                 |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers                                                                                                                                                                                        |
| <b>Description</b> | This command configures the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.<br><br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | retry 3                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <i>count</i> — Specifies the retry count.<br><b>Values</b> 1 to 10                                                                                                                                                        |

## router

|                    |                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>router</b> <i>router-instance</i><br><b>router</b> <b>service-name</b> <i>service-name</i><br><b>no router</b>                                                                                                        |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers                                                                                                                                                                                       |
| <b>Description</b> | This command specifies the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.<br><br>The <b>no</b> form of the command reverts to the default value. |
| <b>Default</b>     | no router                                                                                                                                                                                                                |

## server

|               |                                                                                             |
|---------------|---------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>server</b> <i>server-index</i> [ <b>create</b> ]<br><b>no server</b> <i>server-index</i> |
|---------------|---------------------------------------------------------------------------------------------|

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.</p> <p>Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.</p> <p>The <b>no</b> form of the command removes the server from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <p><i>server-index</i> — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.</p> <p><b>Values</b> 1 to 10 (a maximum of 5 accounting servers)</p> <p><b>create</b> — Keyword used to create the server index.</p>                                                                                                                                                                                                                                                                                     |

## source-address-range

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>source-address-range</b> <i>start-ip-address</i><br><b>no source-address-range</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>This command specifies the first IP address in the range of IPv4 addresses that are assigned to a BB-ISA in a given NAT group for NAT RADIUS accounting. The IP addresses are unique within the NAT group and are used to bind the RADIUS client instantiated on each BB-ISA card. The number of IPv4 addresses allocated is equal to the number of BB-ISAs in a NAT group that are enabled for NAT RADIUS accounting. Although only the first IPv4 address is explicitly configured with this command, each internally allocated IPv4 address associated with the BB-ISA card can be seen in the routing table (via show commands) as /32 with protocol designation 'NAT'.</p> |
| <b>Default</b>     | no source-address-range                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <p><i>start-ip-address</i> — The starting IP address of the IP address range.</p> <p><b>Values</b> 0.0.0.0 - 255.255.255.255</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## timeout

|               |                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>timeout</b> [ <b>sec</b> <i>seconds</i> ] [ <b>min</b> <i>minutes</i> ]<br><b>no timeout</b> |
|---------------|-------------------------------------------------------------------------------------------------|

---

|                    |                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers                                                                                                                                                      |
| <b>Description</b> | <p>This command configures the number of seconds the router waits for a response from a RADIUS server.</p> <p>The <b>no</b> form of the command reverts to the default value.</p>       |
| <b>Default</b>     | timeout sec 5                                                                                                                                                                           |
| <b>Parameters</b>  | <p><i>seconds</i> — Specifies the wait for a response from a RADIUS server, in seconds.</p> <p><i>minutes</i> — Specifies the wait for a response from a RADIUS server, in minutes.</p> |

## accounting

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>accounting</b> [port <i>udp-port</i> ]<br><b>no accounting</b>                                                                                 |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers>server                                                                                                         |
| <b>Description</b> | This command configures accounting for this server.                                                                                               |
| <b>Parameters</b>  | <p><i>port port</i> — Specifies the UDP port number on which to contact the RADIUS server for authentication.</p> <p><b>Values</b> 1 to 65535</p> |

## authentication

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>authentication</b> [port <i>udp-port</i> ]<br><b>no authentication</b>                                                                         |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers>server                                                                                                         |
| <b>Description</b> | This command configures authentication for this server.                                                                                           |
| <b>Default</b>     | no authentication                                                                                                                                 |
| <b>Parameters</b>  | <p><i>port port</i> — Specifies the UDP port number on which to contact the RADIUS server for authentication.</p> <p><b>Values</b> 1 to 65535</p> |

## coa

|               |                                                     |
|---------------|-----------------------------------------------------|
| <b>Syntax</b> | <b>coa</b> [port <i>udp-port</i> ]<br><b>no coa</b> |
|---------------|-----------------------------------------------------|

---

|                    |                                                                 |
|--------------------|-----------------------------------------------------------------|
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers>server                       |
| <b>Description</b> | This command configures Change of Authorization (CoA) messages. |
| <b>Default</b>     | no coa                                                          |

## ip-address

|                    |                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-address</b> <i>ip-address</i><br><b>no ip-address</b>                                                                                                                          |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers>server                                                                                                                                            |
| <b>Description</b> | This command configures the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate. |
| <b>Default</b>     | no ip-address                                                                                                                                                                        |

## secret

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>secret</b> <i>secret-key</i>   <b>hash-key</b> [ <b>hash</b>   <b>hash2</b> ]<br><b>no secret</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Context</b>     | config>aaa>isa-radius-plcy>servers>server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | This command configures the secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default</b>     | no secret                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <p><b>hash</b> — Specifies the key is entered in an encrypted form. If the <b>hash</b> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified</p> <p><b>hash2</b> — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the <b>hash2</b> encrypted variable cannot be copied and pasted. If the <b>hash</b> or <b>hash2</b> parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the <b>hash</b> or <b>hash2</b> parameter specified.</p> |

## user-name-format

|                |                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>user-name-format</b> <i>user-name-format</i> [ <b>mac-format</b> <i>mac-format</i> ]<br><b>no user-name-format</b> |
| <b>Context</b> | config>aaa>isa-radius-plcy                                                                                            |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <p>This command defines the format of the user-name field in the session authentication request sent to the RADIUS server. For authentication of IPv6 triggers (ICMPv6, DHCPv6, IPv6 data-trigger) the user-name format will always fall back to mac only.</p> <p>The <b>no</b> form of the command switches to the default format, <b>mac</b>.</p>                                                                                                                                                                                                                                                                                  |
| Default     | user-name-format mac mac-format alu (the MAC source address of the DHCP DISCOVER message is used in the user-name field)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Parameters  | <p><i>user-name-format</i> — Specifies the user name format in RADIUS message.</p> <p><i>mac-format</i> — Specifies how a MAC address is represented when contacting a RADIUS server. This is only used while the value of is equal to the DHCP client vendor options and if the MAC address is used by default of the DHCP client vendor options.</p> <div><div>Examples:</div><div><div>ab:</div><div>XY-</div><div>mmmm.</div></div><div><div>00:0c:f1:99:85:b8</div><div>00-0C-F1-99-85-B8</div><div>0002.03aa.abff</div></div><div><div>Nokia 7xxx style</div><div>IEEE canonical style</div><div>Cisco style</div></div></div> |

### 7.25.2.8 NAT Syslog Commands

#### syslog

|             |                                                                                        |
|-------------|----------------------------------------------------------------------------------------|
| Syntax      | <b>syslog</b>                                                                          |
| Context     | config>service>nat                                                                     |
| Description | This command enables the context to configure syslog reporting of NAT flow parameters. |

#### syslog-export-policy

|             |                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>syslog-export-policy</b> <i>name</i> [create]<br><b>no syslog-export-policy</b> <i>name</i>                                                                                                                                                                                                                                                                          |
| Context     | config>service>nat>syslog                                                                                                                                                                                                                                                                                                                                               |
| Description | <p>This command creates a syslog export policy with a set of transport parameters that are used to transmit NAT flow records in syslog format to an external collector node. This policy name is then referenced from the NAT policy applied to an inside routing context.</p> <p>The <b>no</b> form of the command removes the policy name from the configuration.</p> |
| Parameters  | <p><i>name</i> — Specifies the syslog export policy name, up to 32 characters.</p> <p><b>create</b> — Keyword used to create the syslog export policy.</p>                                                                                                                                                                                                              |

---

## collector

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>collector router</b> <i>router-name</i> <b>ip</b> <i>ip-address</i> [ <b>create</b> ]<br><b>collector service-name</b> <i>service-name</i> <b>ip</b> <i>ip-address</i> [ <b>create</b> ]<br><b>no collector router</b> <i>router-name</i> <b>ip</b> <i>ip-address</i><br><b>no collector service-name</b> <i>service-name</i> <b>ip</b> <i>ip-address</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>This command defines an external collector node that collects syslog records. The syslog records are streamed to the collector node using UDP transport. Traffic is originated from a random ephemeral UDP port to the destination port 514. Up to two collector nodes can be defined for redundancy purposes.</p> <p>Stateless UDP streams are used as transport due to the significant volume of transactions. However, they do contain 32-bit sequence numbers so packet loss can be identified. The sequence numbers are generated per BB-ISA per collector, and within each stream they are monotonically increased by 1. Overlapping sequence numbers between BB-ISAs can be differentiated by the MDA ID field carried in the syslog message.</p> <p>Multiple syslog records are sent in a single UDP packet. UDP packet transmission is triggered when the packet size containing syslog records exceeds the configured MTU value or the configurable timer, whichever occurs first.</p> <p>The <b>no</b> form of the command removes the parameters from the configuration.</p> |
| <b>Parameters</b>  | <p><i>router-name</i> — Specifies the router instances from which the collector node is reachable.</p> <p><i>ip-address</i> — Specifies the IPv4 address of the external collector node to which the syslog records are sent.</p> <p><i>service-name</i> — Specifies the service name from which the collector node is reachable.</p> <p><b>create</b> — Keyword used to create the collector instance.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## destination-port

|                    |                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>destination-port</b> [ <i>destination-port</i> ]                                                                            |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>collector                                                                       |
| <b>Description</b> | This command configures the destination port (collector port) to which UDP stream containing the syslog flow records are sent. |
| <b>Default</b>     | destination-port 514                                                                                                           |
| <b>Parameters</b>  | <p><i>destination-port</i> — Specifies the destination port to which UDP streams are sent.</p> <p><b>Values</b> 1 to 65535</p> |

---

## ipv4-source-address

|                    |                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipv4-source-address</b> <i>ip-address</i><br><b>no ipv4-source-address</b>                                                                                                                                           |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>collector                                                                                                                                                                |
| <b>Description</b> | <p>This command configures the IPv4 source address from which the UDP streams containing syslog flow records are sourced.</p> <p>The <b>no</b> form of the command removes the IPv4 address from the configuration.</p> |
| <b>Parameters</b>  | <i>ip-address</i> — Specifies the source IPv4 address from which UDP streams are sent.                                                                                                                                  |

## facility

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>facility</b> <i>syslog-facility</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command configures a syslog facility. For more information, refer to the <i>7450 ESS</i>, <i>7750 SR</i>, <i>7950 XRS</i>, and <i>VSR System Management Guide</i>. The <b>config&gt;log&gt;syslog&gt;level</b> hierarchy also applies to this context.</p>                                                                                                                                                                                                                                                                                |
| <b>Default</b>     | facility local0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | <p><i>syslog-facility</i> — Specifies a syslog facility name which represents a specific numeric facility code. The code must be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.</p> <p><b>Values</b>      kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7</p> |

## include

|                    |                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] include</b>                                                                                           |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                |
| <b>Description</b> | <p>This command enables the context to specify the optional fields to include in the NAT syslog messages.</p> |



---

## destination-ip

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] destination-ip</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>include                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | This command includes the destination IP address in the flow log. The <b>destination-ip</b> is significant in Destination Based NAT (DNAT) where the foreign IP address is translated. A foreign IP address is the original IP address toward the destination node and in DNAT it is replaced by the <b>destination-ip</b> . More clearly, on the inside (private side), the IP address of the destination node is referred to as foreign IP (original destination IP), and once this address is translated by DNAT, it is referred to as destination IP (translated destination IP) on the outside (public side). |

The **no** form of the command disables the feature.

## foreign-ip

|                    |                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] foreign-ip</b>                                                                                                                                                                      |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>include                                                                                                                                      |
| <b>Description</b> | This command includes the foreign IP address in the flow log. A foreign IP address is the original IP address toward the destination node and in DNAT it is replaced by the destination IP. |

If DNAT is not used, the foreign IP address (the IP address of the destination node) is the same on both sides of NAT.

The **no** form of the command disables the feature.

## foreign-port

|                    |                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] foreign-port</b>                                                                                                                                                    |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>include                                                                                                                      |
| <b>Description</b> | This command includes the foreign port address in the flow log. A foreign port is the port towards the destination node and this port is not translated by any form of NAT. |

A foreign port (the port towards the destination node) is the same on both sides of NAT.

The **no** form of the command disables the feature.

## nat-policy-name

|               |                             |
|---------------|-----------------------------|
| <b>Syntax</b> | <b>[no] nat-policy-name</b> |
|---------------|-----------------------------|

---

|                    |                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>include                                                                    |
| <b>Description</b> | This command includes the NAT policy name in the flow log.<br><br>The <b>no</b> form of the command disables the feature. |

## sub-id

|                    |                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] sub-id                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy>include                                                                                                                                                                                                                       |
| <b>Description</b> | This command includes the <b>sub-id</b> string in the flow log. The <b>sub-id</b> is applicable only in subscriber-aware NAT. If subscriber-aware NAT is not enabled, the <b>sub-id</b> string is set to '-'.<br><br>The <b>no</b> form of the command disables the feature. |

## log-prefix

|                    |                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>log-prefix</b> <i>prefix-text</i>                                                                                                                                                                                                        |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                                                                                                                                              |
| <b>Description</b> | This command configures the syslog log prefix. For more information, refer to the <i>7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide</i> . The <b>config&gt;log&gt;syslog&gt;level</b> hierarchy also applies to this context. |
| <b>Default</b>     | log-prefix "TMNX"                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>prefix-text</i> — Specifies an alphanumeric string, up to 32 characters. Spaces and colons ( : ) cannot be used in the string.                                                                                                           |

## max-tx-delay

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>max-tx-delay</b> <i>deciseconds</i><br><b>no max-tx-delay</b>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command enables aggregation of flow log messages within a syslog frame. It introduces a delay during which logs are collected in each BB-ISA so they can be sent in a single syslog message to conserve system resources and network bandwidth.<br><br>When aggregation is enabled, generation of a syslog frame carrying multiple flow logs is triggered by one of the two events (whichever occurs first): <ul style="list-style-type: none"><li>• Expiry of the max-tx-delay timer</li></ul> |

- Exceeding MTU size

The **no** form of the command reverts to the default.

|                   |                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | max-tx-delay 3                                                                                             |
| <b>Parameters</b> | <i>deciseconds</i> — Specifies the maximum time a syslog message is delayed in the system's output buffer. |
| <b>Values</b>     | 1 to 100                                                                                                   |

## mtu

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mtu</b> <i>mtu-size</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>The command defines defines the MTU, the maximum size of the IP frame that can be transmitted. The size of the frame includes the syslog message and the IP header. This is an IP-MTU value.</p> <p>When aggregation is enabled (the <b>max-tx-delay</b> command), generation of a syslog frame carrying multiple flow logs is triggered by one of the two events (whichever occurs first):</p> <ul style="list-style-type: none"><li>• Expiry of the max-tx-delay timer</li><li>• Exceeding MTU size</li></ul> |
| <b>Default</b>     | mtu 1500                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>mtu-size</i> — Specifies the MTU size in bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Values</b>      | 512 to 9000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## rate-limit

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>rate-limit</b> <i>packets-per-second</i><br><b>no rate-limit</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>service>nat>syslog>syslog-export-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b> | <p>This command configures the maximum rate limit at which syslog messages are sent. Once the rate limit is exceeded, NAT flow logs will be buffered. Overload condition is characterized by exhaustion of this buffer space. This condition can occur due to imposed rate limit or the software speed limit. Once the buffer space is exhausted, new flow creation will be denied, and the teardown of the existing flows will be delayed until the buffer space becomes available.</p> <p>The <b>no</b> form of the command removes the maximum rate limit from the configuration.</p> |

Parameters

packets-per-second — Specifies the packet rate limit in seconds.

Values

10 to 2147483647

severity-level

Syntax

severity-level *syslog-level*

Context

config>service>nat>syslog>syslog-export-policy

Description

This command configures the severity level.

For more information, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. The **config>log>syslog>level** hierarchy also applies to this context.

Default

severity-level info

Parameters

*syslog-level* — Specifies the severity level.

Values

emergency, alert, critical, error, warning, notice, info, debug

7.25.2.9 NAT Subscriber Management Commands

nat-policy

Syntax

nat-policy *policy-name*  
no nat-policy

Context

config>subscr-mgmt>sub-profile

Description

This command configures the NAT policy to be used for subscribers associated with this subscriber profile.

Parameters

*policy-name* — Specifies the policy name, up to 32 characters.

save-deterministic-script

Syntax

save-deterministic-script

Context

admin>nat

Description

This command saves the script that calculates Deterministic NAT map entries.

Once the location for the Python deterministic NAT script is configured, the script is generated/updated every time deterministic NAT configuration is modified. However, the script must be manually exported to the remote location. This command triggers the export of the script to a remote location.

## upnp

|                    |                                                               |
|--------------------|---------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp</b>                                                   |
| <b>Context</b>     | config>service                                                |
| <b>Description</b> | This command enables the context to configure UPnP parameters |

## upnp-policy

|                    |                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp-policy</b> <i>policy-name</i> [create]<br><b>no upnp-policy</b> <i>policy-name</i>                                                                                                                         |
| <b>Context</b>     | config>service>upnp                                                                                                                                                                                                |
| <b>Description</b> | This command creates a new upnp-policy or enters the configuration context of an existing upnp-policy.<br><br>The <b>no</b> form of the command removes the upnp-policy <i>policy-name</i> from the configuration. |
| <b>Default</b>     | none                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies the name of the UPnP policy up to 32 characters.                                                                                                                                    |

## upnp-policy

|                    |                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp-policy</b> <i>policy-name</i><br><b>no upnp-policy</b>                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>subscr-mgmt>sub-prof                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | This command enables UPnP IGD services for the subscriber. All ESM hosts of the subscriber could use the UPnP protocol to create port mapping. This feature only support L2-Aware NAT host.<br><br>UPnP parameters are defined in the referenced upnp-policy configured in the <b>config&gt;service&gt;upnp</b> context. |
| <b>Default</b>     | no upnp-policy                                                                                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies the UPnP (Universal Plug 'n Play) policy associated with this subscriber profile up to 32 characters.                                                                                                                                                                                     |

---

## http-listening-port

|                    |                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>http-listening-port</b> <i>http-listening-port</i><br><b>no http-listening-port</b>                                     |
| <b>Context</b>     | config>service>upnp>upnp-policy                                                                                            |
| <b>Description</b> | This command specifies the listening port of UPnP server.<br><br>The <b>no</b> form of the command reverts to the default. |
| <b>Default</b>     | http-listening-port 5000                                                                                                   |
| <b>Parameters</b>  | <i>http-listening-port</i> — Specifies the HTTP TCP port this UPnP IGD listens to.<br><b>Values</b> 1 to 65535             |

## mapping-limit

|                    |                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>mapping-limit</b> <i>limit</i><br><b>no mapping-limit</b>                                                                               |
| <b>Context</b>     | config>service>upnp>upnp-policy                                                                                                            |
| <b>Description</b> | This command specifies the maximum number of UPnP mapping per subscriber.<br><br>The <b>no</b> form of the command reverts to the default. |
| <b>Default</b>     | mapping-limit 256                                                                                                                          |
| <b>Parameters</b>  | <i>limit</i> — Specifies the upper limit of the number of UPnP mappings per subscriber.<br><b>Values</b> 1 to 256                          |

## strict-mode

|                    |                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] strict-mode</b>                                                                                                                                 |
| <b>Context</b>     | config>service>upnp>upnp-policy                                                                                                                         |
| <b>Description</b> | This command enable UPnP strict mode. With strict-mode, system only allows changes to existing UPnP mapping if the request comes from same UPnP client. |
| <b>Default</b>     | no strict-mode                                                                                                                                          |

## 7.25.2.10 NAT Subscriber Management BRG Commands

### brg-profile

|                    |                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>brg-profile</b> <i>profile-name</i> [create]<br><b>no brg-profile</b> <i>profile-name</i>                                                                                                                                                                             |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg                                                                                                                                                                                                                                              |
| <b>Description</b> | This command creates the profile Bridged Residential Gateway (BRG) devices. The BRG profile specifies default parameters that are used for host management under a single BRG.<br><br>The <b>no</b> form of the command removes the profile name from the configuration. |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <i>profile-name</i> — Specifies the name of the BRG profile.                                                                                                                                                                                                             |

### connectivity-verification

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>connectivity-verification</b> [count <i>nr-of-attempts</i> ] [timeout <i>timeout-seconds</i> ] [retry-time <i>retry-seconds</i> ]<br><b>no connectivity-verification</b>                                                                                                                                                                                                                                                                                                      |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | This command configures the BRG connectivity verification. The system uses ICMP Echo request messages for connectivity verification.<br><br>When the last host associated to a BRG is removed, a ping mechanism is used to verify if the BRG is still active. This command specifies the parameters used in this mechanism.<br><br>The no form of this command disables the BRG ping mechanism and removes the BRG without verification. Any configured hold-time still applies. |
| <b>Default</b>     | connectivity-verification count 3 timeout 30 retry-time 900                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <b>count</b> <i>nr-of-attempts</i> — Specifies the number of connectivity verification attempts this system makes before a BRG is considered down.<br><br><b>Values</b> 1 to 5<br><br><b>timeout</b> <i>timeout-seconds</i> — Specifies the time, in seconds, after which an unanswered ping is considered failed.<br><br><b>Values</b> 5 to 60                                                                                                                                  |

**retry-time** *retry-seconds* — Specifies the time, in seconds, that the system waits while it considers a BRG down, before it starts a new connectivity verification cycle. If a ping succeeds, the mechanism will be retried after this time.

**Values**      300 to 3600

dhcp-pool

**Syntax**      **dhcp-pool**

**Context**      config>subscr-mgmt>vrgw>brg>brg-profile

**Description**      This command enables the context to configure per-subscriber IPv4 address pool parameters to be used for address allocation. Pools for different subscribers can overlap. Specific pool parameters can be overridden by RADIUS.

lease-time

**Syntax**      **least-time** [**days** *days*] [**hrs** *hrs*] [**min** *min*] [**sec** *sec*]  
                 **lease-time** *seconds*  
                 **no lease-time**

**Context**      config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool

**Description**      This command configures the lease time, in seconds, to be used when allocating addresses from the pool. This time should always be larger than the renew/rebind time.

                 The **no** form of the command reverts to the default.

**Default**      lease-time 600

**Parameters**      *seconds* — Specifies the lease time.

**Values**      10 to 315446399

options

**Syntax**      **options**

**Context**      config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool

**Description**      This command enables the context to configure options that are reflected in DHCP.

**Default**      none



## custom-option

|                    |                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>custom-option</b> <i>option-number</i> <b>address</b> [ <i>ip-address...</i> (upto 4 max)]<br><b>custom-option</b> <i>option-number</i> <b>hex</b> <i>hex-string</i><br><b>custom-option</b> <i>option-number</i> <b>string</b> <i>ascii-string</i><br><b>no custom-option</b> <i>option-number</i>                                                                                   |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool>options                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | This command configures DHCP options.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <i>option-number</i> — Specifies the number of this DHCP option.<br><b>address</b> [ <i>ip-address...</i> (upto 4 max)] —<br><b>hex</b> <i>hex-string</i> — Specifies the hex value of this option.<br><b>Values</b> 0x0 to 0xFFFFFFFF (maximum 254 hex nibbles)<br><b>string</b> <i>ascii-string</i> — Specifies an ASCII value of this option.<br><b>Values</b> 127 characters maximum |

## subnet

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>subnet</b> <i>ip-prefix/prefix-length</i> <b>start</b> <i>ip-address</i> <b>end</b> <i>ip-address</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command configures the subnet that will be used for the I2aware-subscriber. This subnet is only locally significant and can overlap with other subscribers. The subnet is derived by ignoring the host-bits of the ip-address. The ip address specifies the default gateway that will be signaled in DHCP along with the netmask derived from the prefix-length.</p> <p>The start and end addresses specify the addresses that are suitable for allocation within the given subnet, the start and end address included. If the subnet address (host-bits 0), broadcast address (host-bits 1) or default-gw address fall in this range, they will not be considered for allocation.</p> <p>Changing the subnet will only have effect for new subscribers. New and existing hosts for existing subscribers will keep allocating from the original subnet.</p> <p>The <b>no</b> form of this command removes the subnet configuration. New I2-aware subscribers will no longer use this pool and fall back to a pool from radius. Existing subscribers will keep using the original subnet.</p> |
| <b>Default</b>     | no subnet                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>ip-prefix/prefix-length</i> — Specifies the IP prefix and prefix length.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**start** *ip-address* — Specifies the starting IP address.

**end** *ip-address* — Specifies the ending IP address.

## hold-time

|                    |                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>hold-time</b> [ <b>days</b> <i>days</i> ] [ <b>hrs</b> <i>hrs</i> ] [ <b>min</b> <i>min</i> ] [ <b>sec</b> <i>sec</i> ]<br><b>hold-time</b> <i>seconds</i><br><b>no hold-time</b>                                                                                                                                                                                                      |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | When the BRG should be deleted this still holds the BRG object for the specified time. This applies when connectivity-verification fails or when the last host is removed and <b>no connectivity-verification</b> is enabled. Hold time does not apply to an explicit removal via <b>radius</b> or <b>clear</b> commands.<br><br>The <b>no</b> form of the command deletes the hold-time. |
| <b>Default</b>     | no hold-time                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Parameters</b>  | <i>seconds</i> — Specifies the time to hold on to a BRG after this system considered it down.<br><b>Values</b> 30 to 2592000                                                                                                                                                                                                                                                              |

## initial-hold-time

|                    |                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>initial-hold-time</b> [ <b>min</b> <i>min</i> ] [ <b>sec</b> <i>sec</i> ]<br><b>initial-hold-time</b> <i>seconds</i><br><b>no initial-hold-time</b>                                                     |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                    |
| <b>Description</b> | This command configures the time to hold on to a BRG immediately after the system detected its presence. The hold time does not apply in case this system removes the BRG context upon an explicit request |
| <b>Default</b>     | initial-hold-time 300                                                                                                                                                                                      |
| <b>Parameters</b>  | <i>seconds</i> — Specifies the initial time, in seconds, to hold on to a BRG after this system considered it down.<br><b>Values</b> 0 to 900                                                               |

## radius-proxy-server

**Syntax** [**no**] **radius-proxy-server** **router** *router-instance* **name** *server-name*

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b> | <p>This command enables BRG processing on the specified RADIUS proxy server. Whenever an Access-Accept is received with the attribute Alc-BRG-Id present, this will trigger the creation of a BRG. The BRG will use the brg-profile specified in Access-Accept or otherwise fall-back to this brg-profile. When the specified radius-proxy-server has a cache enabled, no cache entries will be created for a transaction identified as BRG. A RADIUS proxy server can only be listed in one brg-profile.</p> <p>This command can be executed multiple times.</p> <p>The <b>no</b> form of this command removes BRG processing for the specified radius-proxy server.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <p><b>router</b> <i>router-instance</i> — Specifies the ID of the VRF where the proxy server is located.</p> <p><b>name</b> <i>server-name</i> — Specifies the name of the RADIUS proxy server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## radius-server-policy

|                    |                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>radius-server-policy</b> <i>policy-name</i><br><b>no radius-server-policy</b>                                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command is used if the BRG needs to be authenticated to the PCMP by the vG. This is required if the BRG does not perform radius authentication via the proxy itself. The vG will originate a valid Access Request using the BRG ID as username.</p> <p>The <b>no</b> form of this command removes the radius-server-policy from the configuration. Setup of an unauthenticated BRG will now fail.</p> |
| <b>Default</b>     | no radius-server-policy                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies the RADIUS server policy up to 32 characters in length to be applied in this subscriber authentication policy.                                                                                                                                                                                                                                                                 |

## sla-profile-string

|                    |                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>sla-profile-string</b> <i>string</i><br><b>no sla-profile-string</b>                                                                                                                                                                                            |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                                                                            |
| <b>Description</b> | <p>This command configures the SLA profile string which will be used as a default for SLA-profile lookup. This string can be overridden during BRG or host authentication.</p> <p>The <b>no</b> form of the command removes the string from the configuration.</p> |

---

|                   |                                                                                |
|-------------------|--------------------------------------------------------------------------------|
| <b>Default</b>    | no sla-profile-string                                                          |
| <b>Parameters</b> | <i>string</i> — Specifies the string to use to look up the subscriber profile. |

## sub-profile-string

|                    |                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>sub-profile-string</b> <i>string</i><br><b>no sub-profile-string</b>                                                                                                                                                          |
| <b>Context</b>     | config>subscr-mgmt>vrgw>brg>brg-profile                                                                                                                                                                                          |
| <b>Description</b> | <p>This string will be used as a default for subscriber-profile lookup. This string can be overridden during BRG or host authentication.</p> <p>The <b>no</b> form of the command removes the string from the configuration.</p> |
| <b>Default</b>     | no sub-profile-string                                                                                                                                                                                                            |
| <b>Parameters</b>  | <i>string</i> — Specifies the string used to look up the subscriber profile.                                                                                                                                                     |

## 7.25.2.11 NAT DNAT Commands

### dnat

|                    |                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] <b>dnat</b>                                                                                     |
| <b>Context</b>     | config>service>nat>nat-policy                                                                        |
| <b>Description</b> | This command defines context for destination NAT (DNAT) specific configuration under the nat-policy. |

### dnat-only

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dnat-only router</b> <i>router-instance</i> <b>nat-group</b> <i>nat-group-id</i><br><b>no dnat-only</b>                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>service>nat>nat-policy>dnat                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command configures outside routing context and nat-group in which DNAT translation should take place. This command is mutually exclusive with the pool command in nat-policy.</p> <p>When DNAT-only is enabled, no source and port NAT (SNAPT) is performed. In other words, only the destination IP address (going from inside to outside) is translated while the source IP address and port are not translated.</p> |

|            |                                                                                                                                                                                           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default    | none                                                                                                                                                                                      |
| Parameters | <b>router</b> <i>router-instance</i> — Specifies the routing context on the outside (public side).<br><b>nat-group</b> <i>nat-group-id</i> — Specifies the NAT group IP.<br>Values 1 to 4 |

dnat-only

|             |                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------|
| Syntax      | <b>dnat-only</b>                                                                                      |
| Context     | config>router>nat>inside<br>config>service>vprn>nat>inside                                            |
| Description | This command enables the context on the NAT inside context where dnat-only parameters are configured. |

source-prefix-list

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>source-prefix-list</b> <i>prefix-list-name</i><br><b>no source-prefix-list</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Context     | config>service>vprn>nat>inside<br>config>router>nat>inside                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Description | <p>This command references the <b>nat-prefix-list</b> that contains source IP addresses on the inside (private side).</p> <p>The source IP addresses on the inside must be known in advance in a <b>dnat-only</b> instance. This is required so the corresponding routes can be installed in the routing table and thus the downstream traffic is properly routed towards the MS-ISAs where the original translation was performed (and state is kept).</p> <p>In the <b>dnat-only</b> case, it is mandatory that the inside (private side) and the outside (public side) are in separated VPRNs.</p> |
| Default     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Parameters  | <i>prefix-list-name</i> — Specifies the name, up to 32 characters in length, of the NAT prefix list that contains the source IP addresses (original IP addresses).                                                                                                                                                                                                                                                                                                                                                                                                                                    |

route-limit

|         |                                                                                  |
|---------|----------------------------------------------------------------------------------|
| Syntax  | <b>route-limit</b> [1..131072]                                                   |
| Context | config>router>nat>outside>dnat-only<br>config>service>vprn>nat>outside>dnat-only |

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command limits the number of source routes (inside routes) that are installed on the outside in <b>dnat-only</b> case. In case that the number of actual routes is larger than the number of configured routes, the excess of the routes will not be installed in the routing table and a log will be raised.</p> <p>The source IP addresses on the inside must be known in advance in a <b>dnat-only</b> instance. This is required so that the corresponding routes can be installed in the routing table and thus the downstream traffic is properly routed towards the MS-ISAs where the original translation was performed (and state is kept).</p> <p>In the dnat-only case, it is mandatory that the inside (private side) and the outside (public side) are in separated VPRNs.</p> |
| <b>Default</b>     | route-limit 32768                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Parameters</b>  | 1..131072 — Specifies the maximum number of source routes installed on the outside the <b>dnat-only</b> scenario.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## classic-lsn-max-subscriber-limit

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>classic-lsn-max-subscriber-limit</b> <i>max</i><br><b>no classic-lsn-max-subscriber-limit</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Context</b>     | config>router>nat>inside<br>config>service>vprn>nat>inside                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>This command sets the granularity of traffic distribution in the upstream direction across the MS-ISA within the scope of an inside routing context. Traffic distribution mechanism is based on the source IPv4 addresses/prefixes. More granular distribution is based on the IPv4 address, while distribution based on the IPv4 prefix (determined by prefix length) will be less granular. The granularity will further decrease with shorter prefix length.</p> <p>For example, a prefix length of 32 will distribute individual /32 IPv4 addresses over multiple MS-ISAs in an ISA group. This will ensure better traffic load balancing at the expense of forwarding table utilization on the outside (public side) where each /32 is installed in the forwarding table. On the contrary, shorter prefixes will ensure better utilization of the forwarding table on the outside, at the expense of coarser spread of IP addresses over multiple MS-ISAs.</p> <p>This command affects all flavors of LSN44 within the inside routing contexts, although its primary use is intended for deterministic NAT and dnat-only.</p> <p>The length of the prefix that is used for distribution purposes is <math>(32-n)</math>, where <math>2^n = \text{classic-lsn-max-subscriber-limit}</math>. For example, if traffic distribution is based on the IPv4 address (prefix length = 32), then <math>n</math> must be 0. From here, it follows that classic-lsn-max-subscriber-limit must be set to 1:</p> <p>Prefix length = 32 -&gt; <math>32-n = 32</math> -&gt; <math>n=0</math> -&gt; <math>2^0 = 1 = \text{classic-lsn-max-subscriber-limit}</math></p> |

The implicit method given by this command uses power of 2 calculations to provide prefix length for traffic distribution purposes. This roundabout approach to determine the prefix-length has roots in deterministic NAT where this command was originally introduced.

Even though deterministic NAT and dnat-only have very little in common, the method (and CLI syntax) for calculating the prefix length using the classic-lsn-max-subscriber-limit parameter for traffic distribution purposes is shared between the two. In dnat-only, this parameter is important from an operational perspective since it affects traffic load balancing over MS-ISA and the size of the routing table.

This command must be configured before any prefix is configured and can be modified only if there are no prefixes configured under the deterministic NAT.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b> | <p><b>max</b> — The power of 2 (<math>2^n</math>) value which in deterministic NAT must match the largest subscriber-limit value in any deterministic pool referenced from this inside routing instance.</p> <p>In <b>dnat-only</b>, this value can be set to any value from the allowed range.</p> <p>In both cases, this value will determine the prefix-length (17-32) that will directly influence load distribution between the MS-ISAs and the size of the routing table.</p> <p><b>Values</b> 1,2,4,8 to 32768</p> |

## nat-classifier

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-classifier</b> <i>nat-classifier-name</i><br><b>no nat-classifier</b>                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>service>nat>nat-policy>dnat                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | <p>This command when configured within the nat-policy, references a nat-classifier and consequently activates DNAT functionality. Unless this command is provisioned, the destination IP address translation will not take place.</p> <p>The <b>nat-classifier</b> identifies the traffic (in a filter-like fashion) that is subjected to DNAT.</p> <p>The <b>no</b> form of the command removes the <i>nat-classifier-name</i> from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>nat-classifier-name</i> — Specifies the name, up to 32 characters, of the NAT classifier.                                                                                                                                                                                                                                                                                                                                                                |

## nat-classifier

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>nat-classifier</b> <i>nat-classifier-name</i> [create]<br><b>no nat-classifier</b> |
|---------------|---------------------------------------------------------------------------------------|

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>service>nat                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>This command creates a nat-classifier. Traffic can be identified in nat-classifier based on the protocol type and destination ports. Once the traffic is identified, an action associated with identified traffic, such as destination NAT (DNAT), can be taken.</p> <p>The <b>no</b> form of the command removes the <i>nat-classifier-name</i> from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <p><i>nat-classifier-name</i> — Specifies the name, up to 32 characters, of the referenced NAT classifier.</p> <p><b>create</b> — Keyword used to create the NAT classifier.</p>                                                                                                                                                                                                |

## nat-prefix-list

|                    |                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-prefix-list</b> <i>name</i><br><b>no nat-prefix-list</b> <i>name</i>                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>subscrib-mgmt>sub-profile                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command specifies the nat-prefix-list referenced within the subscriber-profile is used to associate L2-aware subscriber traffic with additional nat-policies based on the destination IPv4 address of the traffic.</p> <p>The <b>no</b> form of the command removes the prefix list name from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                         |
| <b>Parameters</b>  | <i>name</i> — Specifies the nat prefix list name. Allowed values are any string up to 32 characters long composed of printable,7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.                                             |

## nat-prefix-list

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-prefix-list</b> <i>name</i> [ <b>create</b> ] [ <b>application</b> <i>application-choice</i> ]<br><b>no nat-prefix-list</b> <i>name</i>                                                                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>service>nat                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | <p>This command is used to create configuration context for:</p> <ul style="list-style-type: none"><li>• IP prefixes that are used select multiple nat-policies per subscriber in L2-aware NAT.</li><li>• Inside IP prefixes in DNAT-only scenario. The inside IP prefixes are then setup as downstream routes used to steer the return (downstream) traffic to the proper MS-ISA.</li></ul> <p>The <b>no</b> form of the command removes the prefix list name from the configuration.</p> |



|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b> | <p><i>name</i> — Specifies the nat prefix list name. Allowed values are any string up to 32 characters long composed of printable,7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p><b>application</b> <i>application-choice</i> — Specifies how this NAT prefix list is to be applied.</p> <p><b>Values</b></p> <p><b>I2-aware-dest-to-policy:</b> Specifies that the nat-prefix-list can be applied only within the sub-profile for I2-aware subscribers. It will contain mapping between the destination prefix and a nat-policy.</p> <p><b>dnat-only-subscribers:</b> Specifies that the nat-prefix-list can be applied only to dnat-only-subscribers. It will contain the source-prefix that needs to be install in outside routing context so that the return traffic from the outside can be directed to proper MS-ISA.</p> |

## prefix

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <p><b>prefix</b> <i>ip-prefix/length</i> [<b>nat-policy</b> <i>nat-policy-name</i>]</p> <p><b>no prefix</b> <i>ip-prefix/length</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>service>nat>nat-prefix-list                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command creates a prefix entry in the nat-prefix-list.</p> <p>This prefix can be used to identify traffic with specific destination IP that needs to be associated with corresponding nat-policy (and implicitly the NAT pool) for L2-aware subscribers. In this fashion, a single L2-aware subscriber can direct traffic to multiple NAT pools, depending on the traffic destination.</p> <p>Another use for a prefix is in DNAT-only application (DNAT without SNAPT). In this case the prefix identifies the inside source IP range that will be explicitly configured to ensure proper downstream routing in dNAT-only case.</p> <p>The nat-prefix-list cannot reference the default nat-policy (the one that is referenced in the subscriber-profile).</p> <p>The <b>no</b> form of the command reverts to the default.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <p><i>ip-prefix/length</i> — Specifies the IP prefix for nat prefix list entry in dotted decimal notation.</p> <p><b>Values</b></p> <p><i>ip-prefix:</i> a.b.c.d (host bits must be 0) <i>ipv4-prefix-length:</i> 0 to 32</p> <p><b>nat-policy</b> <i>nat-policy-name</i> — Specifies the NAT policy name. Allowed values are any string up to 32 characters composed of printable,7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes..</p>                                                                                                                                                                                                                                                                                                |

---

## default-dnat-ip-address

|                    |                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-dnat-ip-address</b> <i>ip-address</i><br><b>no default-dnat-ip-address</b>                                                                                                                                                                                |
| <b>Context</b>     | config>service>nat>nat-classifier                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command configures default destination ip address for action DNAT in cases where the destination ip address is not explicitly stated as part of the action or default-action statement.</p> <p>The <b>no</b> form of the command reverts to the default.</p> |
| <b>Default</b>     | no default-dnat-ip-address                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>ip-address</i> — Specifies the IPv4 address in dotted decimal notation.                                                                                                                                                                                           |

## entry

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>entry</b> <i>entry-id</i> [ <b>create</b> ]<br><b>no entry</b> <i>entry-id</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>service>nat>nat-classifier                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>This command creates or edits a nat-classifier entry. Multiple entries can be created using unique entry-id numbers within the nat-classifier. Entries must be sequenced from most to least explicit. An entry may not have any match criteria defined, in which case all UDP traffic will be matched. In case that the action is not explicitly configured, a default-action will be applied.</p> <p>The <b>no</b> form of the command removes the specified entry from the filter. Entries removed from the nat-classifier are immediately removed from all entities to which the nat-classifier is applied.</p> |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <i>entry-id</i> — Specifies an entry-id that uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given entry-ids in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.                                                                                                                                                                                                                                                                                          |
| <b>Values</b>      | 1 to 1000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## match

|                |                                                             |
|----------------|-------------------------------------------------------------|
| <b>Syntax</b>  | <b>match protocol</b> <i>ip-protocol</i><br><b>no match</b> |
| <b>Context</b> | config>service>nat>nat-classifier>entry                     |

|                    |                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | This command configures an IP protocol to be used as a nat-classifier match criterion. When the match criteria have been satisfied the action associated with the match criteria is executed.<br><br>The <b>no</b> form of the command removes the match criteria for the entry-id. |
| <b>Default</b>     | match protocol udp                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <b>protocol</b> <i>ip-protocol</i> — Specifies the text value representing the IP protocol to be used as a match criterion.<br><br><b>Values</b> udp, tcp                                                                                                                           |

## dst-port-range

|                    |                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>dst-port-range start</b> <i>port-number</i> <b>end</b> <i>port-number</i><br><b>no dst-port-range</b>                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>service>nat>nat-classifier>entry>match                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | This command configures a destination TCP or UDP port number or port range.<br><br>Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd,etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.<br><br>The <b>no</b> form of the command removes the destination port match criterion. |
| <b>Default</b>     | dst-port-range start 0 end 65535                                                                                                                                                                                                                                                                                                                                          |
| <b>Parameters</b>  | <b>start</b> <i>port-number</i> — Specifies the start of the port range expressed as a decimal integer.<br><b>Values</b> 0 to 65535<br><b>end</b> <i>port-number</i> — Specifies the end of the port range expressed as a decimal integer.<br><b>Values</b> 0 to 65535                                                                                                    |

## action

|                    |                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>action {dnat forward} [ip-address <i>ip-address</i>]</b><br><b>no action</b>                                                                                              |
| <b>Context</b>     | config>service>nat>nat-classifier>entry                                                                                                                                      |
| <b>Description</b> | This command specifies the action to take for packets that match this nat-classifier entry.<br><br>The <b>no</b> form of the command removes the specified action statement. |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default</b>    | no action. This means that this entry is ignored (skipped). Consequently, the action from another matching entry will be applied. If there are no other matching entries found, the default-action will be applied.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b> | <p><b>dnat</b> — Performs the DNAT function. The destination IP address of the packet traversing the router in the direction from inside to outside is replaced by the configured IP address. Destination port is not translated. In the opposite direction (from outside to inside), the source address in the returning packet is restored to the original value.</p> <p><b>forward</b> — The forward action will ensure that the packet is transparently passed through the nat-classifier.</p> <p><b>ip-address</b> <i>ip-address</i> — The destination IP address that will replace the original IP address in the packet traveling from inside to outside.</p> |

default-action

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-action {dnat forward} [ip-address <i>ip-address</i>]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Context</b>     | config>service>nat>nat-classifier                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p>This command specifies the default action to take for packets in this nat-classifier. The default-action will apply to packet that do not match any configured criteria within nat-classifier.</p> <p>The <b>no</b> form of this command equals action forward.</p>                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Default</b>     | default-action forward                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><b>dnat</b> — Performs the DNAT function. The destination IP address of the packet traversing the router in the direction from inside to outside is replaced by the configured IP address. Destination port is not translated. In the opposite direction (from outside to inside), the source address in the returning packet is restored to the original value.</p> <p><b>forward</b> — The forward action will ensure that the packet is transparently passed through the nat-classifier.</p> <p><b>ip-address</b> <i>ip-address</i> — The destination IP address that will replace the original IP address in the packet traveling from inside to outside.</p> |

default-dnat-ip-address

|                    |                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>default-dnat-ip-address <i>ip-address</i></b><br><b>no default-dnat-ip-address</b>              |
| <b>Context</b>     | config>service>nat>nat-classifier                                                                  |
| <b>Description</b> | This command configures the IP address to substitute for the destination IP address of the packets |

|            |                                                            |
|------------|------------------------------------------------------------|
| Default    | no default-dnat-ip-address                                 |
| Parameters | <i>ip-address</i> — Specifies the default DNAP IP address. |

### 7.25.2.12 NAT MAP-T Commands



**Note:** The MAP-T CLI commands described in this section apply to the Nokia Virtualized Service Router (VSR) only.

#### map-domain

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>map-domain</b> <i>domain-name</i> [create]<br><b>no map-domain</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Context     | config>service>nat                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Description | <p>This command creates a MAP domain template, which is used to define MAP rules and parameters specific to the MAP domain. A MAP domain represents a set of CEs that share the same default gateway (BR's IPv6 prefix - DMR rule) and a set of basic MAP rules (BMRs). As a bordering node between the IPv6 and IPv4 realm, the BR performs stateless IPv4 and IPv6 translation based on MAP rules.</p> <p>A MAP domain can be instantiated within a routing context by referencing an existing MAP domain template in the context.</p> |
| Parameters  | <i>domain-name</i> — Specifies the name of the MAP domain, up to 32 characters. The MAP domain name has local significance.                                                                                                                                                                                                                                                                                                                                                                                                              |

#### dmr-prefix

|             |                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>dmr-prefix</b> <i>dmr-prefix</i><br><b>no dmr-prefix</b>                                                                                                                        |
| Context     | config>service>nat>map-domain                                                                                                                                                      |
| Description | <p>This command configures the IPv6 prefix of the BR (dmr-prefix), which is used as a default MAP rule (route) in the CEs. Each MAP domain in the VSR has a unique dmr-prefix.</p> |
| Parameters  | <i>dmr-prefix</i> — Specifies the IPv6 prefix associated with a MAP domain in the BR. The prefix represents a dmr-rule in the CE.                                                  |
| Values      | <i>&lt;ipv6-prefix/prefix-length&gt;</i> :<br><i>ipv6-prefix</i> — <i>x:x:x:x:x:x:x</i> (eight 16-bit pieces)                                                                      |

*x:x:x:x:x:d.d.d.d*  
*x*—[0 to FFFF]H  
*d*—[0 to 255]D  
*prefix-length*—[0 to 96]

v6-frag-header

|             |                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | [no] v6-frag-header                                                                                                                                                                                                                            |
| Context     | config>service>nat>map-domain>ip-fragmentation                                                                                                                                                                                                 |
| Description | This command enables and disables the insertion of the fragmentation header in an IPv6 packet when translating non-fragmented IPv4 packet with DF=0. This option is disabled by default and the size of the IPv6 packet is reduced by 8 bytes. |
| Default     | no v6-frag-header                                                                                                                                                                                                                              |

mapping-rule

|             |                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------|
| Syntax      | mapping-rule <i>map-rule-name</i> [create]<br>no mapping-rule <i>map-rule-name</i>            |
| Context     | config>service>nat>map-domain                                                                 |
| Description | This command provides a CLI context for configuring MAP rules.                                |
| Parameters  | <i>map-rule-name</i> — Specifies the name of the MAP rule; the name has a local significance. |

ea-length

|             |                                                                                                                                  |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | ea-length <i>ea-bits-length</i><br>no ea-length                                                                                  |
| Context     | config>service>nat>map-domain>mapping-rule                                                                                       |
| Description | This command configures the length of EA bits in the MAP rule. The <b>no ea-length</b> statement sets the <b>ea-length</b> to 0. |
| Default     | no ea-length                                                                                                                     |
| Parameters  | <i>ea-bits-length</i> — Specifies the length of the EA bits.<br>Values 1 to 48                                                   |

## ipv4-prefix

|                    |                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ipv4-prefix</b> <i>ipv4-prefix</i><br><b>no ipv4-prefix</b>                                                                                                                                                                 |
| <b>Context</b>     | config>service>nat>map-domain>mapping-rule                                                                                                                                                                                     |
| <b>Description</b> | This command configures an IPv4 MAP rule prefix.                                                                                                                                                                               |
| <b>Parameters</b>  | <i>ipv4-prefix</i> — Specifies the IPv4 MAP prefix.<br><b>Values</b> < <i>ipv4-prefix</i> >/< <i>ipv4-prefix-length</i> ><br>< <i>ipv4-prefix</i> > : a.b.c.d (host bits must be 0)<br>< <i>ipv4-prefix-length</i> > : [0..32] |

## psid-offset

|                    |                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>psid-offset</b> <i>psid-offset-length</i><br><b>no psid-offset</b>                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>service>nat>map-domain>mapping-rule                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | This command configures the length of the high order bits in the protocol port field whose aggregate value should always be greater than 0. This automatically excludes certain ports (such as well-known ports) from the translation.<br><br>It is a function of the CE to make sure that the psid-offset bits are always greater than 0. The VSR does not check whether those bits are 0. |
| <b>Default</b>     | psid-offset 6                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <i>psid-offset-length</i> — Specifies the length of the psid-offset bits in the protocol port field.<br><b>Values</b> 0 to 16                                                                                                                                                                                                                                                               |

## rule-prefix

|                    |                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>rule-prefix</b> <i>rule-prefix</i><br><b>no rule-prefix</b>                                                                                                               |
| <b>Context</b>     | config>service>nat>map-domain>mapping-rule                                                                                                                                   |
| <b>Description</b> | This command configures a MAP rule prefix.                                                                                                                                   |
| <b>Parameters</b>  | <i>rule-prefix</i> — Specifies the IPv6 MAP rule prefix.<br><b>Values</b> < <i>ipv6-prefix/prefix-length</i> > :<br><i>ipv6-prefix</i> — x:x:x:x:x:x:x (eight 16-bit pieces) |

*x:x:x:x:x:d.d.d.d*  
x—[0 to FFFF]H  
d—[0 to 255]D  
*prefix-length*—[0 to 64]

shutdown

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | [no] shutdown                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Context     | config>service>nat>map-domain>mapping-rule                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Description | <p>This command enables or disables a rule within a MAP domain. A MAP rule can be enabled (<b>no shutdown</b>) only when all parameters within the rule are defined. Disabling a rule within an instantiated MAP domain will withdraw the rule IPv4 routes and disable forwarding for the rule.</p> <p><b>Interactions:</b></p> <p>configure&gt;service&gt;vpn&gt;nat&gt;map&gt;map-domain <i>domain-name</i></p> <p>configure&gt;service&gt;router&gt;nat&gt;map&gt;map-domain <i>domain-name</i></p> <p>Shutdown of an instantiated MAP rule disables the rule (the rule routes will be withdrawn and forwarding will be disabled).</p> |
| Default     | shutdown                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

mtu

|             |                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | mtu <i>mtu-size</i><br>no mtu                                                                                                                                                                                                                                         |
| Context     | config>service>nat>map-domain                                                                                                                                                                                                                                         |
| Description | <p>This command configures the IPv6 MTU in a MAP domain. The configured MTU applies to traffic in the downstream direction, towards the CE. The configured MTU value must be lower than the MTU of the outgoing port for the traffic, which includes L2 overhead.</p> |
| Default     | mtu 8686                                                                                                                                                                                                                                                              |
| Parameters  | <p><i>mtu-size</i> — Specifies the IPMTU size of the translated IPv6 packet.</p> <p><b>Values</b>      160 to 8686</p>                                                                                                                                                |



---

## shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Context</b>     | config>service>nat>map-domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | <p>This command enables or disables a MAP domain. A MAP domain can be enabled (<b>no shutdown</b>) only when the DMR prefix is configured. Disabling an instantiated domain will withdraw all routes associated with it.</p> <p><b>Interactions:</b></p> <p>configure&gt;service&gt;vprn&gt;nat&gt;map&gt;map-domain <i>domain-name</i></p> <p>configure&gt;service&gt;router&gt;nat&gt;map&gt;map-domain <i>domain-name</i></p> <p>Shutdown of a MAP domain template disables the instantiated MAP domain (the routes will be withdrawn and forwarding will be disabled).</p> |
| <b>Default</b>     | shutdown                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## tcp-mss-adjust

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>tcp-mss-adjust segment-size</b><br><b>no tcp-mss-adjust</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>service>nat>map-domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command enables the TCP maximum segment size (MSS) adjustments in a MAP domain. The TCP SYN and SYN-ACK packets are intercepted in both directions, and if their MSS value is larger than the one configured using this command, the MSS value in the packet is re-written (lowered) to the configured value. The end hosts use the lowest setting of the two hosts. The MSS value does not account for the IP or TCP header length.</p> <p>If the MSS value in the SYN or SYN-ACK is not found, a new value is added and set to the configured value.</p> |
| <b>Default</b>     | no tcp-mss-adjust                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Parameters</b>  | <p><i>segment-size</i> — Specifies the maximum size of the segment.</p> <p><b>Values</b> 160 to 8626</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## map-domain

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| <b>Syntax</b>  | <b>map-domain domain-name</b><br><b>no map-domain domain-name</b> |
| <b>Context</b> | config>service>vprn>nat>map                                       |

config>router>nat>map

**Description** This command instantiates a MAP-T domain within a routing context, assuming that the MAP-T domain template is administratively enabled (**no shutdown**). When the MAP-T is instantiated, the forwarding for the MAP-T domain is enabled and its routes can be exported in routing protocols.

Multiple MAP-T domains can be instantiated within a routing context.

**Interactions:**

The referenced MAP domain is defined under the **configure>service>nat** hierarchy.

**Parameters** *domain-name* — Specifies the name of the MAP domain template, up to 32 characters.

7.25.2.13 NAT Filter Commands

action

**Syntax** **action** [**secondary**] **nat** [**nat-policy-name** *nat-policy-name*]  
**no action** [**secondary**]

**Context** config>filter>ip-filter>entry

**Description** This command specifies packets matching the entry criteria will be subject to large-scale NAT.

**Default** no action

**Parameters** **nat** — Specifies that traffic matching the specified criteria will be diverted to NAT.  
*nat-policy-name* — Specifies the NAT policy to be used.

action

**Syntax** **action** [**secondary**] **nat nat-type** *nat-type* [**nat-policy-name** *nat-policy-name*]  
**no action** [**secondary**]

**Context** config>filter>ipv6-filter>entry

**Description** This command specifies packets matching the entry criteria will be subject to large-scale NAT.

**Default** no action

**Parameters** **nat** — Specifies that traffic matching the specified criteria will be diverted to NAT.

*nat-policy-name* — Specifies the NAT policy to be used.

*nat-type* — Specifies the NAT type.

**Values**      dslite, nat64

### 7.25.2.14    Residential Firewall Commands

#### firewall-policy

|                    |                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>firewall-policy</b> <i>policy-name</i><br><b>no firewall-policy</b>                                                                                                                                    |
| <b>Context</b>     | config>subscr-mgmt>sub-prof                                                                                                                                                                               |
| <b>Description</b> | This command enables the IPv6 firewall for this subscriber profile using the specified firewall policy.<br><br>The <b>no</b> form of this command disables the IPv6 firewall for this subscriber profile. |
| <b>Default</b>     | no firewall-policy                                                                                                                                                                                        |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies the name of the firewall policy, up to 32 characters maximum.                                                                                                              |

#### firewall

|                    |                                                                    |
|--------------------|--------------------------------------------------------------------|
| <b>Syntax</b>      | <b>firewall</b>                                                    |
| <b>Context</b>     | config>router<br>config>service>vprn                               |
| <b>Description</b> | This command enables the context to configure firewall parameters. |

#### domain

|                    |                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>domain</b> <i>domain-name</i> [ <b>nat-group</b> <i>nat-group-id</i> ] [ <b>create</b> ]<br><b>no domain</b> <i>domain-name</i>                                                                                        |
| <b>Context</b>     | config>router>firewall<br>config>service>vprn>firewall                                                                                                                                                                    |
| <b>Description</b> | This command configures a domain to contain firewall parameters. Each domain must be assigned to a NAT group where firewall functionality will be performed.<br><br>The <b>no</b> form of the command removes the domain. |

---

|                   |                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <b>create</b> — Mandatory keyword used when creating the domain.<br><i>domain-name</i> — Specifies the name of the domain, up to 32 characters maximum.<br><i>nat-group-id</i> — Specifies the ID of the NAT group where the firewall functionality will be performed.<br><b>Values</b> 1 to 4 |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## prefix

|                    |                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>prefix</b> <i>prefix/prefix-length</i> [ <b>create</b> ]<br><b>no prefix</b> <i>prefix/prefix-length</i>                                                                                                                                                                                                            |
| <b>Context</b>     | config>router>firewall>domain<br>config>service>vpn>firewall>domain                                                                                                                                                                                                                                                    |
| <b>Description</b> | This command specifies a prefix for which firewall functionality will apply within the domain. Prefixes cannot be shared or duplicated across multiple domains in the same routing context. A domain can contain multiple prefixes.<br><br>The <b>no</b> form of the command removes the prefix from the domain.       |
| <b>Parameters</b>  | <b>create</b> — Mandatory keyword used when creating a prefix entry.<br><i>prefix/prefix-length</i> — Specifies the prefix.<br><b>Values</b> <i>prefix</i> — x:x:x:x:x:x:x (eight 16-bit pieces)<br>x:x:x:x:x:d.d.d.d<br>x — 0 to FFFF (in hexadecimal)<br>d — 0 to 255 (in decimal)<br><i>prefix-length</i> — 1 to 64 |

## firewall-policy

|                    |                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>firewall-policy</b> <i>name</i> [ <b>create</b> ]<br><b>no firewall-policy</b>                                                                                                                                                                            |
| <b>Context</b>     | config>service>nat                                                                                                                                                                                                                                           |
| <b>Description</b> | This command configures a firewall policy that can be used in contexts where basic protection from outside attack vectors is required.<br><br>The <b>no</b> form of the command removes the policy, and can only be performed when the policy is not in use. |
| <b>Default</b>     | no firewall-policy                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <b>create</b> — Mandatory keyword used when creating a firewall policy.                                                                                                                                                                                      |

---

*name* — Specifies the name of the firewall policy, up to 32 characters maximum.

## domain

|                    |                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>domain router <i>router-name</i> name <i>domain-name</i></b><br><b>no domain</b>                                                                                                                                                                                                                                                                                                              |
| <b>Context</b>     | config>service>nat>firewall-policy                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | <p>This command specifies a router and domain to which the firewall policy will be applied. All associated traffic must be part of the prefixes specified by this domain.</p> <p>The <b>no</b> form of the command removes the domain association from the firewall policy.</p>                                                                                                                  |
| <b>Default</b>     | no domain                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Parameters</b>  | <p><i>domain-name</i> — Specifies the name of the firewall domain in the specified router instance. 32 characters maximum.</p> <p><i>router-name</i> — Specifies the name of the router instance to use.</p> <p><b>Values</b>     <i>router-name</i>   <i>vprn-svc-id</i><br/>              <i>router-name</i> — “Base”, “management”<br/>              <i>vprn-svc-id</i> — 1 to 2147483647</p> |

## 7.25.2.15 NAT Show Commands

### nat-accounting-policy

|                    |                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-accounting-policy</b><br><b>nat-accounting-policy <i>policy-name</i></b><br><b>nat-accounting-policy <i>policy-name</i> associations</b><br><b>nat-accounting-policy</b>                                   |
| <b>Context</b>     | show>aaa                                                                                                                                                                                                          |
| <b>Description</b> | This command displays NAT accounting policy information.                                                                                                                                                          |
| <b>Parameters</b>  | <p><i>policy-name</i> — Specifies the NAT policy name up to 32 characters.</p> <p><b>associations</b> — Keyword that displays the router instances and/or subscriber profiles associated with the NAT policy.</p> |
| <b>Output</b>      | The following is an example output for this command.                                                                                                                                                              |

#### Sample Output

```

A:SR12_PPPOE# show aaa nat-accounting-policy "my-acct-plcy"
=====
NAT accounting policy "my-acct-plcy"
=====
Description : my accounting policy

RADIUS accounting server settings

Access algorithm : direct
Retry : 3
Router : 101
Source address start : 10.10.10.10
Source address end : 10.10.10.20
Timeout (s) : 5
Last management change : 01/28/2012 14:47:59
Include attributes : framed-ip-addr nas-identifier nat-subscriber-
 string user-name inside-service-id outside-
 service-id outside-ip port-range-block hardware-
 timestamp release-reason multi-session-id frame-
 counters octet-counters session-time
=====
Servers for "my-acct-plcy"
=====
Index Address Port

1 10.0.0.5 1813
2 10.0.0.1 1813
=====
Servers ISA group connection status for "my-acct-plcy"
=====
Index Group Member State Tx-rq Rq-timeout Send-retry

1 3 1 out-of-service 3 1 2
1 3 2 out-of-service 9 3 6
2 3 1 in-service 1 0 0
2 3 2 out-of-service 6 2 4
=====
A:SR12_PPPOE#

A:SR12_PPPOE# show aaa nat-accounting-policy "my-acct-plcy" associations
=====
NAT groups associated with "my-acct-plcy"
=====
Group

1
3

No. of groups: 2
=====
A:SR12_PPPOE#

```

## nat-group

**Syntax**     **nat-group**  
**nat-group** *nat-group-id* [**associations**]  
**nat-group** *nat-group-id* **mda** *mda-id* **l2-aware-bypass**  
**nat-group** *nat-group-id* **statistics** **mda** *mda-id* [**non-zero-value-only**]  
**nat-group** *nat-group-id* **member** [1..255]  
**nat-group** *nat-group-id* **member** [1..255] **reassembly-statistics** [**non-zero-value-only**]  
**nat-group** *nat-group-id* **member** [1..255] **statistics** [**non-zero-value-only**]  
**nat-group** [*nat-group-id*] **members**

**Context**     show>isa

**Description**     This command lists all used (active) member ISAs (or group members). Up to 16 group members can be displayed (16 is the supported number of LAG links). Members can share physical ISAs (MDAs) and the physical locality of the group members can be determined from the **Mda** column in the output.

The number of group members will be <=X and the actual number of displayed group members will depend on the configuration based calculation.

**Parameters**     *nat-group-id* — Specifies the NAT group ID.

**Values**         1 to 4

**associations** — Displays associations applicable to the specified NAT group.

**statistics** — Displays NAT group statistics.

**member** — Displays statistics information about the resources of a member of a NAT ISA group.

**non-zero-value-only** — Displays statistics information display whose value is bigger than zero.

**reassembly-statistics** — Displays statistics information about IP datagram reassembly on NAT-capable ISA groups.

**Output**         The following shows output examples.

### Sample Output

```
show isa nat-group
=====
ISA NAT Group Summary
=====
Mda Group 1 Group 2 Group 3

3/1 active - -
3/2 - active busy
4/1 - busy active
4/2 - standby standby
=====
```

```
*A:SR12_PPPOE>config>isa>nat-group# show isa nat-group 1
=====
ISA NAT Group 1
=====
Admin state : inService
Operational state : inService
Active MDA limit : 2

NAT specific information for ISA group 1

Reserved sessions : 0
High Watermark (%) : (Not Specified)
Low Watermark (%) : (Not Specified)
Accounting policy : my-acct-plcy
Last Mgmt Change : 01/28/2012 14:47:59

ISA Group 1 members
=====
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio

1 1 active 3/1 3 3 < 1 N 0
1 2 active 3/2 4 4 < 1 N 0

No. of members: 2
=====
A:SR12_PPPOE#
```

```
*A:SR12_PPPOE>config>isa>nat-group# show isa nat-group
=====
ISA NAT Group Summary
=====
Mda Group 1 Group 2 Group 3 Group 4

2/1 - provisioned - -
3/1 active - up -
3/1 active - up -
3/2 active - up -
3/2 active - up -
=====
A:SR12_PPPOE#
```

```
*A:SR12_PPPOE>config>isa>nat-group# show isa nat-group 1
=====
ISA NAT Group 1
=====
Admin state : inService
Operational state : inService
Active MDA limit : 2

NAT specific information for ISA group 1

Reserved sessions : 0
High Watermark (%) : (Not Specified)
Low Watermark (%) : (Not Specified)
```



```

Accounting policy : my-acct-plcy
Last Mgmt Change : 01/28/2012 14:47:59

=====
ISA Group 1 members
=====
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio

1 1 active 3/1 3 3 < 1 N 0
1 2 active 3/2 4 4 < 1 N 0

No. of members: 2
=====
A:SR12_PPPOE#

A:SR12_PPPOE# show isa nat-group 3 member 1 statistics
=====
ISA NAT Group 3 Member 1
=====
no resource : 0
pkt rx on wrong port : 0
unsupported protocol : 0
no host or host group : 0
no ip or port : 0
no matching flow : 3
max flow exceeded : 0
TCP no flow for RST : 0
TCP no flow for FIN : 0
TCP no flow : 0
addr. dep. filtering : 0
ICMP type unsupported : 0
ICMP local unsupported : 0
ICMP checksum error : 0
ICMP embedded checksum error : 0
ICMP unsupported L4 : 0
ICMP too short : 0
ICMP length error : 0
Pkt not IPv4 or IPv6 : 0
Pkt rcv error : 0
Pkt error : 0
IPv4 header checksum violation : 0
IPv4 header malformed : 0
IPv4 malformed packet : 0
IPv4 ttl zero : 0
IPv4 opt /IPv6 ext headers : 0
IPv4 undefined error : 0
IPv6 fragments unsupported : 0
TCP/UDP malformed : 0
TCP/UDP checksum failure : 0
TCP/UDP length error : 0
Pkt send error : 0
no buf to copy pkt : 0
no policy : 0
locked by mgmt core : 0
port range log failed : 0
MTU exceeded : 0
DS Lite unrecognized next hdr : 0
DS Lite unknown AFTR : 0

```

```

too many fragments for IP packet : 0
too many fragmented packets : 0
too many fragment holes : 0
too many frags buffered : 0
fragment list expired : 0
fragment rate too high : 0
flow log failed : 0
no multiple host or subscr. IPs allowed : 0
to local : 1
to local ignored : 0
NAT64 disabled : 0
NAT64 invalid src addr : 0
NAT64 frag has zero checksum : 0
NAT64 v4 has zero checksum : 0
NAT64 ICMP frag unsupported : 0
CPM out of memory : 0
new flow : 1
TCP closed : 1
TCP expired : 0
UDP expired : 0
ICMP expired : 0
ICMP local : 0
found flow : 34
ARPs ignored : 4
Fragments RX L2A : 0
Fragments RX LSN : 0
Fragments RX DSL : 0
Fragments RX OUT : 0
Fragments TX L2A : 0
Fragments TX LSN : 0
Fragments TX DSL : 0
Fragments TX NAT64 : 0
Fragments TX OUT : 0
flow create logged : 0
flow delete logged : 0
flow log pkt tx : 0
=====
A:SR12_PPPOE#

config>isa# show isa nat-group 1 member 1 statistics
=====
ISA NAT Group 1 Member 1
=====
no resource : 0
[eNatFlowNoResource] "no resource",\
->the default, all errors without more specific reason

[eNatFlowWrongPort] "pkt rx on wrong port",\
-> packet came in on wrong port on ISA

[eNatFlowWrongProt] "unsupported protocol",\
-> protocol is not UDMP/TCP/ICMP

[eNatFlowNoHostGrp] "no host or host group",\
-> can not create new host group because out of resources, or
current host group is not usable at the moment (because in a transient
state)

```

```

[eNatFlowNoIpOrPort] "no ip or port",\
 -> no Ip or port range available

[eNatFlowNoMatchingFlow] "no matching flow",\
 -> no matching flow found

[eNatFlowMaxExceeded] "max flow exceeded",\
 -> max flows for subscriber exceeded

[eNatFlowTcpUnexpectedRst] "TCP no flow for RST",\
[eNatFlowTcpUnexpectedFin] "TCP no flow for FIN",\
[eNatFlowTcpUnexpected] "TCP no flow",\
 -> TCP state machine problem

[eNatFlowAddressDependentFiltering] "addr. dep. filtering",\
 -> pkt dropped because of addr. dependent filtering

[eNatFlowUnsupportedICMP] "ICMP type unsupported",\
 -> unsupported icmp type

[eNatFlowUnsupportedLocalICMP] "ICMP local unsupported",\
 -> packet to ip address on ISA is not an echo request

[eNatFlowIcmpChecksumError] "ICMP checksum error",\
 -> ICMP checksum error

[eNatFlowIcmpEmbeddedPktChecksumError] "ICMP embedded checksum
error",\
 -> checksum error on embedded IP header

[eNatFlowIcmpEmbeddedPktUnsupportedL4] "ICMP unsupported L4",\
 -> embedded IP packet is not UDP/TCP

[eNatFlowIcmpTooShort] "ICMP too short",\
 -> packet too short to include the ICMP header

[eNatFlowIcmpLengthError] "ICMP length error",\
 -> packet too short to include the embedded header

[eNatFlowPacketErrorNotIp] "Pkt not IPv4 or IPv6",\
[eNatFlowPacketErrorRecv] "Pkt rcv error",\
[eNatFlowPacketError] "Pkt error",\
[eNatFlowPacketErrorIpv4HdrChk] "IPv4 header checksum
violation",\
[eNatFlowPacketErrorIpv4HdrMal] "IPv4 header malformed",\
[eNatFlowPacketErrorIpv4PktMal] "IPv4 malformed packet",\
[eNatFlowPacketErrorIpv4TtlZero] "IPv4 ttl zero",\
[eNatFlowPacketErrorIpv4Optv6Ext] "IPv4 opt /IPv6 ext headers",\
[eNatFlowPacketErrorIpv4Bad] "IPv4 undefined error", \
[eNatFlowPacketErrorIpv6Frag] "IPv6 fragments unsupported",\
[eNatFlowPacketErrorTcpUdpMal] "TCP/UDP malformed",\
[eNatFlowPacketErrorTcpUdpChk] "TCP/UDP checksum failure",\
[eNatFlowPacketErrorTcpUdpLen] "TCP/UDP length error",\
 -> malformed incoming packet

[eNatFlowPacketSendError] "Pkt send error",\
 -> failed to tx the packet

[eNatFlowPacketNoCpyBuf] "no buf to copy pkt",\

```

```

-> failed to copy the packet to another buffer needed for
correct processing

[eNatFlowLockedByMgmtCore] "locked by mgmt core",\
-> resources temp. locked by the mgmt core

[eNatFlowPRLogFailed] "port range log failed",\
-> port range log failed

[eNatFlowMtuExceeded] "MTU exceeded",\
-> outgoing packet too big for DS-Lite tunnel or nat64 mtu

[eNatFlowDslUnrecNextHdr] "DS Lite unrecognized next
hdr",\
->ipv6 pkt has wrong next header

[eNatFlowDslUnknownAFTR] "DS Lite unknown AFTR",\
-> AFTR address is unrecognised

[eNatFlowTooManyFrgsForIpPkt] "too many fragments for IP
packet",\
[eNatFlowTooManyFragmentedPkts] "too many fragmented
packets",\
[eNatFlowTooManyFragHoles] "too many fragment holes",\
[eNatFlowFragListExpire] "fragment list expired",\
[eNatFlowTooManyFragBufs] "too many frags buffered",\
[eNatFlowFragRateTooHigh] "fragment rate too high",\
-> various fragment problems

[eNatFlowNoPolicy] "no policy",\
->vrf not mapped to a policy

[eNatFlowLogFailed] "flow log failed",\
-> flow logging can not follow the setup rate

[eNatFlowMultiHostOrSubscrIp] "no multiple host or
subscr. IPs allowed",\
->multiple hosts or subscribers on the inside in use without
port translation

[eNatFlowToLocalError] "to local ignored",\
-> radius authentication failure (?)

[eNatFlow64Disabled] "NAT64 disabled",\
-> nat64 was disabled

[eNatFlow64InvalidSource] "NAT64 invalid src addr",\
-> source address matches pref64

[eNatFlow64FragZeroChecksum] "NAT64 frag has zero
checksum",\
-> v4 UDP frag has zero checksum

[eNatFlow64ZeroChecksum] "NAT64 v4 has zero checksum",\
-> v4 UDP has zero checksum, and policy configured to drop

[eNatFlow64FragIcmp] "NAT64 ICMP frag unsupported"\
->v4 fragmented ICMP

```

```
show isa nat-group <nat-group-id> members
ISA Group 1 members
=====
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio

1 1 active 1/2 17 2088 < 1 N 0
1 2 active 1/2 17 2088 < 1 N 0
1 3 bypass 1/2 17 2088 < 1 N 0
1 4 active 2/2 17 2088 < 1 N 0
1 5 active 2/2 17 2088 < 1 N 0

No. of members: 5
=====
```

**Table 51** Member State Descriptions

| State        | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active       | The member is actively serving traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Failed       | The member is in a failed state where forwarding is not possible and L2-aware bypass redundancy mode is disabled. This event is normally associated with an MS-ISA failure.                                                                                                                                                                                                                                                                                                                                                                                 |
| failedBypass | <p>The member is in failed state and the subscribers that it was serving before the failover occurred are in a bypass mode. In a bypass mode, subscribers are normally routed according to the routing table in the inside routing context (as opposed to steered to MS-ISA where NAT is performed). The operator should ensure that the routing leads those subscribers to a centralized CGN node that serve as a backup device.</p> <p>This event is normally associated with an MS-ISA failure while the L2-aware bypass redundancy mode is enabled.</p> |
| activeBypass | The member transitions in this state after a recovery while the L2-aware bypass mode of operation is enabled. Some subscribers that this member was serving before the failover are in bypass mode, while others that came on-line after the restoration are actively being served by this member.                                                                                                                                                                                                                                                          |

## firewall-hosts

**Syntax** `firewall-hosts [subscriber sub-ident] [ip ipv6-address/prefix-length] [mac ieee-address]  
[firewall-policy policy-name] [router router-instance]`

**Context** `show>service>nat`



```
firewall_slaac_0 IPv6 Firewall policy for SLAAC on service Base
firewall_slaac_300 IPv6 Firewall policy for SLAAC on service 300
firewall_slaac_4 IPv6 Firewall policy for SLAAC on service 4

```

No. of firewall policies: 6

```
Node# show service nat firewall-policy "firewall_slaac_4"
```

```
=====
Firewall policy firewall_slaac_4
=====
```

```
Description : IPv6 Firewall policy for SLAAC on
 service 4
Domain : domain_slaac_4
Router : vprn4
Filtering : endpointIndependent
Port forwarding range end : 1023
Session limit : 65535
Reserved sessions : 0
Session usage High Watermark (%) : (Not Specified)
Session usage Low Watermark (%) : (Not Specified)
ALG enabled : ftp
Prioritized forwarding classes : (Not Specified)
Timeout TCP established (s) : 7440
Timeout TCP transitory (s) : 240
Timeout TCP SYN (s) : 15
Timeout TCP TIME-WAIT (s) : 0
Timeout TCP RST (s) : 0
Timeout UDP mapping (s) : 300
Timeout UDP initial (s) : 15
Timeout UDP DNS (s) : 15
Timeout ICMPv6 Query (s) : 60
Timeout SIP Inactive Media (s) : 120
Timeout unknown protocol (s) : 300
UDP inbound refresh : false
TCP MSS Adjust : (Not Specified)
Unknown protocols : (Not Specified)
Last Mgmt Change : 01/23/2017 14:32:27
=====
```

```
Node# show service nat firewall-policy "firewall_slaac_4" associations
```

```
=====
Subscriber profile associations
=====
```

```
Subprof_1

```

No. of subscriber profiles: 1

## I2-aware-hosts

**Syntax** **I2-aware-hosts** [**outside-router** *router-instance*] [**outside-ip** *outside-ip-address*] [**inside-ip-prefix** *ip-prefix/mask*] [**vas-filter** *vas-filter-name*]

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Context     | show>service>nat                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Description | This command displays layer-2 aware NAT hosts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Parameters  | <i>nat-policy-name</i> — Specifies the NAT policy name, up to 32 characters.<br><i>nat-group-id</i> — Specifies the NAT group ID.<br><b>Values</b> 1 to 4<br><i>router-instance</i> — Specifies the router instance.<br><b>Values</b><br>router-name: Base , management<br>service-id: 1 to 2147483647<br>svc-name: A string up to 64 characters in length.<br><br><i>outside-ip-address</i> — Specifies the outside IP address.<br><b>Values</b> a.b.c.d<br><i>sub-ident</i> — Specifies the identifier, up to 32 characters. |
| Output      | The following is sample output for this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Sample Output

```
show service nat l2-aware-hosts
=====
Layer-2-Aware NAT hosts
=====
Inside IP Out-Router Outside IP Subscriber

10.0.0.100 Base 10.81.0.0 Sub001
10.0.0.102 Base 10.81.0.0 Sub001
10.0.0.101 Base 10.81.0.203 Sub002
10.0.0.103 Base 10.81.0.0 Sub003

No. of hosts: 4
=====
```

l2-aware-subscribers

|             |                                                                                                                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>l2-aware-subscribers subscriber sub-ident</b><br><b>l2-aware-subscribers [nat-policy nat-policy-name] [nat-group nat-group-id] [member [1..255]] [outside-router router-instance] [outside-ip outside-ip-address] [firewall-policy policy-name]</b> |
| Context     | show>service>nat                                                                                                                                                                                                                                       |
| Description | This command displays layer-2 aware NAT subscribers.                                                                                                                                                                                                   |
| Parameters  | <i>nat-policy-name</i> — Specifies the NAT policy name, up to 32 characters.                                                                                                                                                                           |



*nat-group-id* — Specifies the NAT group ID.

**Values** 1 to 4

*router-instance* — Specifies the router instance.

**Values**

router-name: Base, management  
service-id: 1 to 2147483647  
svc-name: A string up to 64 characters.

*outside-ip-address* — Specifies the outside IP address.

**Values** a.b.c.d

*sub-ident* — Specifies the identifier, up to 32 characters.

**Output** The following is sample output for this command.

### Sample Output

```
show service nat l2-aware-subscribers
=====
Layer-2-Aware NAT subscribers
=====
Subscriber Policy Group/Member
Outside IP Router Ports

Sub001 outPolicy 1/1
10.81.0.0 Base 32-33
Sub002 outPolicy2 1/1
10.81.0.203 Base 32-41
Sub003 outPolicy 1/1
10.81.0.0 Base 34-35

No. of subscribers: 3
=====

show service nat l2-aware-subscribers subscriber "Sub881"
=====
Layer-2-Aware NAT subscriber Sub001
=====
Policy : outPolicy
ISA NAT group : 1
ISA NAT group member : 1
Outside router : Base
Outside IP : 10.81.0.0
ICMP Port usage (%) : < 1
ICMP Port usage high : false
UDP Port usage (%) : < 1
UDP Port usage high : false
TCP Port usage (%) : < 1
TCP Port usage high : false
Session usage (%) : < 1
Session usage high : false
Number of sessions : 0
```

```
Number of reserved sessions : 0
Ports : 32-33
=====
```

## nat-policy

|                    |                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-policy</b> <i>nat-policy-name</i> <b>associations</b><br><b>nat-policy</b> <i>nat-policy-name</i><br><b>nat-policy</b> <i>nat-policy-name</i> <b>statistics</b><br><b>nat-policy</b>                                                                                                       |
| <b>Context</b>     | show>service>nat                                                                                                                                                                                                                                                                                  |
| <b>Description</b> | This command displays NAT policy information.                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <i>nat-policy-name</i> — Specifies the NAT Policy name.<br><b>Values</b> 32 chars max<br><b>associations</b> — Keyword; displays the router instances and/or subscriber profiles associated with the NAT policy.<br><b>statistics</b> — Keyword; displays statistics of the specified NAT policy. |
| <b>Output</b>      | The following is sample output for this command.                                                                                                                                                                                                                                                  |

### Sample Output

```
show service nat nat-policy
=====
NAT policies
=====
Policy Description

outPolicy
outPolicy2
outPolicy3

No. of NAT policies: 3
=====

*A:SR12_PPPOE>show>router>nat# show service nat nat-policy "priv-nat-policy"
=====
NAT Policy priv-nat-policy
=====
Pool : privpool
Router : Base
Filtering : endpointIndependent
Block limit : 4
Reserved ports : 0
Port usage High Watermark (%) : (Not Specified)
Port usage Low Watermark (%) : (Not Specified)
Port forwarding limit : 64
```

```

Session limit : 65535
Reserved sessions : 0
Session usage High Watermark (%) : (Not Specified)
Session usage Low Watermark (%) : (Not Specified)
ALG enabled : ftp rtsp sip
Prioritized forwarding classes : (Not Specified)
Timeout TCP established (s) : 7440
Timeout TCP transitory (s) : 240
Timeout TCP SYN (s) : 15
Timeout TCP TIME-WAIT (s) : 0
Timeout UDP mapping (s) : 300
Timeout UDP initial (s) : 15
Timeout UDP DNS (s) : 15
Timeout ICMP Query (s) : 60
Timeout SIP Inactive Media (s) : 120
Subscriber retention (s) : 0
UDP inbound refresh : false
TCP MSS Adjust : (Not Specified)
Destination-NAT IP : (Not Specified)
IPFIX export policy : (Not Specified)
Last Mgmt Change : 01/28/2012 14:47:59
=====

```

\*A:SR12\_PPPOE>show>router>nat#

```
show service nat nat-policy "outPolicy2" associations
```

```
=====
NAT Policy outPolicy2 Subscriber Profile Associations
=====
```

```
sub_prof_B_3

```

```
No. of subscriber profiles: 1
=====
```

```
show service nat nat-policy "outPolicy2" statistics
```

```
=====
NAT Policy outPolicy2 Statistics
=====
```

```
mda 3/1

```

```

hostsActive : 1
hostsPeak : 1
sessionsTcpCreated : 0
sessionsTcpDestroyed : 0
sessionsUdpCreated : 0
sessionsUdpDestroyed : 0
sessionsIcmpQueryCreated : 0
sessionsIcmpQueryDestroyed : 0
=====

```

## firewall

**Syntax**    **firewall**

**Context**   **show>router**

**Description** This command enables the context to configure commands to display firewall information.

## domain

**Syntax** **domain** [*domain-name*]

**Context** show>router>firewall

**Description** This command lists an overview of all firewall domains that are provisioned in the routing instance.

Configuring the *domain-name* parameter will display operational details for the specified firewall domain.

**Parameters** *domain-name* — Specifies the name of a firewall domain, up to 32 characters maximum.

**Output** The following output is an example of firewall domain information.

### Sample Output

```
Node# show router 4 firewall domain
=====
Firewall domains
=====
Domain NAT-group Admin-state

demo_domain_01 1 in-service
domain_slaac_4 1 in-service

No. of firewall domains: 2
=====

Node# show router 4 firewall domain "domain_slaac_4"
=====
Firewall domain "domain_slaac_4"
=====
ISA group : 1
Administrative state : in-service
Last management change : 01/23/2017 10:47:24
=====
Firewall domain prefixes
=====
Prefix Description

2001:db8:5ffe::/32 (Not Specified)

No. of prefixes: 1
=====
```

## summary

|                    |                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>summary</b>                                                                                           |
| <b>Context</b>     | show>router>firewall                                                                                     |
| <b>Description</b> | This command displays a simple overview of all firewall configurations specific to the routing instance. |
| <b>Output</b>      | The following output is an example of summary firewall information.                                      |

### Sample Output

```
Node# show router 4 firewall summary
=====
Firewall policies
=====
Policy : firewall_dhcp6_4

Domain : domain_dhcp6_4
ISA group : 1
Administrative state : in-service
Policy : firewall_slaac_4

Domain : domain_slaac_4
ISA group : 1
Administrative state : in-service

No. of policies: 2
=====
```

## pcp-server-policy

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>pcp-server-policy</b><br><b>pcp-server-policy <i>name</i></b> |
| <b>Context</b>     | show>router>nat                                                  |
| <b>Description</b> | This command displays PCP server policy information.             |

## port-forwarding-entries

|                    |                                                  |
|--------------------|--------------------------------------------------|
| <b>Syntax</b>      | <b>port-forwarding-entries</b>                   |
| <b>Context</b>     | show>service>nat                                 |
| <b>Description</b> | This command displays port forwarding entries.   |
| <b>Output</b>      | The following is sample output for this command. |

**Sample Output**

```

*A:SR12_PPPOE# show service nat port-forwarding-entries
=====
NAT port forwarding entries
=====
Subscriber
iRtr iAddress prot iPort type
oRtr oAddress persist-id oPort expiry
=====
100 10.2.3.4 tcp 666 classic-lsn-sub
Base 10.0.0.6 N/A 666 N/A
100 10.2.3.4 udp 666 classic-lsn-sub
Base 10.0.0.6 N/A 666 N/A

No. of entries: 2
=====
*A:SR12_PPPOE#

```

**syslog-export-policy**

|                    |                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>syslog-export-policy</b> <i>name</i> <b>associations</b><br><b>syslog-export-policy</b> <i>name</i><br><b>syslog-export-policy</b>                                   |
| <b>Context</b>     | show>service>nat>syslog                                                                                                                                                 |
| <b>Description</b> | This command displays information about syslog export policies.                                                                                                         |
| <b>Parameters</b>  | <i>name</i> — Displays information about the specified NAT syslog export policy.<br><b>associations</b> — Displays where the <b>syslog-export-policy</b> is configured. |
| <b>Output</b>      | The following is an example of syslog export policy information.                                                                                                        |

**Sample Output**

```

*SR-OS-NODE-1# show service nat syslog syslog-export-policy <name>
=====
NAT syslog policy
=====
Description
Facility
Log prefix
Max tx delay (deciseconds)
MTU
Rate limit (pps)
Severity level
Includes
Last management change

```

```
Collectors

Router
Source IP address
Administrative state
Destination port
IP address
Last management change

```

The following output is an example of syslog export policy associations.

### Sample Output

```
*A:Dut-C# show service nat syslog syslog-export-policy <name> associations
=====
policies with syslog-export-policy <name>
=====
Policy

No. of policies
=====
```

The following output is an example of syslog-export-policy <name> information.

```
*A:Dut-C# show service nat nat-policy <name>
=====
NAT Policy policy_lsn_1_3
=====
Description :

Pool :
Router :
Filtering :
Block limit :
Reserved ports :
Port usage High Watermark (%) :
Port usage Low Watermark (%) :
Port forwarding limit :
Port forwarding range end :
Session limit :
Reserved sessions :
Session usage High Watermark (%) :
Session usage Low Watermark (%) :
ALG enabled :
Prioritized forwarding classes :
Timeout TCP established (s) :
Timeout TCP transitory (s) :
Timeout TCP SYN (s) :
Timeout TCP TIME-WAIT (s) :
Timeout TCP RST (s) :
Timeout UDP mapping (s) :
Timeout UDP initial (s) :
Timeout UDP DNS (s) :
Timeout ICMP Query (s) :
```

```

Timeout SIP Inactive Media (s) :
Subscriber retention (s) :
UDP inbound refresh :
TCP MSS Adjust :
Destination NAT classifier :
Destination-NAT-only router :
Destination-NAT-only ISA NAT group :
IPFIX export policy :
Syslog export policy ? syslog-export-
policy associated with this nat-policy
Reset unknown TCP :
L2 outside :
Last Mgmt Change :

```

The following is an example of syslog-export-policy information.

```

*A:Dut-C>show>service>nat>syslog# syslog-export-policy
=====
Syslog export policies
=====
Syslog export policy
Description? description of each syslog-export-policy

No. of syslog export policies:

```

[Table 52](#) displays syslog export policy field descriptions.

**Table 52**      **syslog-export-policy Fields**

| Field                      | Description                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                | Displays the description for the syslog export policy.                                                                                                                                                                                            |
| Facility                   | Displays information about the facility.<br>Valid values: kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7 |
| Log prefix                 | Displays information about the log prefix.                                                                                                                                                                                                        |
| Max tx delay (deciseconds) | Displays the time waited to aggregate multiple events into a single log message (event aggregation).                                                                                                                                              |
| MTU                        | Displays information about the IP MTU of the syslog frame.                                                                                                                                                                                        |
| Rate limit (pps)           | Displays the rate limit imposed on syslog frames sent toward the collector.                                                                                                                                                                       |
| Severity level             | Displays the syslog severity level.<br>Valid values: emergency, alert, critical, error, warning, notice, info, debug                                                                                                                              |



**Table 52**      **syslog-export-policy Fields (Continued)**

| Field                         | Description                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------|
| Includes                      | Displays the optional fields related to the flow that can be included in the flow log message. |
| Last management change        | Displays the time and date of the last configuration change.                                   |
| Router                        | Displays the routing instance from which the collector is reachable.                           |
| Source IP address             | Displays the source IP address of the syslog frame.                                            |
| Administrative state          | Displays the administrative state of the collector.                                            |
| Destination port              | Displays the destination port of the collector.                                                |
| IP address                    | Displays the IP address of the collector.                                                      |
| Syslog export policy          | Displays the syslog export policy associated with this NAT policy.                             |
| No. of syslog export policies | Displays the number of syslog export policies configured in the system.                        |

## l2-aware-blocks

- Syntax**    **l2-aware-blocks** [**outside-ip-prefix** *ip-prefix/length*] [**outside-port** [1..65535]] [**pool** *pool-name*]
- Context**    show>router>nat
- Description**    This command displays Layer 2 aware NAT blocks.
- Parameters**    *ip-prefix* — Specifies the IP prefix.  
                     **Values**      a.b.c.d (host bits must be 0)  
                     *length* — Specifies the IP prefix length.  
                     **Values**      1 to 32  
                     *pool-name* — Specifies the pool name up to 32 characters.
- Output**        The following is sample output for this command.

### Sample Output

```
show router nat l2-aware-blocks
=====
Layer-2-Aware NAT blocks for Base
=====
```

```

10.81.0.0 [32..33]
Pool : MyPool
Policy : outPolicy
Started : 2010/02/04 16:24:55
Subscriber ID : Sub001
10.81.0.0 [34..35]
Pool : MyPool
Policy : outPolicy
Started : 2010/02/04 16:25:24
Subscriber ID : Sub003
10.81.0.203 [32..41]
Pool : MyPool2
Policy : outPolicy2
Started: 2010/02/04 16:25:21
Subscriber ID : Sub002

```

```

Number of blocks: 3
=====

```

## lsn-blocks

|                    |                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>lsn-blocks</b> [ <b>inside-router</b> <i>router-instance</i> ] [ <b>inside-ip</b> <i>ip-address</i> ] [ <b>outside-ip-prefix</b> <i>ip-prefix/length</i> ] [ <b>outside-port</b> [0..65535]] [ <b>pool</b> <i>pool-name</i> ] |
| <b>Context</b>     | show>router>nat                                                                                                                                                                                                                  |
| <b>Description</b> | This command displays large scale NAT blocks.                                                                                                                                                                                    |
| <b>Parameters</b>  | <i>router-instance</i> — Specifies the router instance name and service ID.                                                                                                                                                      |
|                    | <b>Values</b>                                                                                                                                                                                                                    |
|                    | router-name: Base , management                                                                                                                                                                                                   |
|                    | service-id: 1 to 2147483647                                                                                                                                                                                                      |
|                    | svc-name: A string up to 64 characters.                                                                                                                                                                                          |

*ip-address* — Specifies the IP address in a.b.c.d format.

*ip-prefix* — Specifies the IP prefix.

**Values** a.b.c.d (host bits must be 0)

*length* — Specifies the IP prefix length.

**Values** 1 to 32

*pool-name* — Specifies the pool name, up to 32 characters.

**Output** The following is sample output for this command.

### Sample Output

```

*A:SR12_PPP0E>show>router>nat# show router Base nat lsn-blocks
=====
Large-Scale NAT blocks for Base

```

```
=====
10.0.0.5 [1024..1527]
Pool : privpool
Policy : priv-nat-policy
Started : 2012/01/28 19:10:17
Inside router : vprn100
Inside IP address : 2001:db8:470:1F00:FFFF:189

Number of blocks: 1
=====
A:SR12_PPPOE#
```

## pool

|                    |                                                                  |
|--------------------|------------------------------------------------------------------|
| <b>Syntax</b>      | <b>pool</b> <i>pool-name</i><br><b>pool</b>                      |
| <b>Context</b>     | show>router>nat                                                  |
| <b>Description</b> | This command displays NAT pool information.                      |
| <b>Parameters</b>  | <i>pool-name</i> — Specifies the pool name, up to 32 characters. |
| <b>Output</b>      | The following is sample output for this command.                 |

### Sample Output

```
show router nat pool
=====
NAT pools
=====
Pool NAT-group Type Admin-state

MyPool 1 l2Aware inService
MyPool2 1 l2Aware inService

No. of pools: 2
=====

*A:SR12_PPPOE>show>router>nat# show router "Base" nat pool "privpool"
=====
NAT Pool privpool
=====
ISA NAT Group : 3
Pool type : largeScale
Admin state : inService
Mode : auto (napt)
Port forwarding range : 1 - 1023
Port reservation : 128 blocks
Block usage High Watermark (%) : (Not Specified)
Block usage Low Watermark (%) : (Not Specified)
Subscriber limit per IP address : 65535
Active : true
Last Mgmt Change : 01/28/2012 14:47:59
```

```
=====
NAT address ranges of pool privpool
=====
Range Drain Num-blk

10.0.0.5 - 10.0.0.6 1

No. of ranges: 1
=====
NAT members of pool privpool ISA NAT group 3
=====
Member Block-Usage-% Hi

1 < 1 N
2 < 1 N

No. of members: 2
=====
A:SR12_PPPOE#
```

subscriber-identification

- Syntax** summary
- Context** show>router>nat
- Description** This command displays the NAT subscriber identification information.

summary

- Syntax** summary
- Context** show>router>nat
- Description** This command displays the NAT information summary.
- Output** The following is sample output for this command.

Sample Output

```
*A:SR12_PPPOE>show>router>nat# show router Base nat summary
=====
NAT pools
=====
Pool NAT-group Type Admin-state

privpool 3 largeScale inService
pubpool 1 largeScale inService

No. of pools: 2
=====
A:SR12_PPPOE#
```

## upnp

|                    |                                                                     |
|--------------------|---------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp</b>                                                         |
| <b>Context</b>     | show>service                                                        |
| <b>Description</b> | This command enables the context to display UPnP policy parameters. |

## upnp-policy

|                    |                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp-policy</b> <i>policy-name</i><br><b>upnp-policy</b> <i>policy-name</i> <b>statistics</b><br><b>upnp-policy</b>                                              |
| <b>Context</b>     | show>service>upnp                                                                                                                                                   |
| <b>Description</b> | This commands displays upnp-policy related information.<br><br>Without any parameters the system outputs a list of configured UPnP policies.                        |
| <b>Parameters</b>  | <i>policy-name</i> — The system displays the configuration of the specified policy.<br><b>statistics</b> — The system displays statistics for the specified policy. |
| <b>Output</b>      | The following is sample output for this command.                                                                                                                    |

### Sample Output

```
show service upnp upnp-policy
=====
UPnP policies
=====
Policy Description

test

No. of UPnP policies: 1
=====

show service upnp upnp-policy "test"
=====
UPnP Policy test
=====
Description : (Not Specified)
Mapping limit : 256
Strict mode : false
HTTP listening port : 5000
Last Mgmt Change : 01/26/2015 19:23:41

Active mappings : 2
Mapped subscribers : 1
Associated subscribers : 1
=====
```

```
show service upnp upnp-policy "test" statistics
=====
UPnP Policy test Statistics
=====
rx SSDP M-SEARCH : 109
rx HTTP GET device description : 0
rx HTTP GET service description : 109
rx UPnP AddPortMapping : 6
rx UPnP ClearPortMapping : 0
rx UPnP DeletePortMapping : 1
rx UPnP ForceTermination : 0
rx UPnP GetConnectionTypeInfo : 0
rx UPnP GetExternalAddress : 6
rx UPnP GetGenericPortMappingEntry : 43
rx UPnP GetNATRSIPStatus : 8
rx UPnP GetSpecificPortMappingEntry : 1
rx UPnP GetStatusInfo : 49
rx UPnP RequestConnection : 0
rx UPnP SetConnectionType : 0
rx UPnP unsupported optional action : 6
rx UPnP invalid request : 0
tx SSDP M-SEARCH : 109
tx TCP reset : 0
tx HTTP OK : 109
tx UPnP OK : 101
tx UPnP error : 19
drop no memory : 0
portmapping created : 4
portmapping updated : 1
portmapping failed: conflict with other host : 0
portmapping failed: conflict with pinhole : 0
portmapping failed: hit limits : 0
portmapping failed: other reason : 0
=====
```

7.25.2.16 MAP-T Show Commands



**Note:** The MAP-T CLI show commands described in this section apply to the Nokia Virtualized Service Router (VSR) only.

frag-stats

|             |                                                          |
|-------------|----------------------------------------------------------|
| Syntax      | frag-stats                                               |
| Context     | show>service>nat>map                                     |
| Description | This command displays NAT MAP fragmentation information. |

**Output** The following is sample output for this command, and [Table 53](#) describes the fields.

### Sample Output

```
*A:Dut-D>show>service>nat>map# show service nat map frag-stats
=====
NAT MAP fragmentation statistics
=====
Rx Resolved Packets : 0
Rx Unresolved Packets : 0
Tx Frags : 0
Dropped Frags : 0
Created Flows : 0
Flow Collisions : 0
Exceeded Max Flows : 0
Exceeded Max Timeouts : 0
Exceeded Max Buffers : 0
Exceeded Max Buffers Per Flow : 0
In-Use Flows % : 0
Max Flows % : 0
In-Use Buffers % : 0
Max Buffers % : 0
=====
```

**Table 53** Map Frag-Stats Output Fields

| Label                 | Description                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rx Resolved Packets   | Specifies fragments that were resolved and never buffered. This includes: <ul style="list-style-type: none"><li>• first fragments (MF=1, FO=0), which are always resolved by definition</li><li>• non-first fragments that have matching flow records</li></ul>                                                                                  |
| Rx Unresolved Packets | Specifies the number of packets that were queued in the system since the last clear command was invoked. For example, out-of-order fragments without a matching flow record (missing the first fragment). These packets can be eventually resolved and forwarded, or discarded (for example, as a result of timeout).                            |
| Tx Frags              | Specifies the fragments that were transmitted (Rx Resolved and Rx Unresolved that were eventually resolved) out of the fragmentation logic within the VSR. There is no guarantee that these fragments will be transmitted out of the system as they may be dropped on egress due to congestion or restrictions imposed by the configured filter. |
| Dropped Frags         | Specifies the dropped fragments due to some fragmentation issue (timeout, buffer full).                                                                                                                                                                                                                                                          |

**Table 53 Map Frag-Stats Output Fields (Continued)**

| Label                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Created Flows                 | <p>A cumulative counter that represents the total number of flow records since the last <b>clear</b> command was invoked. It only counts the first fragment and roughly represents the amount of fragmented packets that were processed by the system since the last clear command.</p> <p>The counter does not provide any indication about the number of flows (packets whose fragments were transmitted fully) that were actually transmitted.</p> |
| Flow Collisions               | Represents the number of overlapping first fragments. For example, when a flow record already exists and another first fragment for this flow is received.                                                                                                                                                                                                                                                                                            |
| Exceeded Max Flows            | Specifies the number of occurrences when the number of flows in the system exceeded its maximum supported value.                                                                                                                                                                                                                                                                                                                                      |
| Exceeded Max Timeouts         | <p>Specifies the number of fragments that have timed out (since the last <b>clear</b> command):</p> <ul style="list-style-type: none"> <li>• Rx unresolved (buffered) fragments that have timed out, due to a missing first fragment</li> <li>• deleted flow-records because they have not received all fragments within the timeout period</li> </ul>                                                                                                |
| Exceeded Max Buffers          | Specifies the number of occurrences when the number of buffers in the system exceeded its maximum supported value.                                                                                                                                                                                                                                                                                                                                    |
| Exceeded Max Timeouts         | <p>Specifies the number of fragments that have timed out (since the last clear command):</p> <ul style="list-style-type: none"> <li>• Rx unresolved (buffered) fragments that have timed out, due to a missing 1st fragment</li> <li>• deleted flow-records because they have not received all fragments within the timeout period</li> </ul>                                                                                                         |
| Exceeded Max Buffers          | Specifies the number of occurrences when the number of buffers in the system exceeded its maximum supported value.                                                                                                                                                                                                                                                                                                                                    |
| Exceeded Max Buffers Per Flow | Specifies the number of occurrences when a fragment count per flow has exceeded its limit.                                                                                                                                                                                                                                                                                                                                                            |
| In-Use Flows                  | An approximation of the number of flow records that are currently in use. The counter provides an estimate, expressed in percent, of the number of fragmented packets that were being processed at the time the counter was invoked.                                                                                                                                                                                                                  |
| Max Flows                     | Specifies the amount of time in seconds that the system will remain in a hold down state before being used again.                                                                                                                                                                                                                                                                                                                                     |



**Table 53 Map Frag-Stats Output Fields (Continued)**

| Label          | Description                                                                                                                                                                                                                                                                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In-Use Buffers | Represents the amount of buffered fragments, expressed in percent of the maximum buffer space, that can be used for fragmentation.                                                                                                                                                                                                   |
| Max Buffers    | A non-cumulative counter that represents the maximum number of buffers allocated since the last <b>clear</b> command. The counter captures the highest value of the <b>buffers-in-use</b> counter since the last <b>clear</b> command. The counter shows the percentage of the total buffer space that can be used by fragmentation. |

## map-domain

**Syntax** **map-domain**  
**map-domain** *domain-name*  
**map-domain** *domain-name* **mapping-rule** *map-rule-name*  
**map-domain** *domain-name* **statistics**

**Context** show>service>nat>map

**Description** This command displays the MAP domains configured in the system and shows whether the domain is instantiated (that is, shows the association with the routing context). It also provides information about the domain and the specific rules configured within the domain

**Parameters** *domain-name* — Specifies the MAP domain name.

**Values** 32 chars maximum

*map-rule-name* — Specifies the MAP rule name.

**Values** 32 chars maximum

**mapping-rule** — Keyword; displays the router instances and/or subscriber profiles associated with the NAT policy.

**statistics** — Keyword; displays statistics of the specified MAP domain.

**Output** The following is sample output for the **map-domain** command, and [Table 54](#) describes the fields.

### Sample Output

```
*A:Dut-D>show>service>nat>map# show service nat map map-domain
=====
MAP domains
=====
Name Admin-state Router

AZ in-service 221
```

```

AZb in-service N/A

No. of domains: 2
=====

```

**Table 54** Map-Domain Output Fields

| Label       | Description                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin-state | Configured admin-state of the MAP domain. The state can be either <b>shutdown</b> or <b>no shutdown</b> .                                                  |
| Router      | Specifies the routing context in which the MAP domain is instantiated. When set to "N/A", it indicates that the MAP domain is not instantiated in the VSR. |

The following is sample output for the **map-domain domain-name** command, and [Table 55](#) describes the fields.

**Sample Output**

```

*A:Dut-D>show>service>nat>map# map-domain "AZ"
=====
MAP-T domain "AZ"
=====
Description : bAAAA
Default Mapping Rule prefix : 1000::/4
MTU : 9212
TCP MSS adjust : 0
IP fragmentation
 v6-frag-header : enabled
Administrative state : in-service
Router : 221
Last management change : 07/14/2016 21:04:04
Mapping rule "rule A-11"

Description : basic mapping rule 11
Rule prefix : 2001:db8::/44
IPv4 prefix : 192.0.2.0/24
Embedded Address bits : 12
PSID offset : 4
Address sharing ratio : 0
No. of excluded ports : 0
No. of ports per user : 0
Administrative state : out-of-service
Last management change : 07/08/2016 01:15:12
Mapping rule "rule A-12"

Description : (Not Specified)
Rule prefix : (Not Specified)
IPv4 prefix : (Not Specified)
Embedded Address bits : 0
PSID offset : 6
Address sharing ratio : 0

```

```

No. of excluded ports : 0
No. of ports per user : 0
Administrative state : out-of-service
Last management change : 07/08/2016 01:15:12
Mapping rule "rule A-13"

Description : basic mapping rule 11
Rule prefix : 2001:db8::/44
IPv4 prefix : 192.0.2.0/24
Embedded Address bits : 9
PSID offset : 15
Address sharing ratio : 2
No. of excluded ports : 2
No. of ports per user : 32767
Administrative state : in-service
Last management change : 07/14/2016 21:11:43
=====

```

**Table 55** Map-Domain <domain-name> Output Fields

| Label                 | Description                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------|
| Address sharing ratio | Specifies the number of CEs covered by this rule, that share the same IPv4 address, each with different PSID. |
| No. of excluded ports | Specifies the ports excluded from PSID, according to the configured PSID offset.                              |
| No. of ports per user | Specifies the number of PSID ports available to each user.                                                    |

The following is sample output for the **map-domain** *domain-name* command, which shows the details of the specific rule within a given MAP domain.

### Sample Output

```

*A:Dut-D>show>service>nat>map# map-domain "AZ" mapping-rule "rule A-13"
=====
MAP-T domain "AZ"
=====
Description : bAAAA
Default Mapping Rule prefix : 1000::/4
MTU : 9212
TCP MSS adjust : 0
IP fragmentation
 v6-frag-header : enabled
Administrative state : in-service
Router : 221
Last management change : 07/14/2016 21:04:04
Mapping rule "rule A-13"

Description : basic mapping rule 11
Rule prefix : 2001:db8::/44
IPv4 prefix : 192.0.2.0/24
Embedded Address bits : 9

```

```

PSID offset : 15
Address sharing ratio : 2
No. of excluded ports : 2
No. of ports per user : 32767
Administrative state : in-service
Last management change : 07/14/2016 21:11:43
=====

```

The following is sample output for the **map-domain statistics** command, which shows the forwarding statistics for a MAP-T domain, and [Table 56](#) describes the fields.

### Sample Output

```

*A:Dut-D>show>service>nat>map# show service nat map map-domain "AZ" statistics
=====
MAP domain "AZ"
=====
Upstream (IPv6->IPv4) forwarded packets : 0
Upstream (IPv6->IPv4) forwarded octets : 0
Upstream (IPv6->IPv4) dropped packets : 0
Upstream (IPv6->IPv4) dropped octets : 0
Downstream (IPv4->IPv6) forwarded packets : 0
Downstream (IPv4->IPv6) forwarded octets : 0
Downstream (IPv4->IPv6) dropped packets : 0
Downstream (IPv4->IPv6) dropped octets : 0
=====

```

**Table 56** Map-Domain Statistics Output Fields

| Label                                      | Description                                                                                  |
|--------------------------------------------|----------------------------------------------------------------------------------------------|
| Upstream (IPv6 → IPv4) forwarded packets   | Specifies the number of forwarded packets in the upstream direction within the MAP domain.   |
| Upstream (IPv6 → IPv4) forwarded octets    | Specifies the number of forwarded octets in the upstream direction within the MAP domain.    |
| Upstream (IPv6 → IPv4) dropped packets     | Specifies the number of dropped packets in the upstream direction within the MAP domain.     |
| Upstream (IPv6 → IPv4) dropped octets      | Specifies the number of dropped octets in the upstream direction within the MAP domain.      |
| Downstream (IPv4 → IPv6) forwarded packets | Specifies the number of forwarded packets in the downstream direction within the MAP domain. |
| Downstream (IPv4 → IPv6) forwarded octets  | Specifies the number of forwarded octets in the downstream direction within the MAP domain.  |

**Table 56 Map-Domain Statistics Output Fields (Continued)**

| Label                                    | Description                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------|
| Downstream (IPv4 → IPv6) dropped packets | Specifies the number of dropped packets in the downstream direction within the MAP domain. |
| Downstream (IPv4 → IPv6) dropped octets  | Specifies the number of dropped octets in the downstream direction within the MAP domain.  |

## 7.25.2.17 NAT Clear Commands

### nat-group

|                    |                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-group</b> <i>nat-group-id</i> <b>member</b> [1 ..255] <b>l2-aware-subscribers</b><br><b>nat-group</b> <i>nat-group-id</i> <b>statistics</b> <i>mda mda-id</i><br><b>nat-group</b> <i>nat-group-id</i> <b>member</b> [1 ..255] <b>resource-peak-values</b><br><b>nat-group</b> <i>nat-group-id</i> <b>member</b> [1 ..255] <b>statistics</b>                          |
| <b>Context</b>     | clear>nat>isa                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b> | This command clears ISA nat-group commands related statistics or removes all the subscribers that are associated with a specific nat-group member                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <i>nat-group-id</i> — Specifies the NAT group ID to clear.<br><b>Values</b> 1 to 4<br><b>l2-aware-subscribers</b> — Specifies to clear the NAT group ID's l2-aware subscribers.<br><b>statistics</b> — Specifies to clear the NAT group ID's statistics.<br><b>resource-peak-values</b> — Specifies to reset the resource peak values to the current resource measurements. |

### upnp-mappings

|                    |                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp-mappings subscriber</b> <i>sub-ident-string</i> <b>protocol</b> {tcp   udp} <b>outside-port</b> <i>port-number</i><br><b>upnp-mappings subscriber</b> <i>sub-ident-string</i> |
| <b>Context</b>     | clear>nat                                                                                                                                                                             |
| <b>Description</b> | This command remove UPnP mappings for the specified subscriber. If <b>protocol</b> and <b>outside-port</b> are not specified, then all UPnP mappings of subscriber will be removed.   |
| <b>Parameters</b>  | <b>subscriber</b> <i>sub-ident-string</i> — clears mappings for the specified subscriber.                                                                                             |

**protocol {tcp | udp}** — Clears the mappings for the specified protocol.

**outside-port *port-number*** — Clears mappings for the specified outside-port.

## upnp-policy-statistics

|                    |                                                                              |
|--------------------|------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>upnp-policy-statistics</b> <i>policy-name</i>                             |
| <b>Context</b>     | clear>nat                                                                    |
| <b>Description</b> | This command clears UPnP policy statistics.                                  |
| <b>Parameters</b>  | <i>policy-name</i> — Clears UPnP policy statistics for the specified policy. |

## gateway

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>gateway brg-id <i>brg-ident</i></b><br><b>gateway brg-id <i>brg-ident</i> idle-bindings [<i>binding</i> <i>ieee-address</i>]</b><br><b>gateway all-gateways</b><br><b>gateway brg-id <i>brg-ident</i> all-hosts</b><br><b>gateway brg-id <i>brg-ident</i> host <i>ieee-address</i></b>                                                                                                                                                                                        |
| <b>Context</b>     | clear>subscr-mgmt>vrgw>brg                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command clears Bridged Residential Gateway (BRG) data.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parameters</b>  | <b>brg-id <i>brg-ident</i></b> — Specifies the string that represents the identifier of a Bridged Residential Gateway.<br><b>idle-bindings</b> — Clears data for idle bindings only.<br><b>binding <i>ieee-address</i></b> — Specifies a binding address for which to clear data.<br><b>all-gateways</b> — Clears data for all gateways.<br><b>all-hosts</b> — Clears data for all hosts.<br><b>host <i>ieee-address</i></b> — Specifies a host address for which to clear data. |

### 7.25.2.18 MAP-T Clear Commands



**Note:** The MAP-T CLI clear commands described in this section apply to the Nokia Virtualized Service Router (VSR) only.

## frag-stats

|                    |                                                        |
|--------------------|--------------------------------------------------------|
| <b>Syntax</b>      | <b>frag-stats</b>                                      |
| <b>Context</b>     | clear>nat>map>statistics                               |
| <b>Description</b> | This command clears the MAP fragmentation information. |

## map-domain

|                    |                                                                          |
|--------------------|--------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>map-domain</b> <i>domain-name</i>                                     |
| <b>Context</b>     | clear>nat>map>statistics                                                 |
| <b>Description</b> | This command clears the MAP domains statistics.                          |
| <b>Parameters</b>  | <i>domain-name</i> — Specifies the MAP domain name, up to 32 characters. |

## 7.25.2.19 NAT Tools Commands

### nat

|                    |                                                         |
|--------------------|---------------------------------------------------------|
| <b>Syntax</b>      | <b>nat</b>                                              |
| <b>Context</b>     | tools>dump<br>tools>perform                             |
| <b>Description</b> | This command enables the dump or perform tools for NAT. |

### isa

|                    |                                                  |
|--------------------|--------------------------------------------------|
| <b>Syntax</b>      | <b>isa</b>                                       |
| <b>Context</b>     | tools>dump>nat                                   |
| <b>Description</b> | This command enables the dump tools for NAT ISA. |

## performance

|                |                                                               |
|----------------|---------------------------------------------------------------|
| <b>Syntax</b>  | <b>performance mda</b> <i>mda-id last time-span time-unit</i> |
| <b>Context</b> | tools>dump>nat>isa                                            |

- Description** This command generates an overview of the processing load and data processed by the specified ISA over a period of time. The following time periods are supported:
- last minute with seconds granularity
  - last hour with minutes granularity
  - last day with hours granularity
  - last 31 days with days granularity
- Parameters** *mda-id* — Specifies the MDA for getting performance measurements in format *slot/mda*.
- Values** slot — 1 to 10  
mda — 1 to 2
- time-span* — Specifies the period for which to get measurements.
- Values** 1 to 60 (sec) | 1 to 60 (min) | 1 to 24 (hrs) | 1 to 31 (days)
- time-unit* — Specifies the period for which to get measurements.
- Values** sec | min | hrs | days

## resources

- Syntax** **resources mda mda-id**
- Context** tools>dump>nat>isa
- Description** This command enables dump ISA resources for an MDA.
- Output** The following is sample output for this command.

### Sample Output

```
AR12_PPPOE# tools dump nat isa resources mda 3/1
```

```
Resource Usage for Slot #3 Mda #1:
```

|                           | Total       | Allocated | Free        |
|---------------------------|-------------|-----------|-------------|
| Flows                     | 6291456     | 0         | 6291456     |
| Policies                  | 256         | 2         | 254         |
| Port-ranges               | 1310720     | 128       | 1310592     |
| Ports                     | 12884901888 | 0         | 12884901888 |
| IP-addresses              | 65536       | 1         | 65535       |
| Large-scale hosts         | 524288      | 0         | 524288      |
| L2-aware subscribers      | 65536       | 0         | 65536       |
| L2-aware hosts            | 65536       | 0         | 65536       |
| Delayed ICMP's            | 200         | 0         | 200         |
| ALG session               | 1572864     | 0         | 1572864     |
| LI entries                | 8191        | 0         | 8191        |
| Upstream fragment lists   | 16384       | 0         | 16384       |
| Downstream fragment lists | 16384       | 0         | 16384       |
| Upstream fragment holes   | 131072      | 0         | 131072      |
| Downstream fragment holes | 131072      | 0         | 131072      |



|                          |       |   |       |
|--------------------------|-------|---|-------|
| Upstream fragment bufs   | 13824 | 0 | 13824 |
| Downstream fragment bufs | 13824 | 0 | 13824 |
| flow log dest. set 0     | 2     | 0 | 2     |
| flow log packets set 0   | 50    | 0 | 50    |
| flow log dest. set 1     | 2     | 0 | 2     |
| flow log packets set 1   | 50    | 0 | 50    |
| flow log dest. set 2     | 1     | 0 | 1     |
| flow log packets set 2   | 50    | 0 | 50    |

A:SR12\_PPPOE#

## sessions

**Syntax** `sessions [nat-group nat-group-id] [mda mda-id] [protocol {gre | icmp | icmp6 | tcp | udp | unknown}] [inside-ip ip-prefix[/ip-prefix-length]] [inside-router router-instance] [inside-port port-number] [outside-ip ipv4-address] [outside-port port-number] [foreign-ip ip-address] [foreign-port port-number] [dslite-address ipv6-address] [wlan-gw-ue ieee-address] [next-index index] [upnp] [member member-id] [nat-policy policy-name] [dest-ip ip-address] [firewall-policy policy-name] [address-type addr-type] [l2-aware-subscriber sub-ident]`

**Context** tools>dump>nat

**Description** This command dumps ISA sessions.

**Parameters** **icmp** — Specifies to dump only ICMP information.

*ieee-address* — Specifies a MAC address, using the format xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

*ip-address* — Specifies an IPv4 or IPv6 address.

**Values** *ipv4-address* — a.b.c.d  
*ipv6-address* — x:x:x:x:x:x:x (eight 16-bit pieces)  
x:x:x:x:x:d.d.d.d  
x — 0 to FFFF (in hexadecimal)  
d — 0 to 255 (in decimal)

*ipv4-address* — Specifies an IPv4 address.

**Values** a.b.c.d

*ipv6-address* — Specifies an IPv6 address.

**Values** x:x:x:x:x:x:x (eight 16-bit pieces)  
x:x:x:x:x:d.d.d.d  
x — 0 to FFFF (in hexadecimal)  
d — 0 to 255 (in decimal)

*mda-id* — Specifies an MDA ID.

**Values** *slot/mda*

*nat-group-id* — Specifies a NAT group ID.

**Values** 1 to 4

*policy-name* — Specifies a policy name, up to 32 characters maximum.

*port-number* — Specifies a port number.

**Values** 0 to 65535

*router-instance* — Specifies a router name or service ID.

**tcp** — Specifies to dump only TCP information.

**udp** — Specifies to dump only UDP information.

**upnp** — Specifies to dump only UPNP information.

**Output** The following is sample output for this command.

### Sample Output

```
*A:SR12_PPPOE# tools dump nat sessions
=====
Matched 2 sessions on Slot #3 MDA #1
=====
Owner : LSN-Host@10.2.3.4
Router : 100
FlowType : UDP PortFwd
Inside IP Addr : 10.2.3.4 Inside Port : 666
Outside IP Addr : 10.0.0.6 Outside Port : 666
Foreign IP Addr : * Foreign Port : *
Dest IP Addr : * Dest Port : *

Owner : LSN-Host@10.2.3.4
Router : 100
FlowType : TCP PortFwd
Inside IP Addr : 10.2.3.4 Inside Port : 666
Outside IP Addr : 10.0.0.6 Outside Port : 666
Foreign IP Addr : * Foreign Port : *
Dest IP Addr : * Dest Port : *

=====
Matched 1 session on Slot #3 MDA #2
=====
Owner : LSN-Host@2001:db8:470:1F00:FFFF:189
Router : 100
FlowType : TCP Timeout (sec) : 6769
Inside IP Addr : 192.168.16.218 Inside Port : 41555
Outside IP Addr : 10.0.0.5 Outside Port : 1529
Foreign IP Addr : 10.0.0.1 Foreign Port : 22
Dest IP Addr : 10.0.0.1 Dest Port : 22

=====
*A:SR12_PPPOE#
```

## histogram

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>histogram router</b> <i>router-instance</i> <b>pool</b> <i>pool-name</i> <b>bucket-size</b> [1..65536] <b>num-buckets</b> [2..50]                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Context</b>     | tools>dump>nat                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | This command displays a NAT pool port usage histogram                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Parameters</b>  | <b>router</b> <i>router-instance</i> — Specifies the router instance.<br><b>pool</b> <i>pool-name</i> — Specifies the identification of the NAT pool.<br><b>bucket-size</b> [1..65536] — Specifies the unit of the X-axis of the histogram; a value of ten, for example, would return in a histogram with results for [0-9], [10-19], [20-29], ... ports.<br><b>num-buckets</b> [2..50] — Specifies the size of the histogram; a value of five, for example, would result in five results: [0-9], [10-19], [20-29], [30-39], [40-infinite]. |

## port-forwarding-action

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <b>Syntax</b>      | <b>port-forwarding-action</b>                      |
| <b>Context</b>     | tools>perform>nat                                  |
| <b>Description</b> | This command displays NAT port forwarding actions. |

## l2-aware

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>l2-aware create subscriber</b> <i>sub-ident-string</i> <b>ip</b> <i>ip-address</i> <b>protocol</b> {tcp   udp} [ <b>port</b> <i>port</i> ] <b>lifetime</b> <i>lifetime</i> [ <b>outside-ip</b> <i>ip-address</i> ] [ <b>outside-port</b> <i>port</i> ] [ <b>nat-policy</b> <i>policy-name</i> ]<br><b>l2-aware delete subscriber</b> <i>sub-ident-string</i> <b>ip</b> <i>ip-address</i> <b>protocol</b> {tcp   udp} <b>port</b> <i>port</i> [ <b>nat-policy</b> <i>policy-name</i> ]<br><b>l2-aware modify subscriber</b> <i>sub-ident-string</i> <b>ip</b> <i>ip-address</i> <b>protocol</b> {tcp   udp} <b>port</b> <i>port</i> <b>lifetime</b> <i>lifetime</i> [ <b>nat-policy</b> <i>policy-name</i> ] |
| <b>Context</b>     | tools>perform>nat>port-forwarding-action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command enables Layer-2-Aware NAT port forwarding action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## lsn

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <b>lsn create router</b> <i>router-instance</i> [ <b>b4</b> <i>ipv6-address</i> ] [ <b>afr</b> <i>ipv6-address</i> ] <b>ip</b> <i>ip-address</i> <b>protocol</b> {tcp   udp} [ <b>port</b> <i>port</i> ] <b>lifetime</b> <i>lifetime</i> [ <b>outside-ip</b> <i>ipv4-address</i> ] [ <b>outside-port</b> <i>port</i> ] [ <b>nat-policy</b> <i>nat-policy-name</i> ]<br><b>lsn delete router</b> <i>router-instance</i> [ <b>b4</b> <i>ipv6-address</i> ] <b>ip</b> <i>ip-address</i> <b>protocol</b> {tcp   udp} <b>port</b> |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```

 port [nat-policy nat-policy-name]
lsn modify router router-instance [b4 ipv6-address] ip ip-address protocol {tcp | udp} port
port lifetime lifetime [nat-policy nat-policy-name]

```

**Context** tools>perform>nat>port-forwarding-action

**Description** This command enables large-scale NAT port forwarding actions.

**Output** The following is sample output for this command.

### Sample Output

```

*A:SR12_PPPOE# tools perform nat port-forwarding-action lsn create router 100
ip 10.2.3.4 protocol tcp lifetime infinite outside-port 666
*A:SR12_PPPOE# tools perform nat port-forwarding-action lsn create router 100
ip 10.2.3.4 protocol udp lifetime infinite outside-port 666
*A:SR12_PPPOE# configure system persistence nat-port-forwarding location cf3:
*A:SR12_PPPOE# tools dump persistence nat-port-forwarding

Persistence Info

Client : nat-fwds
File Info :
 Filename : cf3:\nat_fwds.002
 File State : CLOSED (Not enough space on disk)
Subsystem Info :
 Nbr Of Registrations : 524288
 Registrations In Use : 2
 Subsystem State : NOK
*A:SR12_PPPOE#

show+service+nat
| | | +---port-forwarding-entries
| | | +---classic-lsn-sub
| | | +---dslite-lsn-sub
| | | +---l2-aware-sub
| | | +---nat64-lsn-sub

```

## recover-l2aw-bypass

**Syntax** recover-l2aw-bypass mda

**Context** tools>perform>nat

**Description** This command restores NAT resources to the recovered MS-ISA and resumes forwarding subscriber traffic.

## 8 Residential Firewall

### 8.1 Residential Firewall Overview

The residential firewall protects a home by tracking all flows to or from the home. Only inbound traffic that matches flows that originated inside of the home is allowed to pass through the firewall. By blocking other flows, an attacker cannot initiate a connection to a vulnerable service within the home. The residential firewall also provides protection against fingerprinting, port scanning, and DoS attacks. The dynamic flow tracking functionality provides a better user experience compared to static firewall rules because it does not limit any connection that has been set up within the home.

The residential firewall is based entirely on the tracking of Layer 3 and Layer 4 flows. Minimal application layer gateway (ALG) support is provided to allow protocols that use multiple flows, but application layer protection is not supported. The firewall only supports IPv6 flows. It is recommended to use Layer 2-aware NAT to provide similar protection for IPv4 flows within the same residential subscriber.

#### 8.1.1 Supported Protocols and Extension Headers

The residential firewall distinguishes between known and unknown protocols or known and unknown extension headers.

Unknown protocols will create or match flows only based on Layer 3 information. For a known protocol, the firewall will inspect Layer 4 information to create or match flows more precisely. The following known protocols are supported:

- TCP
- UDP
- ICMPv6

Known extension headers will be allowed by the firewall and processing will continue on the remainder of the packet. The following extension headers are treated as known:

- Hop-by-hop (0)
- Fragment Header (44)
- Authentication Header (51)

- Destination Options (60)
- Shim Header (140)

### 8.1.1.1 Unknown Protocols

Unknown protocols are created and matched by a 3-tuple identifier that has the format <source IP, destination IP, protocol>. No Layer 4 data is used to differentiate between possible sub-flows. Because the firewall is unaware of unknown protocol states, removal of flows with unknown protocols is only governed by a single configurable timeout.

### 8.1.1.2 TCP and UDP

TCP and UDP flows are created and matched by a 5-tuple identifier that has the format <source IP, destination IP, protocol, source port, destination port>. Multiple configurable timeouts can apply depending on the exact flow state.

### 8.1.1.3 ICMPv6

ICMPv6 error messages (codes up to 127) are handled based on the encapsulated invoking packet. Layer 3 and Layer 4 information is re-extracted from the packet and is used to perform a flow lookup. If an existing flow is found, then the error message will be forwarded; otherwise, it will be dropped.

ICMPv6 echo flows are created and matched by a 4-tuple identifier that has the format <source IP, destination IP, protocol, identifier>. Echo replies must always match an existing flow. A single configurable timeout applies to these flows.

Other informational or non-transit ICMPv6 messages will be dropped by the firewall.

## 8.1.2 Application Layer Gateway

Application layer gateways (ALGs) are used to track protocols where one flow triggers the creation of several associated flows. For example, a single session initiation protocol (SIP) session can trigger several additional media connections. These flows are not always triggered from inside the home, but traffic should still be allowed to pass. To support this, the residential firewall creates additional flows when a supported ALG connection is recognized and enabled.

## 8.1.3 Additional Filtering Control

The residential firewall has two filtering modes that control which action to take when an inbound packet does not match an existing flow.

In address and port-dependent filtering mode, security is considered most important and packets that do not match an existing flow are dropped. This could interfere with the operation of some applications that rely on multiple connections using the same host port.

In endpoint independent filtering mode, application transparency is considered most important. When a packet matches any flow that has the correct protocol and destination IP address, the packet will be allowed to pass, and the IP address and port of the foreign endpoint are ignored. The assumption is that the application that triggers the original session may require additional remotely-triggered sessions for correct operation. This can be a security concern when an application with known vulnerabilities is used, as all firewall functionality for that application ceases as soon as the application itself opens one flow. Additionally, this exposes the host to fingerprinting attacks.

In addition to filtering, it is possible to limit the number of sessions, or flows, per subscriber. Sessions can be split into priority and non-priority categories based on their mapped forwarding class. Separate limits apply to each category to avoid starvation of priority sessions by non-priority sessions. This granularity of control helps to protect the firewall and the host against DoS attacks and resource starvation.

## 8.1.4 TCP MSS Adjustment

TCP maximum segment size (MSS) adjustment can be used to clamp the MSS value that is sent during a TCP handshake. If the MSS option is not present, or is bigger than the configured value, then the firewall will change it to the configured value.

This is useful when a low-MTU link is used, such as during tunneling. If the MSS is changed to match the low MTU, IP layer packet fragmentation can be avoided, improving the performance of both the firewall and the end hosts.

## 8.1.5 Static Port Forwards and DMZ

The residential firewall supports static port forwards and DMZ to selectively allow inbound network-initiated traffic flows. Static port forwards allow operators to open up a specific subset of traffic. An exact IP address and a protocol must be provided. For TCP and UDP traffic, the system also requires at least one port. A foreign prefix or port may also be provided to limit the pinhole to a specific connection.

DMZ is enabled on a per-host basis and disables the firewall for that specific host. Before traffic can be forwarded on SLAAC hosts, the exact /128 address must be learned, either by DAD snooping, or initial upstream traffic. For security reasons, the system does not send any ND for a completely unknown /128 address for network-initiated flows.

Static port forwards are configured under the AAA Context. Refer to the 7750 SR and VSR RADIUS Attributes Reference Guide for more information.



## 8.2 Residential Firewall Provisioning

Residential firewalls are provisioned in three steps.

1. A firewall domain is created in the router or VPRN where the firewall is connected to an unsafe network, such as the Internet. In this domain, a list of prefixes specify which prefixes are subject to firewall rules.
2. A firewall policy is created that specifies operational rules for the firewall and which domain should be used.
3. The firewall policy is linked to an ESM subscriber using the subscriber profile.

```
Node# /configure service vprn 4 firewall
Node>config>service>vprn>firewall# info

 domain "domain_4" nat-group 1 create
 prefix 2001:DB8::/32 create
 exit
 no shutdown
 exit

Node# /configure service nat
Node>config>service>nat# info

 firewall-policy "firewall_4" create
 description "IPv6 Firewall policy for VPRN 4"
 domain router 4 name "domain_4"
 filtering address-and-port-dependent
 exit

Node# /configure subscriber-mgmt
Node>config>subscr-mgmt# info

 sub-profile "profile_1" create
 firewall-policy "firewall_4"
 exit

```

### 8.2.1 Domains and Addressing

A firewall domain specifies both the network (router or VPRN) to which a firewall is connected and which IP prefixes in that network are protected by the firewall. Hosts of a firewall-enabled subscriber will automatically be protected if they are assigned an IP address from a domain prefix. It is possible to mix protected and unprotected hosts within one subscriber, but unprotected hosts must receive an IP address that is outside of the firewall domain.

---

The router or VPRN where the firewall domain is configured must not be the same as the router or VPRN where the subscriber is terminated. This function replaces classic ESM wholesale/retail for firewall hosts.

## 9 TCP MSS Adjustment

### 9.1 Overview

This feature adds support for adjustment of MSS of TCP packets with SYN flag according to access/aggregation network in order to prevent fragmentation of upstream and downstream TCP packets using ISA-BB.

There are two modes of adjustment operations supported: TCP MSS Adjustment for ESM Hosts, and TCP MSS Adjustment for NAT Services.

## 9.2 TCP MSS Adjustment for ESM Hosts

This feature adds support for adjustment of the MSS size of TCP packets with SYN flag according to the access/aggregation network in order to prevent fragmentation of upstream and downstream TCP packets using ISA-BB diverted by IP/IPv6 filter actions.

The following ESM host types are supported:

- IPv4/IPv6 IPoE hosts
- Locally terminated PPPoE hosts (without L2TP LAC)
- L2TP LNS hosts

### Configuration steps

1. Create a NAT group used for an MSS adjustment.

```
config>isa
nat-group 1
active-mda-limit 2
mda 1/1
mda 1/2
```

2. Associate the NAT group with a routing instance and configure the MSS value.

```
config>router
config>service>vprn
mss-adjust-group 1 segment-size 1452
```

3. Create an IPv4/IPv6 filter to perform an MSS adjust.

```
config>filter>ip-filter>entry
egress-pbr default-load-balancing
match tcp-syn
action tcp-mss-adjust
config>filter>ipv6-filter>entry
match tcp-syn
action tcp-mss-adjust
```

4. Apply an IPv4/IPv6 filter to the SLA profile.

---

## 9.3 TCP MSS Adjustment for NAT Services

This feature provides MSS adjustment for TCP packets to be translated by NAT services.

### Configuration steps

1. Create a NAT-group used for NAT services with MSS adjustment.

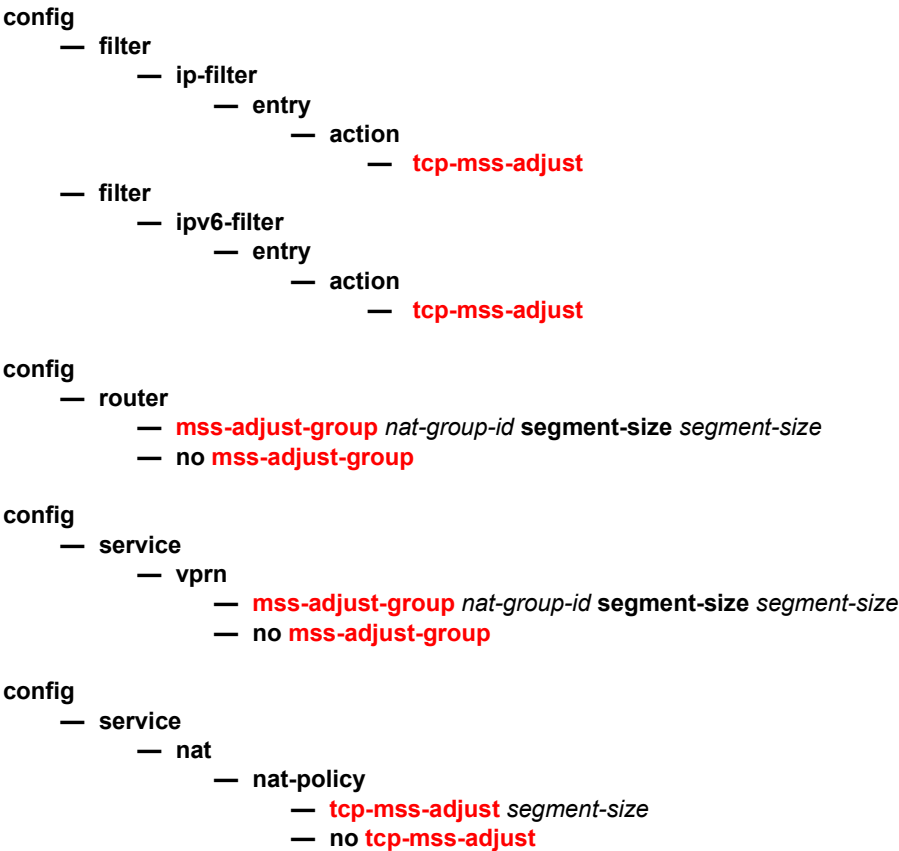
```
config>isa
 nat-group 1
 active-mda-limit 2
 mda 1/1
 mda 1/2
```

2. Create a NAT-policy that also adjusts MSS.

```
configure>service>nat
 nat-policy "policy-for-mss-adjust" crate
 tcp-mss-adjust 1452
```

## 9.4 TCC MSS Adjustment Commands

### 9.4.1 Command Hierarchy



#### 9.4.1.1 TCC MSS Adjustment Command Descriptions

##### mss-adjust-group

**Syntax** mss-adjust-group nat-group-id segment-size segment-size  
no mss-adjust-group

**Context** config>router  
config>service>vprn

|             |                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | This command associate the MSS adjust group consisting of multiple ISAs with the routing context in which the application requiring TCP MSS adjust resides.                                                                              |
| Parameters  | <i>nat-group-id</i> — specifies the NAT group used for a TCP MSS adjustment<br><i>segment-size</i> — specifies the value to put into the TCP Maximum Segment Size (MSS) option if not already present, or if the present value is higher |
| Values      | 160 to 10240                                                                                                                                                                                                                             |

tcp-mss-adjust

|             |                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------|
| Syntax      | tcp-mss-adjust                                                                                                        |
| Context     | config>filter>ip-filter>entry>action<br>config>filter>ipv6-filter>entry>action                                        |
| Description | This command activates the adjustment of the TCP Maximum Segment Size (MSS) option of TCP packets matching the entry. |

tcp-mss-adjust

|             |                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | tcp-mss-adjust <i>segment-size</i><br>no tcp-mss-adjust                                                                                                        |
| Context     | config>service>nat>nat-policy                                                                                                                                  |
| Description | This command configures the Maximum Segment Size (MSS) adjustment for TCP packets.<br><br>The <b>no</b> form of the command disables adjusting tcp-mss values. |
| Parameters  | <i>segment-size</i> — Specifies the segment size.                                                                                                              |
| Values      | 160 to 10240                                                                                                                                                   |



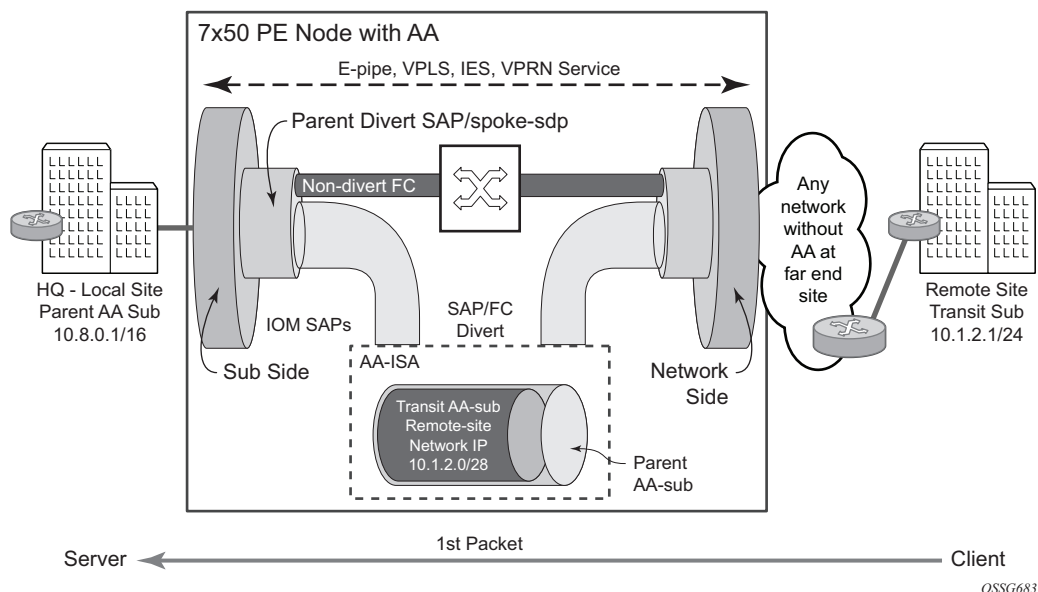


## 10 L2TP Network Server

### 10.1 Subscriber agg-rate-limit on LNS

In non-LNS ESM environment, the existing **agg-rate-limit** command is applied to the subscriber within the subscriber profile (sub-profile). However, the agg-rate-limit cannot be the highest level in subscriber's HQoS hierarchy. The agg-rate-limit will be only effective if it is applied to a subscriber that is tied to a port-scheduler. In other words, the port-scheduler in subscriber's HQoS hierarchy is a prerequisite for successful operation of agg-rate-limit. On regular MDAs, the port-scheduler is directly applied to a physical port. The port between the carrier IOM and the ISA is an internal port that is not exposed in the CLI. This is shown in [Figure 89](#).

**Figure 89** QoS Hierarchy on LNS



The port-scheduler will be applied to the internal Ins-esm port in the egress direction. The Ins-esm egress port is a port between the carrier IOM and the ISA that is passing traffic from all VRFs that have subscriber L2TP sessions terminated in the corresponding ISA.

The port-scheduler will be applied to each Ins-esm port with the following CLI:

**CLI Syntax:**

```
configure
port-policy <port-policy-name>
```

```
egress-scheduler-policy <port-scheduler-policy-
name>
```

Port-policy at the root CLI level will create a port policy manager that can apply various policies (port scheduler) to hidden, dynamically created ports for WLAN GW/LNS/NAT.

**CLI Syntax:**

```
configure
isa
 lns-group <grp-id>
 mda <card>/<slot>
 mda <card>/<slot>
 :
 port-policy <port-policy-name>
```

The port policy itself will be applied to internal LNS port under the lns-group CLI hierarchy. The port scheduler will automatically be applied to egress lns-esm ports on carrier IOMs towards every LNS ISA in the lns-group. The port schedulers will have the same configuration on every lns-esm port in the lns group but will operate independently on each port. Additional consideration:

- An ISA can be assigned to a single lns-group. In other words, two or more LNS-groups can not contain the same ISA. However, an ISA can belong simultaneously to an LNS-group and a NAT group. The port scheduler will affect only LNS traffic.
- The port scheduler rates are wire rates that are based on the encapsulation between the carrier IOM and the ISA which is Ethernet QinQ. However, the queue rates, the billing stats and the agg-rate-limit rates can be optionally based on the last mile encapsulation in the same way as they have been supported in non-LNS environment with **queue-frame-based-accounting** and **encap-offset** commands.

The ability to calculate queue rates or the agg-rate-limit based on the last mile encapsulation is referred to as Last Mile Aware Shaping.

For example, the **encap-offset** command will cause the queue rates, the billing stats and the agg-rate-limit to be based on the wire encapsulation in the last mile. For ATM in the last mile, the wire overhead will be calculated per each packet (including ATM cellification overhead and padding). For Ethernet in the first mile, a fixed last mile encapsulation (defined with the **encap-offset** command or the RFC 5515, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*) wire overhead will be considered in rate calculation. In essence the length of the PPPoE Ethernet QinQ header that is used on the link between the carrier IOM and the ISA will be artificially modified so that it matches the length of the header used in the last mile. The net effect is rate shaping on LNS based on the virtual packet length that is present in the last mile.

The last mile encapsulation information that is used in Last Mile Aware Shaping can be obtained either statically through the explicit value in the **encap-offset** command or dynamically by the RFC 5515 method (AVP 144 in ICRQ). The latter will be the case if the **encap-offset** command does not have any explicitly configured value.

In the absence of the **encap-offset** command, the queue rates, the billing stats and the agg-rate-limit rates will be based on the Ethernet QinQ encapsulation between the carrier IOM and the ISA. Depending on the queue-frame-based-accounting configuration option, those rates can be wire based or data based (Layer 2 encapsulation only).

- The agg-rate-limit is not applicable to ingress direction (LNS or non LNS ESM).
- V-Port is not applicable in LNS configuration.

## 10.2 LNS Reassembly

### 10.2.1 Overview

In certain cases PPPoE clients do not honor the negotiated MRU during the LCP phase and consequently they will send packets larger than the negotiated MRU. This applies to control and data packets.

In this case, the LAC will fragment IPv4 packets which will then have to be reassembled in LNS.

In general, reassembly processing applies only to the end nodes that are receiving fragments. In tunneled environment a fragmented packet must be reassembled before it is de-encapsulated.

### 10.2.2 Reassembly Function

LNS reassembly is implemented through a generic IPv4 reassembly function that can be shared across multiple ISAs in a nat-group. The same ISA can be independently part of an lns-group and a nat-group.

Traffic that needs to be reassembled is steered to the nat-group via filters. Once the fragmented traffic is in the nat-group, it will be reassembled and injected back within the same routing context to the lns-group for further L2TP processing.

Configuration steps:

Configure two isa groups, a nat-group providing generic reassembly function and a lns-group providing the L2TP services. The ISAs can be shared amongst the groups, or they can be separated per each group:

**CLI Syntax:**

```
configure
isa
 nat-group 1
 active-mda-limit 2
 mda 1/1
 mda 1/1
 lns-group 1
 mda 1/1
 mda 1/2
```

Configure redirection of the L2TP traffic to the nat-group performing reassembly:

**CLI Syntax:**

```
configure
filter
 ip-filter 10
 entry 5
 match
 dst-ip 10.10.10.10 - traffic
 classification criteria ; in
 this case LNS tunnel endpoint.
 action reassemble
 default-action forward
```

Apply 'reassembly' filter on the incoming L2TP traffic:

**CLI Syntax:**

```
configure
router
 interface from-lac
 address 10.0.0.1/24
 port 2/2/2
 ingress
 filter ip 10
```

Associate the reassembly context with the same service where LNS is configured.

**CLI Syntax:**

```
configure
service
 vprn 10
 reassembly-group 1
 l2tp
 group "lns-vrf-10" create
 ppp
 authentication-policy "lns"
 proxy-authentication
 proxy-lcp
 tunnel "lns-test-tunnel" create
 lns-group 1
 no shutdown

 subscriber-interface "int1" create
 address 10.20.20.254/24
 group-interface "lns-grp-10" lns
 create
 sap-parameters
 sub-sla-mgmt
 sub-ident-policy "sub-ident"
 dhcp
 server 192.168.1.1
```

```
trusted
client-applications ppp
gi-address 10.20.20.1
```

### 10.2.3 Load Sharing Between the ISAs

All traffic matching the criteria associated with the filter action reassemble will be forwarded to the reassembly function, regardless of whether the traffic is fragmented or not.

In case that there are multiple ISAs in the NAT-group, traffic is load shared between them based on the source IP address and the incoming service id (routing context).

### 10.2.4 Inter-chassis ISA Redundancy

In case that an active ISA fails in a nat-group, the standby ISA will take over the reassembly function. However, the switchover is not stateful and consequently traffic destined to the failed ISA will be lost until it is restarted.

## 10.3 MLPPPoE, MLPPP(oE)oA with LFI on LNS

MLPPPoX is generally used to address bandwidth constraints in the last mile. The following are other uses for MLPPPoX:

- To increase bandwidth in the access network by bundling multiple links/VCs together. For example it is less expensive for a customer with an E1 access to add another E1 link in order to increase the access b/w, rather than to upgrade to the next circuit speed (E3).
- LFI on a single link to prioritize small packet size traffic over traffic with large size packets. This is needed in the upstream and downstream direction.

PPPoE and PPPoEoA/PPPoA v4/v6 host types are supported.

### 10.3.1 Terminology

The term MLPPPoX is used to reference MLPPP sessions over ATM transport (oA), Ethernet over ATM transport (oEoA) or Ethernet transport (oE). Although MLPPP in subscriber management context is not supported natively over PPP/HDLC links, the terms MLPPP and MLPPPoX terms can be used interchangeably. The reason for this is that link bundling, MLPPP encapsulation, fragmentation and interleaving can be in a broader scope observed independently of the transport in the first mile. However, MLPPPoX terminology will be prevailing in this document in an effort to distinguish MLPPP functionality on ASAP MDA (outside of ESM) and MLPPPoX in LNS (inside of ESM).

Terms speed and rate are interchangeably used throughout this section. Usually speed refers to the speed of the link in general context (high or low) while rate usually quantitatively describes the link speed and associates it with the specific value in b/s.

### 10.3.2 LNS MLPPPoX

This functionality is supported through LNS on BB-ISA. LNS MLPPPoX can be used then as a workaround for PTA deployments, whereby LAC and LNS can be run back-to-back in the same system (connected via an external loop or a VSM2 module), and thus locally terminate PPP sessions.

MLPPPoX can:

- Increase bandwidth in the last mile by bundling multiple links together.

- LFI/reassembly over a single MLPPPoX capable link (plain PPP does not support LFI).

### 10.3.3 MLPPP Encapsulation

Once the MLPPP bundle is created in the 7750 SR, traffic can be transmitted by using MLPPP encapsulation. However, MLPPP encapsulation is not mandatory over an MLPPP bundle.

MLPPP header is primarily required for sequencing the fragments. But in case that a packet is not fragmented, it can be transmitted over the MLPPP bundle using either plain PPP encapsulation or MLPPP encapsulation.

### 10.3.4 MLPPPoX Negotiation

MLPPPoX is negotiated during the LCP session negotiation phase by the presence of the Max-Received-Reconstructed Unit (MRRU) field in the LCP ConfReq. MRRU option is a mandatory field required in MLPPPoX negotiation. It represents the maximum number of octets in the Information field of a reassembled packet. The MRRU value negotiated in the LCP phase must be the same on all member links and it can be greater or lesser than the PPP negotiated MRU value of each member link. This means that the reassembled payload of the PPP packet can be greater than the transmission size limit imposed by individual member links within the MLPPPoX bundle. Packets will always be fragmented so that the fragments are within the MRU size of each member link.

Another field that could be optionally present in an MLPPPoX LCP Conf Req is an Endpoint Discriminator (ED). Along with the authentication information, this field can be used to associate the link with the bundle.

The last MLPPPoX negotiated option is the Short Sequence Number Header Format Option which allows the sequence numbers in MLPPPoX encapsulated frames/fragments to be 12-bit long (instead 24-bit long, by default).

Once the multilink capability is successfully negotiated via LCP, PPP sessions can be bundled together over MLPPPoX capable links.

The basic operational principles are:

- LCP session is negotiated on each physical link with MLPPPoX capabilities between the two nodes.



- Based on the ED and/or the authentication outcome, a bundle is created. A subsequent IPCP negotiation is conveyed over this bundle. User traffic is sent over the bundle.
- If a new link tries to join the bundle by sending a new MLPPPoX LCP Conf Request, the LCP session will be negotiated, authentication performed and the link will be placed under the bundle containing the links with the same ED and/or authentication outcome.
- IPCP/IPv6CP will be in the whole process negotiated only once over the bundle. This negotiation will occur at the beginning, when the first link is established and MLPPPoX bundle created. IPCP and IPv6CP messages are transmitted from the 7750 SR LNS without MLPPPoX encapsulation, while they can be received as MLPPPoX encapsulated or non-MLPPPoX encapsulated.

### 10.3.5 Enabling MLPPPoX

The lowest granularity at which MLPPPoX can be enabled is an L2TP tunnel. An MLPPPoX enabled tunnel is not limited to carrying only MLPPPoX sessions but can carry normal PPP(oE) sessions as well.

In addition to enabling MLPPPoX on the session terminating LNS node, MLPPPoX can also be enabled on the LAC via PPP policy. The purpose of enabling MLPPPoX on the LAC is to negotiate MLPPPoX LCP parameters with the client. Once the LAC receives the MRRU option from the client in the initial LCP ConfReq, it will change its tunnel selection algorithm so that all sessions of an MLPPPoX bundle are mapped into the same tunnel.

The LAC will negotiate MLPPPoX LCP parameters regardless of the transport technology connected to it (ATM or Ethernet). LCP negotiated parameters are passed by the LAC to the LNS via Proxy LCP in ICCN message. In this fashion the LNS has an option to accept the LCP parameters negotiated by the LAC or to reject them and restart the negotiation directly with the client.

The LAC will transparently pass session traffic handed to it by the LNS in the downstream direction and the MLPPPoX client in the upstream direction. The LNS and the MLPPPoX client will perform all data processing functions related to MLPPPoX such as fragmentation and interleaving.

Once the LCP negotiation is completed and the LCP transition into an open state (configuration ACKs are sent and received), the Authentication phase on the LAC will begin. During the Authentication phase the L2TP parameters will become known (l2tp group, tunnel, etc), and the session will be extended by the LAC to the LNS via L2TP. In case that the Authentication phase does not return L2TP parameters, the

session will be terminated because the 7750 SR does not support directly terminated MLPPPoX sessions.

In the case that MLPPPoX is not enabled on the LAC, the LAC will negotiate plain PPP session with the client. In case that the client accepts plain PPP instead of MLPPPoX as offered by the LAC, when the session is extended to the LNS, the LNS will re-negotiate MLPPPoX LCP with the client on a MLPPPoX enabled tunnel. The LNS will learn about the MLPPPoX capability of the client via Proxy LCP message in ICCN (first Conf Req received from the client is also send in Proxy LCP). If there is no indication of the MLPPPoX capability of the client, the LNS will establish a plain PPP(oE) session with the client.

There is no dependency between ATM autosensing on LAC and MLPPPoX since autosensing operates on a lower layer than PPP (LCP).

### 10.3.6 Link Fragmentation and Interleaving (LFI)

The purpose of LFI is to ensure that short high priority packets are not delayed by the transmission delay of large low priority packets on slow links.

For example it takes ~150ms to transmit a 5000B packet over a 256 kb/s link, while the same packet is transmitted in only 40us over a 1G link (~4000 times faster transmission). To avoid the delay of a high priority packet by waiting in the queue while the large packet is being transmitted, the large packet can be segmented into smaller chunks. The high priority packet can be then interleaved with the smaller fragments. This approach can significantly reduce the delay of high priority packets.

The interleaving functionality is only supported on MLPPPoX bundles with a single link. If more than one link is added into a interleaving capable MLPPPoX bundle, then interleaving will be internally disabled and the `tmnxMlpppBundleIndicatorsChange` trap will be generated.

With interleaving enabled on an MLPPPoX enabled tunnel, the following session types are supported:

- Multiple LCP sessions tied into a single MLPPPoX bundle. This scenario assumes multiple physical links on the client side. Theoretically it would be possible to have multiple sessions running over the same physical link in the last mile. For example, two PPPoE sessions going over the same Ethernet link in the last mile, or two ATM VCs on the same last mile link. Whichever the case might be, the LAC/LNS is unaware of the physical topology in the last mile (single or multiple physical links). Interleaving functionality will be internally disabled on such MLPPPoX bundle.

- A single LCP session (including dual stack) over the MLPPPoX bundle. This scenario assumes a single physical link on the client side. Interleaving will be supported on such single session MLPPPoX bundle as long as the conditions for interleaving are met. Those conditions are governed by max-fragment-delay parameter and calculation of the fragment size as described in subsequent sections.
- An LCP session (including dual stack) over a plain PPP/PPPoE session. This type of session is a regular PPP(oE) session outside of any MLPPPoX bundle and therefore its traffic is not MLPPPoX encapsulated.

Packets on an MLPPPoX bundle are MLPPPoX encapsulated unless they are classified as high priority packets when interleaving is enabled.

### 10.3.6.1 MLPPPoX Fragmentation, MRRU and MRU Considerations

A packet of the size greater than the internally calculated fragment length cannot be natively transmitted over an MLPPPoX bundle. Such packet will be MLPPPoX encapsulated and consequently fragmented. This is irrespective of whether the fragmentation is enabled or disabled. The size of the internally calculated fragment length depends on:

- The desired transmission delay in the last mile.
- The fragment “payload to encapsulation overhead” efficiency ratio.
- Various MTU sizes in the 7750 SR dictated mainly by received MRU, received MRRU and configured PPP MTU under the following hierarchy:
  - configure service vprn l2tp group ppp mtu
  - configure service vprn l2tp group tunnel ppp mtu
  - configure router l2tp group ppp mtu
  - configure router l2tp group tunnel ppp mtu

In cases where MLPPPoX fragmentation is disabled with the **no max-fragment-delay** command, it is expected that packets are not MLPPPoX fragmented but rather only MLPPPoX encapsulated in order to be load balanced over multiple physical links in the last mile. However, even if MLPPPoX fragmentation is disabled, it is possible that fragmentation occurs under certain circumstances. This behavior is related to the calculation of the MTU values on an MLPPPoX bundle.

MLPPPoX in the 7750 SR is concerned with two MTUs:

- **bundle-mtu** determines the maximum length of the original IP packet that can be transmitted over the entire bundle (collection of links) before any MLPPPoX processing takes place on the transmitting side. This is also the maximum size of the IP packet that the receiving node can accept once it de-encapsulates and assembles received MLPPPoX fragments of the same packet. Bundle-mtu is relevant in the context of the collection of links.
- **link-mtu** determines the maximum length of the payload before it is PPP encapsulated and transmitted over an individual link within the bundle. Link-mtu is relevant in the context of the single link within the bundle.

Assuming that the CPE advertised MRRU and MRU values are smaller than any configurable mtu on MLPPPoX processing modules in the 7750 SR (carrier IOM and BB-ISA), the bundle-mtu and the link-mtu will be based on the received MRRU and MRU values, respectively. For example, the bundle-mtu will be set to the received MRRU value while link-bundle will be set to the MRU value minus the MLPPPoX encapsulation overhead (4 or 6 bytes).

Consider an example where received MRRU value sent by CPE is 1500B while received MRU is 1492B. In this case, our bundle-mtu will be set to 1500B and our link-mtu will be set to 1488B (or 1486B) to allow for the additional 4/6B of MLPPPoX encapsulation overhead. Consequently, IP payload of 1500B can be transmitted over the bundle but only 1488B can be transmitted over any individual link. In case that an IP packet with the size between 1489B and 1500B needs to be transmitted from the 7750 SR towards the CPE, this packet would be MLPPPoX fragmented in the 7750 SR as dictated by the link-mtu. This is irrespective of whether MLPPPoX fragmentation is enabled or disabled (as set by no max-fragment-delay flag).

To entirely avoid MLPPPoX fragmentation in this case, the received MRRU sent by CPE should be lower than the received MRU for the length of the MLPPPoX header (4 or 6 bytes). In this case, for IP packets larger than 1488B, IP fragmentation would occur (assuming that DF flag in the IP header allows it) and MLPPPoX fragmentation would be avoided.

On the 7750 SR side, it is not possible to set different advertised MRRU and MRU values with the **ppp-mtu** command. Both MRRU and MRU advertised values adhere to the same configured ppp mtu value.

### 10.3.7 LFI Functionality Implemented in LNS

As mentioned in the previous section, LFI on LNS is implemented only on MLPPPoX bundles with a single LCP session.

There are two major tasks associated with LFI on the LNS:

- Executing subscriber QoS in the carrier IOM based on the last mile conditions. The subscriber QoS rates are the last mile on-the-wire rates. Once traffic is QoS conditioned, it is sent to the BB-ISA for further processing.
- Fragmentation and artificial delay (queuing) of the fragments so that high priority packets can be injected in-between low priority fragments (interleaved). This operation is performed by the BB-ISA.

Most of this is also applicable to non-lfi case. The only difference between lfi and non-lfi is that there is no artificial delay performed in non-lfi case.

Examine an example to further clarify functionality of LFI. The parameters, conditions and requirements that will be used in our example to describe the desired behavior are the following:

- High priority packets must not be delayed for more than 50ms in the last mile due to the transmission delay of the large low priority packets. Considering that tolerated end-to-end VoIP delay must be under 150ms, limiting the transmission delay to 50ms on the last mile link is a reasonable choosing.
- The link between the LNS and LAC is 1Gb/s Ethernet.
- The last mile link rate is 256 kb/s.
- Three packets arrive back-to-back on the network side of the LNS (in the downstream direction). The large 5000B low priority packet P1 arrives first, followed by two smaller high priority packets P2 and P3, each 100B in length. Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).
- The transmission time on the internal 10G link between the BB-ISA and the carrier IOM for the large packet (5000B) is 4us while the transmission time for the small packet (100B) is 80ns.
- The transmission time on the 1G link (LNS->LAC) for the large packet (5000B) is 40us while the transmission time for the small packet (100B) is 0.8us.
- The transmission time in the last mile (256 kb/s) for the large packet is ~150ms while the transmission time for the small packet on the same link is ~3ms.
- Last mile transport is ATM.

To satisfy the delay requirement for the high priority packets, the large packets will be fragmented into three smaller fragments. The fragments will be carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there will be window of opportunity to interleave the two smaller high priority packets.

This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG).

The five points are:

1. [Last Mile QoS Awareness in the LNS](#)
2. [BB-ISA Processing](#)
3. [LNS-LAC Link](#)
4. [AN-RG Link](#)
5. [Home Link](#)

### 10.3.7.1 Last Mile QoS Awareness in the LNS

By implementing MLPPPoX in LNS, we are effectively transferring the traffic treatment functions (QoS/LFI) of the last mile to the node (LNS) that is multiple hops away.

The success of this operation depends on the accuracy at which we can simulate the last mile conditions in the LNS. The assumption is that the LNS is aware of the two most important parameters of the last mile:

- The last mile encapsulation — This is needed for the accurate calculation of the overhead associated of the transport medium in the last mile for traffic shaping and interleaving.
- The last mile link rate — This is crucial for the creation of artificial congestion and packet delay in the LNS.

The subscriber QoS in the LNS is implemented in the carrier IOM and is performed on a per packets basis before the packet is handed over to the BB-ISA. Per packet, rather than per fragment QoS processing will ensure a more efficient utilization of network resources in the downstream direction. Discarding fragments in the LNS would have detrimental effects in the RG as the RG would be unable to reconstruct a packet without all of its fragments.

High priority traffic within the bundle is classified into the high priority queue. This type of traffic is not MLPPPoX encapsulated unless its packet size exceeds the link MTU as described in [MLPPPoX Fragmentation, MRRU and MRU Considerations](#). Low priority traffic is classified into a low priority queue and is always MLPPPoX encapsulated. In case that the high priority traffic becomes MLPPPoX encapsulated/fragmented, the MLPPPoX processing module (BB-ISA) will consider it as low-priority. The assumption is that the high priority traffic is small in size and consequently MLPPPoX encapsulation/fragmentation an degradation in priority can be avoided. The aggregate rate of the MLPPPoX bundle is on-the-wire rate of the last mile as shown in Figure 3.

ATM on-the-wire overhead for non-MLPPPoX encapsulated high priority traffic will include:

- ATM encapsulation (VC-MUX, LLC/NLPID, LLC/SNAP).
- AAL5 trailer (8B).
- AAL5 padding to 48B cell boundary (this makes the overhead dependent on the packet size).
- Multiplication by 53/48 to account for the ATM cell headers.

For low priority traffic which is always MLPPPoX encapsulated, an additional overhead related to MLPPPoX encapsulation and possibly fragmentation must be added (blue arrow in Figure 3). In other words, each fragment carries ATM+MLPPPoX overhead.

The 48B boundary padding can be avoided for all fragments except the last one. This can be done by choosing the fragment length so that it is aligned on the 48B boundary (rounded down if based on max-fragment-delay or rounded up if based on the encapsulation/utilization).

For Ethernet in the last mile, our implementation always assures that the fragment size plus the encapsulation overhead is always larger or equal to the minimum Ethernet packet length (64B).

### 10.3.7.2 BB-ISA Processing

MLPPPoX encapsulation, fragmentation and interleaving are performed by the LNS in BB-ISA. If we refer to our example, a large low priority packet (P1) is received by the BB-ISA, immediately followed by the two small high priority packets (P2 and P3). Since our requirement stipulates that there is no more than 50ms of transmission delay in the last mile (including on-the-wire overhead), the large packet must be fragmented into three smaller fragments each of which will not cause more than 50ms of transmission delay.

The BB-ISA would normally send packets/fragments to the carrier IOM at the rate of 10Gb/s. In other words, by default the three fragments of the low priority packet would be sent out of the BB-ISA back-to-back at the very high rate before the high priority packets even arrive in the BB-ISA. In order to interleave, the BB-ISA must simulate the last mile conditions by delaying the transmission of the fragments. The fragments will be paced out of the BB-ISA (and out of the box) at the rate of the last mile. High priority packets will get the opportunity to be injected in front of the fragments while the fragments are being delayed.

As shown in [Figure 89](#) (point 2) the first fragment F1 is sent out immediately (transmission delay at 10G is in the 1us range). The transmission of the next fragment F2 is delayed by 50ms. While the transmission of the second fragment F2 is being delayed, the two high priority packets (P1 and P2 in red) are received by the BB-ISA and are immediately transmitted ahead of fragments F2 and F3. This approach relies on the imperfection of the IOM shaper which is releasing traffic in bursts (P2 and P3 right after P1). The burst size is dependent on the depth of the rate token bucket associated with the IOM shaper.

By the time the second fragment F2 is transmitted, the first fragment F1 has traveled a long way (50ms) on high rate links towards the Access Node (assuming that there is no queuing delay along the way), and its transmission on the last mile link has already begun (if not already completed).

This is not applicable for this discussion, but nonetheless worth noticing is that the LNS BB-ISA also adds the L2TP encapsulation to each packet/fragment. The L2TP encapsulation is removed in the LAC before the packet/fragment is transmitted towards the AN.

### 10.3.7.3 LNS-LAC Link

This is the high rate link (1Gb/s) on which the first fragment F1 and the two consecutive high priority packets, P2 and P3, are sent back-to-back by the BB-ISA (BB-ISA->carrier IOM->egress IOM-> out-of-the-LNS).

The remaining fragments (F2 and F3) are still waiting in the BB-ISA to be transmitted. They are artificially delayed by 50ms each.

Additional QoS based on the L2TP header can be performed on the egress port in the LNS towards the LAC. This QoS is based on the classification fields inside of the packet/fragment headers (DSCP, dot1.p, EXP).

The LAC-AN link is not really relevant for the operation of LFI on the LNS. This link can be either Ethernet (in case of PPPoE) or ATM (PPPoE or PPP). The rate of the link between the LAC and the AN is still considered a high speed link compared to the slow last mile link.



#### 10.3.7.4 AN-RG Link

Finally, this is the slow link of the last mile, the reason why LFI is performed in the first place. Assuming that LFI played its role in the network as designed, by the time the transmission of one fragment on this link is completed, the next fragment arrives just in time for unblocked transmission. In between the two fragments, we can have one or more small high priority packets waiting in the queue for the transmission to complete.

On the AN-RG link in [Figure 89](#) that packets P2 and P3 are ahead of fragments F2 and F3. Therefore the delay incurred on this link by the low priority packets is never greater than the transmission delay of the first fragment (50ms). The remaining two fragments, F2 and F3, can be queued and further delayed by the transmission time of packets P2 and P3 (which is normally small, in our example 3ms for each).

If many low priority packets are waiting in the queue, then they would have caused delay and would have further delayed the fragments that are in transit from the LNS to the LAC. This condition is normally caused by bursts and it should clear itself out over time.

#### 10.3.7.5 Home Link

High priority packets P2 and P3 are transmitted by the RG into the home network ahead of the packet P1 although the fragment F1 has arrived in the RG first. The reason for this is that the RG must wait for the fragments F2 and F3 before it can re-assemble packet P1.

#### 10.3.7.6 Optimum Fragment Size Calculation by LNS

Fragmentation in LFI is based on the optimal fragment size. LNS implementation calculates the two optimal fragment sizes, based on two different criteria:

- Optimal fragment size based on the payload efficiency of the fragment given the fragmentation/transportation header overhead associated with the fragment encapsulation based fragment size.
- Optimal fragment size based on the maximum transmission delay of the fragment set by configuration delay-based fragment size.

At the end only one optimal fragment size will be selected. The actual fragments length will be of the optimal fragment size.

- The parameters required to calculate the optimal fragment sizes are known to the LNS either via configuration or via signaling. These, in-advance known parameters are:
- Last mile maximum transmission delay (max-fragment-delay obtained via CLI)
- Last mile ATM Encapsulation (in our example the last mile is ATM but in general it can be Ethernet for MLPPPoE)
- MLPPP encapsulation length (depending on the fragment sequence number format)
- The last mile on-the-wire rate for the MLPPPoX bundle

Examine closer each of the two optimal fragment sizes.

#### 10.3.7.6.1 Encapsulation Based Fragment Size

One needs to be mindful of the fact that fragmentation may cause low link utilization. In other words, during fragmentation a node may end up transporting mainly overhead bytes in the fragment as opposed to payload bytes. This would only intensify the problem that fragmentation is intended to solve, especially on an ATM access link that tend to carry larger encapsulation overhead.

To reduce the overhead associated with fragmentation, the following is enforced in the 7750 SR:

The minimum fragment payload size will be at least 10times greater than the overhead (MLPPP header, ATM Encapsulation and AAL5 trailer) associated with the fragment.

The optimal fragment length (including the MLPPP header, the ATM Encapsulation and the AAL5 trailer) is a multiple of 48B. Otherwise, the AAL5 layer would add an additional 48B boundary padding to each fragment which would unnecessary expand the overhead associated with fragmentation. By aligning all-but-last fragments to a 48B boundary, only the last fragment will potentially contain the AAL5 48B boundary padding which is no different from a non-fragmented packet. For future reference we will refer to all fragments except for the last fragment as non-padded fragments. The last fragment will obviously be padded if it is not already natively aligned to a 48B boundary.

As an example, calculate the optimal fragment size based on the encapsulation criteria with the maximum fragment overhead of 22B. To achieve >10x transmission efficiency the fragment payload size must be 220B (10\*22B). To avoid the AAL5 padding, the entire fragment (overhead + payload) will be rounded UP on a 48B boundary. The final fragment size will be 288B [22B + 22B\*10 + 48B\_alignment].

In conclusion, an optimal fragment size was selected that will carry the payload with at least 90% efficiency. The last fragment of the packet cannot be artificially aligned on a 48B boundary (it is a natural reminder), so it will be padded by the AAL5 layer. Therefore the efficiency of the last fragment will probably be less than 90% in our example. In the extreme case, the efficiency of this last fragment may be only 2%.

The fragment size chosen in this manner is purely chosen based on the overhead length. The maximum transmission delay did not play any role in the calculations.

For Ethernet based last mile, the CPM always makes sure that the fragment size plus encapsulation overhead is larger or equal to the minimum Ethernet packet length of 64B.

#### **10.3.7.6.2 Fragment Size Based on the Max Transmission Delay**

The first criterion in selecting the optimal fragment size based on the maximum transmission delay mandates that the transmission time for the fragment, including all overheads (MLPPP header, ATM encapsulation header, AAL5 overhead and ATM cell overhead) must be less than the configured max-fragment-delay time.

The second criterion mandates that each fragment, including the MLPPP header, the ATM Encapsulation header, the AAL5 trailer and the ATM cellification overhead be a multiple of 48B. The fragment size is rounded down to the nearest 48B boundary during the calculations in order to minimize the transmission delay. Aligning the fragment on the 48B boundary eliminates the AAL5 padding and therefore reduces the overhead associated with the fragment. The overhead reduction will not only improve the transmission time but it will also increase the efficiency of the fragment.

Given these two criteria along with the configuration parameters (ATM Encapsulation, MLPPP header length, max-fragment-delay time, rate in the last mile), the implementation calculates the optimal non-padded fragment length as well as the transmission time for this optimal fragment length.

#### **10.3.7.6.3 Selection of the Optimum Fragment Length**

So far the implementation has calculated the two optimum fragment lengths, one based on the length of the MLPPP/transport encapsulation overhead of the fragment, the other one based on the maximum transmission delay of the fragment. Both of them are aligned on a 48B boundary. The larger of the two is chosen and the BB-ISA will perform LFI based on this selected optimal fragment length.

## 10.3.8 Upstream Traffic Considerations

Fragmentation and interleaving is implemented on the originating end of the traffic. In other words, in the upstream direction the CPE (or RG) is fragmenting and interleaving traffic. There is no interleaving or fragmentation processing in the upstream direction in the 7750 SR. The 7750 SR will be on the receiving end and is only concerned with the reassembly of the fragments arriving from the CPE. Fragments will be buffered until the packet can be reconstructed. If all fragments of a packet are not received within a preconfigured timeframe, the received fragments of the partial packet will be discarded (a packet cannot be reconstructed without all of its fragments). This time-out and discard is necessary in order to prevent buffer starvation in the BB-ISA. Two values for the time-out can be configured: 100ms and 1s.

## 10.3.9 Multiple Links MLPPPoX With No Interleaving

Interleaving over MLPPPoX bundles with multiple links will not be supported. However, fragmentation is supported.

In order to preserve packet order, all packets on an MLPPPoX bundle with multiple links will be MLPPPoX encapsulated (monotonically increased sequence numbers).

We will not support multiclass MLPPP (RFC 2686, *The Multi-Class Extension to Multi-Link PPP*). Multiclass MLPPP would require another level of intelligent queuing in the BB-ISA which we do not have.

## 10.3.10 MLPPPoX Session Support

The following session types in the last mile will be supported:

- MLPPPoE — Single physical link or multilink. The last mile encapsulation is Ethernet over copper (This could be Ethernet over VDSL or HSDSL). The access rates (especially upstream) are still limited by the xDSL distance limitation and as such interleaving is required on a slow speed single link in the last mile. It is possible that the last mile encapsulation is Ethernet over fiber (FTTH) but in this case, users would not be concerned with the link speed to the point where interleaving and link aggregation is required.

Finally, this is the slow link of the last mile, the reason why LFI is performed in the first place. Assuming that LFI played its role in the network as designed, by the time the transmission of one fragment on this link is completed, the next fragment arrives just in time for unblocked transmission. In between the two fragments, we can have one or more small high priority packets waiting in the queue for the transmission to complete.

We can see on the AN-RG link in Figure 2 that packets P2 and P3 are ahead of fragments F2 and F3. Therefore the delay incurred on this link by the low priority packets is never greater than the transmission delay of the first fragment (50ms). The remaining two fragments, F2 and F3, can be queued and further delayed by the transmission time of packets P2 and P3 (which is normally small, in our example 3ms for each).

If many low priority packets were waiting in the queue, then they would have caused delay for each other and would have further delayed the fragments in transit from the LNS to the LAC. This condition is normally caused by bursts and it should clear itself out over time.

- MLPPP(oEo)A — A single physical link or multilink. The last mile encapsulation is ATM over xDSL.

Some other combinations are also possible (ATM in the last mile, Ethernet in the aggregation) but they all come down to one of the above models that are characterized by:

- Ethernet or ATM in the last mile.
- Ethernet or ATM access on the LAC.
- MLPPP/PPPoE termination on the LNS

### 10.3.11 Session Load Balancing Across Multiple BB-ISAs

PPP/PPPoE sessions are by default load balanced across multiple BB-ISAs (max 6) in the same group. The load balancing algorithm considers the number of active session on each BB-ISA in the same group.

The load balancing algorithm does not take into account the number of queues consumed on the carrier IOM. Therefore a session can be refused if queues are depleted on the carrier IOM even though the BB-ISA may be lightly loaded in terms of the number of sessions that is hosting.

With MLPPPoX, it is important that multiple sessions per bundle be terminated on the same LNS BB-ISA. This can be achieved by per tunnel load balancing mode where all sessions of a tunnel are terminated in the same BB-ISA. Per tunnel load balancing mode is mandatory on LNS BB-ISAs that are in the group that supports MLPPPoX.

On the LAC side, all sessions in an MLPPPoX bundle are automatically assigned to the same tunnel. In other words an MLPPPoX bundle is assigned to the tunnel. There can be multiple tunnels created between the same pair of LAC/LNS nodes.

### 10.3.12 BB-ISA Hashing Considerations

All downstream traffic on an MLPPPoX bundle with multiple links is always MLPPPoX encapsulated. Some traffic is fragmented and served in a octet oriented round robin fashion over multiple member links. However, fragments are never delayed in case that the bundle contains multiple links.

In a per fragment/packet load sharing algorithm, there is always the possibility that there is uneven load utilization between the member links. A single link overload will most likely go unnoticed in the network all the way to the Access Node. The access node is the only node in the network that actually has multiple physical links connected to it. All other session-aware nodes (LAC and LNS) only see MLPPPoX as a bundle with multiple sessions without any mechanism to shape traffic per physical link. Other nodes in this case being 7750 SRs. Other vendors may have the ability to condition (shape) traffic per session.

If one of the member sessions is perpetually overloaded by the LNS, traffic will be dropped in the last mile since the corresponding physical link cannot absorb traffic beyond its physical capabilities. This would have detrimental effects on the whole operation of the MLPPPoX bundle. To prevent this perpetual overloading of the member links that can be caused by per packet/fragment load balancing scheme, the load balancing scheme that takes into account the number of octets transmitted over each member link. The octet counter of a new link will be initialized to the lowest value of any existing link counter. Otherwise the load balancing mechanism would show significant bias towards the new link until the byte counter catches up with the rest of the links.

## 10.3.13 Last Mile Rate and Encapsulation Parameters

The last mile rate information along with the encapsulation information is used for fragmentation (to determine the maximum fragment length) and interleaving (delaying fragments in the BB-ISA). In addition, the aggregate subscriber rate (aggregate-rate-limit) on the LNS is automatically adjusted based on the last mile link rate and the number of links in the MLPPPoX bundle.

### Downstream Data Rate in the Last Mile

The subscriber aggregate rates (agg-rate-limit) used in (H)QoS on the carrier IOM and in the BB-ISA (for interleaving) must be wire based in the last mile. This rule applies equally to both, the LAC and LNS.

The last mile on-the-wire rates of the subscriber can be submitted to the LAC and the LNS via various means. Here is the break down on how the last mile wire rates will be passed to each entity:

### LAC

The last mile link rate is taken via the following methods in the order of listed priority:

- LUDB — **rate-down** command under the host hierarchy in LUDB.
- RADIUS Alc-Access-Loop-Rate-Down VSA. Although this VSA is stored in the state of plain PPP(oE) sessions (MLPPPoX bundled or not), it is applicable only to MLPPPoX bundles.
- PPPoE tags — Vendor Specific Tags (RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*; tag type 0x0105; tag value is Enterprise Number 3561 followed by the TLV sub-options as specified in TR-101 -> Actual Data Rate Downstream 0x82)

As long as the link rate information is available in the LAC, it will always be passed to the LNS in the ICRQ message using the standard L2TP encoding. This cannot be disabled.

In addition, an option is available to control the source of the rate information can be conveyed to the LNS via TX Connect Speed AVP in the ICCN message. This can be used for compatibility reasons with other vendors that can only use TX Connect Speed to pass the link rate information to the LNS. By default, the maximum port speed (or the sum of the maximum speeds of all member ports in the LAG) will be reported in TX Connect Speed. Unlike the rate conveyed in ICRQ message, The TX Connect Speed content is configurable via the following command:

```
config>subscr-mgmt
 sla-profile <name>
 egress
```

```
report-rate agg-rate-limit | scheduler <scheduler-name> | pppoe-actual-
rate
| rfc5515-actual-rate
```

The report-rate configuration option will dictate which rate will be reported in the TX Connect Speed as follows:

- agg-rate-limit => statically configured agg-rate-limit value or RADIUS QoS override will be reported
- scheduler <scheduler-name> => virtual schedulers are not supported in MLPPPoX
- pppoe-actual-rate => rate taken from PPPoE Tags will be reported. Rate reported via RFC5515 can still be different if the source for both methods is not the same.
- rfc5515-actual-speed => the rate is taken from RFC5515.

The RFC 5515 relies on the same encoding as PPPoE tags (vendor id is ADSL Forum and the type for Actual Data Rate Downstream is 0x82). The two methods of passing the line rate to the LNS are using different message types (ICRQ and ICCN).

The LAC on the 7750 SR is not aware of MLPPPoX bundles. As such, the aggregate subscriber bandwidth on the LAC is configured statically via usual means (sub-profile, scheduler-policy) or dynamically modified via RADIUS. The aggregate subscriber (or MLPPPoX bundle) bandwidth on the LAC is not automatically adjusted according to the rates of the individual links in the bundle and the number of the links in the bundle. As such, an operator must ensure that the statically provided rate value for aggregate-rate-limit is the sum of the bandwidth of each member link in the MLPPPoX bundle. The number of member links and their bandwidth must be therefore known in advance. The alternative is to have the aggregate rate of the MLPPPoX bundle set to a high value and rely on the QoS treatment performed on the LNS.

## LNS

The sources of information for the last mile link rate on the LNS will be taken in the following order:

- LUDB (during user authentication phase, same as in LAC)
- RADIUS (same as in LAC)
- ICRQ message — Actual Data Downstream Rate (RFC 5515)
- ICCN message — TX Connect Speed



There will be no configuration option to determine the priority of the source of information for the last mile link rate. TX Connect Speed in ICCN message will only be taken into consideration as a last resort in absence of any other source of last mile rate information.

Once the last mile rate information is obtained, the subscriber aggregate rate (aggregate-rate-limit will be automatically adjusted to the minimum value of:

- The smallest link speed in the MLPPPoX bundle multiplied by the number of links in the bundle.
- Statically configured aggregate-rate-limit

The link speed of each link in the bundle must be the same, i.e. different link speeds within the bundle are not supported. In the case that we receive different link speed values for last mile links within the bundle, we will adopt the minimum received speed and apply it to all links.

In case that the obtained rate information from the last mile for a session within the MLPPP bundle is out of bounds (1 kb/s to 100 Mb/s), the session within the bundle will be terminated.

### Encapsulation

Wire-rates are dependent on the encapsulation of the link to which they apply. The last mile encapsulation information can be extracted via various means.

### LAC

- Static configuration via LUDB.
- RADIUS — Alc-Access\_Loop-Encap-Offset VSA.
- PPPoE tags — Vendor Specific Tags (RFC 2516; tag type 0x0105; tag value is Enterprise Number 3561 followed by the TLV sub-options as specified in TR-101 -> Actual Data Rate Downstream 0x82).

The LAC will pass the line encapsulation information to the LNS via ICRQ message using the encoding defined in the RFC 5515.

### LNS

The LNS will extract the encapsulation information in the following order:

- Static configuration via LUDB.
- RADIUS — Alc-Access-Loop-Encap-Offset VSA.
- ICRQ message (RFC 5515)

In case that the encapsulation information is not provided by any of the existing means (LUDB, RADIUS, AVP signaling, PPPoE Tags), then by default pppoa-null encapsulation will be in effect. This applies to LAC and LNS.

### 10.3.14 Link Failure Detection

The link failure in the last mile is detected via the expiration of session keepalives (LCP). The LNS will tear down the session over the failed link and notify the LAC via a CDN message.

### 10.3.15 CoA Support

CoA request for the subscriber aggregate-rate-limit change is honored on the LAC and the LNS.

CoA for the rate change of an individual link within the bundle is supported through the same VSA that can be used to initially assign the rate parameter to each member link. This is supported only on LNS. The rate override via CoA is applied to all active link members within the bundle.

Change of the access link parameters via CoA is supported in the following fashion:

- Change of access loop encap: refused (NAK)
- Change of access loop rate down:
- On L2TP LAC session: refused (NAK). On LAC the access loop rate down is not locally used for any rate limiting function but instead it is just passed to the LNS at the beginning when the session is first established. Mid-session changes on LAC via CoA are not propagated to the LNS.
- On L2TP LNS session:
  - Plain session: ignored. The rate is stored in the MIB table but no rate limiting action is taken. In other words, this parameter is internally excluded from rate calculations and advertisements. However, it is shown in the output of the relevant show commands.
- Bundle session: applied on all link sessions. The aggregate rate limit of the bundle is set to the minimum of the:
- CoA obtained local loop down rate multiplied by the number of links in the bundle
- The aggregate rate limit configured statically or obtained via CoA.

- Fragment length will be affected by this change. In case that interleaving is enabled on a single link bundle, the interleave interval will be affected.
- Non-L2TP: ignored. The rate is stored in the MIB table but no rate limiting action is taken. In other words, this parameter is internally excluded from rate calculations and advertisements. However, it will be shown in the output of the relevant show commands.

Similar behavior is exhibited if at mid-session, the parameters are changed via LUDB with the exception of the rate-down parameter in LAC. If this parameter is changed on the LAC, all sessions are disconnected.

### 10.3.16 Accounting

Accounting counters on the LNS include all packet overhead (wire overhead from the last mile). There is only one accounting session per bundle.

On the LAC, there is one accounting session per pppoe session (link).

In tunnel-accounting mode there is one accounting session per link.

On LNS only the stop-link of the last link of the bundle will carry all accounting data for the bundle.

### 10.3.17 Filters and Mirroring

Filters and mirrors (LI) are not supported on an MLPPPoX bundle on LAC. However, filters and ip-only mirror type are supported on the LNS.

### 10.3.18 PTA Considerations

Locally terminated MLPPPoX (PTA) solution is offered based on the LAC and the LNS hosted in the same system. An external loop (or VSM2) is used to connect the LAC to the LNS within the same box. The subscribers will be terminated on the LNS.

## 10.3.19 QoS Considerations

### 10.3.19.1 Dual-Pass

HQoS and LFI are performed in two stages that involve double traversal (dual-pass) of traffic through the carrier IOM and the BB-ISA. The following are the functions performed in each pass:

- In the first pass through the carrier IOM, traffic is marked (dot1p bits) as high or low priority. This will play crucial role in the execution of LFI in the BB-ISA.
- In the first pass through the BB-ISA this prioritization from the 1st step, will be an indication (along with the internally calculated fragment size) of whether the traffic will be interleaved (non MLPPP encapsulated) or not (MLPPP encapsulated). Consequently the BB-ISA will add the necessary padding related to last mile wire overhead to each packet. This padding will be used in the second pass on the carrier IOM to perform last mile wire based QoS functions.
- In the second pass through the carrier IOM, the last mile wire based HQoS will be performed based on the padding added in the first pass through the BB-ISA.
- In the second pass through the BB-ISA, previously added overhead will be stripped off and LFI/MLPPP encapsulation functions will be performed.

### 10.3.19.2 Traffic Prioritization in LFI

The delivery of high priority traffic within predefined delay bounds on a slow speed last mile link is ensured by proper QoS classification and prioritization. High priority traffic will be interleaved with low priority fragments on a single link MLPPPoX bundle with LFI enabled. The classification of traffic into proper (high or low priority) forwarding class is performed on the downstream ingress interface. However, traffic can be re-classified (re-mapped into another forwarding class) on the egress access interface of the carrier IOM, just before packets are transmitted to the BB-ISA for MLPPPoX processing. This can be achieved via QoS sap-egress policy referenced in the LNS sla-profile.

The priority of the forwarding class in regular QoS (on IOM) is determined by the properties (Expedited, non-expedited queue type, CIR and PIR rates) of the queue to which the forwarding class is mapped. In contracts, traffic prioritization in LFI domain (in BB-ISA) is determined by the outer dot1p bits that are set by the carrier IOM while transmitting packets towards the BB-ISA. The outer dot1p bits are marked based on the forwarding class information determined by classification/re-classification on ingress/carrier IOM. This marking of outer dot1p bits in the Ethernet header between the carrier IOM and the BB-ISA is fixed and defined in the default sap-egress LNS ESM policy 65537. The marking definition is as follows:

```
FC be -> dot1p 0
FC l2 -> dot1p 1
FC af -> dot1p 2
FC l1 -> dot1p 3
FC h2 -> dot1p 4
FC ef -> dot1p 5
FC h1 -> dot1p 6
FC nc -> dot1p 7
```

In LFI (on BB-ISA), dot1p bits [0,1,2 and 3] are considered low priority while dot1p bits (4,5,6 and 7) are considered high priority. Consequently, forwarding classes BE, L2, AF and L1 are considered low priority while forwarding classes H2, EF, H1 and NC are considered high priority. High priority traffic (assuming that the packet size does not exceed maximum fragment size) will be interleaved with low priority traffic.

The following describes the reference points in traffic prioritization for the purpose of LFI in the 7750 SR:

- Classification on downstream ingress interface (entrance point into the 7750 SR) - packets can be classified into one of the following eight forwarding classes: be, l2, af, l1, h2, ef, h1 and nc. Depending on the type of the ingress interface (access or network), traffic can be classified based on dot1p, exp, DSCP, TOS bits or ip-match criteria (dscp, dst-ip, dst-port, fragment, src-ip, src-port and protocol-id).
- Re-classification on downstream access egress interface between the carrier IOM and the BB-ISA - in the carrier IOM, downstream traffic can be re-classified into another forwarding class, just before it is forwarded to the BB-ISA. Re-classification on access egress is based on the same fields as on ingress except for the dot1p and exp bits since Ethernet or MPLS headers from ingress are not carried from ingress to egress.
- Marking on downstream access egress interface between the carrier IOM and the BB-ISA - once the forwarding class is available on the carrier IOM in the egress direction (towards BB-ISA), it will be used to mark outer dot1p bits in the new Ethernet header that will be used to transport the frame from the carrier IOM to the BB-ISA. The marking of the dot1p bits on the egress SAP between the carrier IOM and the BB-ISA cannot be changed for MLPPPoX even if the **no qos-marking-from-sap** command is configured under the sla-profile on egress.

### 10.3.19.3 Shaping Based on the Last Mile Wire Rates

Accurate QoS, amongst other things, require that the subscriber rates in the first mile on an MLPPPoX bundle be properly represented in the LNS. In other words, the rate limiting functions in the LNS must account for the last mile on-the-wire encapsulation overhead. The last mile encapsulation can be Ethernet or ATM.

For ATM in the last mile, the LNS will account for the following per fragment overhead:

- PID
- MLPPP encapsulation header
- ATM Fixed overhead (ATM encap + fixed AAL5 trailer)
- 48B boundary padding as part of AAL5 trailer
- 5B per each 48B of data in ATM cell.

In case of Ethernet encapsulation in the last mile, the overhead will be:

- PID
- MLPPP header per fragment
- Ethernet Header + FCS per fragment
- Preamble + IPG overhead per fragment

The **encap-offset** command under the sub-profile egress CLI node will be ignored in case of MLPPPoX. MLPPPoX rate calculation will be by default always based on the last mile wire overhead.

The HQoS rates (port-scheduler, aggregate-rate-limit and scheduler) on LNS are based on the wire overhead of the entity to which the HQoS is applied. For example, if the port-scheduler is managing bandwidth on the link between the BB-ISA and the carrier IOM, then the rate of such scheduler will account for the q-in-q Ethernet encapsulation on that link along with the preamble and inter packet gap (20B).

While virtual schedulers (attached via sub-profile) are supported on LNS for plain PPPoX sessions, they are not supported for MLPPPoX bundles. Only aggregate-rate-limit along with the port-scheduler can be used in MLPPPoX deployments.

### 10.3.19.4 Downstream Bandwidth Management on Egress Port

Bandwidth management on the egress physical ports (Physical Port 1 and Physical Port 2 in Figure 8) is performed at the egress port itself on the egress IOM instead on the carrier IOM. By default, the forwarding class (FC) information is preserved from network ingress to network egress. However, this can be changed via QoS configuration applied to the egress SAP of the carrier IOM towards the BB-ISA.

L2TP traffic originated locally in LNS can be marked via the router/service vprn->sgt-qos hierarchy.

### 10.3.20 Sub/Sla-Profile Considerations

#### Sub-profile

In the MLPPPoX case on LNS, multiple sessions are tied into the same subscriber aggregate-rate-limit via a sub-profile. The consequence is that the aggregate rate of the subscriber can be adjusted dynamically depending on the advertised link speed in the last mile and the number of links in the bundle. Shaping in the LNS is performed per the entire MLPPPoX bundle (subscriber) rather than per individual member links within the bundle. The exception is obviously a MLPPPoX bundle with the single member link (interleaving case) where the relationship between the session and the MLPPPoX bundle is 1:1.

In the LAC, the subscriber aggregate rate cannot be dynamically changed based on the number of links in the bundle and their rate. The LAC has no notion of MLPPPoX bundles. However, multiple sessions that in reality belong to an MLPPPoX bundle under the subscriber are shaped as an aggregate (agg-rate-limit under the sub-profile). This in essence yields the same shaping behavior as on LNS.

#### Sla-profile

Sessions within the MLPPPoX bundle in LNS share a single sla-profile instances (queues).

In the LAC, as long as the sessions within the subscriber6 are on the same SAP, they can also share the same sla-profile. This will be the case in MLPPPoX.

The manner in which sub/sla-profile are applied to MLPPPoX bundles and the individual sessions within results in aggregate shaping per MLPPPoX bundle as well as allocation of unique set of queues per MLPPPoX bundle. This is valid irrespective of the location where shaping is executed (LAC or LNS). Other vendors may have implemented shaping per session within the bundle and this is something that needs to be taken into consideration during the migration process.

## 10.3.21 Example of MLPPPoX Session Setup Flow

### LAC behavior

- A new PPP(oEoA) session request will arrive to the LAC (PADI or LCP Conf Req).
- The LAC will negotiate PADx session if applicable.
- The LAC may negotiate MLPPPoX LCP phase with its own endpoint discriminator, or it may reject MLPPPoX specific options in LCP if MLPPPoX on the LAC is disabled (i.e. no accept-mrru in the LAC's ppp-policy). If MLPPPoX options (seq num header format, ED, MRRU) are rejected, the assumption is that the client will renegotiate plain PPP(oEoA) session with the LAC.
- Once LCP (MLPPPoX capable or not) is negotiated, the session will be authenticated (PAP/CHAP).
- Upon successful authentication, an L2TP tunnel will be identified to which the session belongs.
- If the session is a non-L2TP session (PTA MLPPPoX capable session for which the tunnel cannot be determined), the session will be terminated.
- Otherwise, the QoS constructs will be created for the subscriber hosts: the session will be assigned to a sub/sla-profiles.
- The session LCP parameters will be sent to the LNS via call management messages.
- If another LCP session is requested on the same bundle, the LAC will create a new LCP session and join this session to the existing subscriber as another host. In other words, the LAC is bundle agnostic and the two sessions will appear as two hosts under the same subscriber.

The following assumes that MLPPPoX is configured on the LNS under the L2TP group or the tunnel hierarchy.

### LNS behavior

- The LNS have the option to accept the LCP parameters or to reject them and start renegotiating LCP parameters directly with the client.
- If the LNS choose to renegotiate LCP parameters with the client directly, this renegotiation will be completely transparent to the LAC by the means of a T-bit (control vs. data) in the L2TP header. LCP will be renegotiated on the LNS with all the options necessary to support MLPPPoX. Endpoint Discriminator is not mandatory in the MLPPPoX negotiation. If the client rejects it, the LNS must still be able to negotiate MLPPPoX capable session (same is valid for the LAC). If the client's endpoint discriminator is invalid (bad format, invalid class, etc.), the 7750 SR will not negotiate MLPPPoX and instead a plain PPP session will be created.



- If the LNS is configured to accept the LCP Proxy parameters, the LNS will determine the capability of the client.

If there is no indication of MLPPPoX capability in the Proxy LCP (not even in the original ConfReq), the LNS may accept plain (non MLPPPoX capable) LCP session or renegotiate from scratch the non MLPPPoX capable session.

If there is an indication of MLPPPoX capability in the Proxy LCP (either completely negotiated on the LAC or at least attempted from the client), the LNS will try to either accept the MLPPPoX negotiated session by the LAC or renegotiate the MLPPPoX capable session directly with the client.

If the LCP Proxy parameters with MLPPPoX capability are accepted by the LNS, then the endpoint as negotiated on the LAC will also be accepted.

- Once the MLPPPoX capable LCP session is negotiated or accepted, authentication can be performed on the LNS. Authentication on the LNS can be restarted (CHAP challenge/response with the client), or accepted (chap challenge/response accepted and verified by the LNS via RADIUS).
- If the authentication is successful, depending on the evaluation of the parameters negotiated up to this point a new MLPPPoX bundle will be created or an existing MLPPPoX bundle will be joined. In case that a new bundle is established, the QoS constructs for the subscriber(-host) will be created (sub/sla-profile). Session negotiation will advance to IPCP phase.
- The decision whether a new session should join an existing MLPPPoX bundle, or trigger creation of a new one is governed by RFC 1990, *The PPP Multilink Protocol (MP)*, section 5.1.3, page 16, cases 1,2,3, and 4.
- Interleaving is supported only on MLPPPoX bundles with single session in them.

## 10.3.22 Other Considerations

- IPv6 is supported.
- AA is supported at LNS where full IP packets can be redirected via AA policies.
- Intra-chassis redundancy is supported:
  - CPM — stateful failover
  - BB-ISA — non-stateful failover

## 10.4 Configuration Notes

MLPPP in subscriber management context is supported only over ATM, Ethernet over ATM or plain Ethernet transport (MLPPPoX). Native MLPPP over PPP/HDLC links is supported outside of the subscriber management context on the ASAP MDA.

MLPPPoX is supported only on LNS.

Interleaving is supported only on MLPPPoX bundles with a single member link. If more than one link is present in an MLPPPoX bundle, the interleaving will be automatically disabled and a SNMP trap will be generated. The MIB for this even is defined as `tmnxMlpppBundleIndicatorsChange`.

If MLPPPoX is enabled on LNS, the load balancing mode between the BB-ISAs within the group should be set to per tunnel. This will ensure that all sessions of the same MLPPPoX bundle are terminated on the same BB-ISA. On the LAC, sessions of the same bundle are setup in the same tunnel.

Virtual schedulers are not supported on MLPPPoX tunnels on LNS. However, aggregate-rate-limit is supported.

The aggregate-rate-limit on LNS will be automatically adjusted to the minimum value of:

- configured aggregate-rate-limit
- minimum last mile rate (obtained via LUDB, RADIUS or PPPoE tags) multiplied by the number of links in the bundle.

The aggregate-rate-limit on the LAC is not adjusted automatically. Therefore, if configured it should be set to a high value and thus the traffic treatment should rely on QoS performed on the LNS.

The rate (rate-down information) of the member links within the bundle must be the same. Otherwise the lowest rate is selected and applied to all member links.

A single CoA for a rate change (Alc-Access-Loop-Rate-Down) of an individual link in an MLPPPoX bundle will modify rates of all links in the bundle. This is applicable on LNS only.

The range of supported last mile rate (rate-down information) for the member links on an MLPPPoX session is 1 kb/s — 100 Mb/s. On the LNS the last mile rate can be obtained:

- From the LAC via Tx-Connect-Speed AVP or by standard L2TP encoding as described in the RFC 5515, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*.

- From the LAC via LUDB or RADIUS
- Directly on the LNS via LUDB or RADIUS.

The session will fail to come up if the obtained rate-down information is outside of the allowable range (1 kb/s — 100 Mb/s).

A session within the MLPPPoX bundle will be terminated if the rate-down information for the session is out of bounds (1kb/s — 100 Mb/s).

If a member link in the last mile fails, traffic will be blackholed until the LNS is notified of this failure. The failure detection in the LNS relies on PPP keepalives.

Shaping is performed per MLPPPoX bundle and not individually per member links.

If encapsulation overhead associated with fragmentation is too large in comparison to payload, the fragments will be sized based on the encapsulation overhead (to increase link efficiency) rather than on maximum transmission delay.

There can be only a single MLPPPoX bundle per subscriber.

MLPPPoX bundles and non-MLPPPoX (plain L2TP PPPE) sessions cannot coexist under the same subscriber.

Filters and mirrors (LI) are not supported on MLPPPoX bundles on LAC.

**ip-only** type mirrors are supported on MLPPPoX bundles.

In MLPPP scenario, downstream traffic is traversing Carrier IOM and BB-ISA twice. This is referred to as dual-pass and effectively cuts the throughput for MLPPP in half (for example, 5Gb/s of MLPPP traffic on a 10Gb/s capable BB-ISA).



## 10.5 L2TP Network Server Command Reference

### 10.5.1 Command Hierarchies

#### 10.5.1.1 ISA Commands

```
config
 — isa
 — ins-group ins-group-id [create]
 — no ins-group ins-group-id
 — description description-string
 — no description
 — mda mda-id [drain]
 — no mda mda-id
 — port-policy policy-name
 — no port-policy
 — [no] shutdown

config
 — port-policy policy-name [create]
 — no port-policy policy-name
 — description description-string
 — no description
 — egress-scheduler-policy port-sched-plcy
 — no egress-scheduler-policy
```

#### 10.5.1.2 MLPPP on LNS Commands

```
config
 — subscriber-mgmt
 — local-user-db local-user-db-name [create]
 — no local-user-db local-user-db-name
 — ppp
 — host host-name [create]
 — no host host-name
 — [no] access-loop-encapsulation
 — encap-offset [type encap-type]
 — no encap-offset
 — rate-down rate
 — no rate-down
 — ppp-policy ppp-policy-name [create]
 — no ppp-policy ppp-policy-name
 — mlppp
 — [no] accept-mrru
```

```

— [no] short-sequence-numbers

config
— router
 — l2tp
 — group tunnel-group-name [create]
 — group tunnel-group-name [create] [protocol protocol]
 — no group tunnel-group-name
 — load-balance-method {per-session | per-tunnel}
 — no load-balance-method
 — mlppp
 — endpoint ip ip-address
 — endpoint mac ieee-address
 — endpoint system-ip
 — endpoint system-mac
 — no endpoint
 — [no] interleave
 — max-fragment-delay milliseconds
 — no max-fragment-delay
 — max-links max-links
 — no max-links
 — reassembly-timeout {{100 | 1000} milliseconds}
 — no reassembly-timeout
 — tunnel tunnel-name [create]
 — no tunnel tunnel-name
 — load-balance-method {per-session | per-tunnel}
 — no load-balance-method
 — mlppp
 — admin-state {up | down}
 — no admin-state
 — endpoint ip ip-address
 — endpoint mac ieee-address
 — endpoint system-ip
 — endpoint system-mac
 — no endpoint
 — interleave {always | never}
 — no interleave
 — max-fragment-delay milliseconds
 — no max-fragment-delay
 — max-links max-links
 — no max-links
 — reassembly-timeout {{100 | 1000} milliseconds}
 — no reassembly-timeout

config
— service
 — vprn
 — l2tp
 — group tunnel-group-name [create]
 — group tunnel-group-name [create] [protocol protocol]
 — no group tunnel-group-name
 — load-balance-method {per-session | per-tunnel}
 — no load-balance-method
 — mlppp

```

- endpoint ip *ip-address*
- endpoint mac *ieee-address*
- endpoint system-ip
- endpoint system-mac
- no endpoint
- [no] **interleave**
- max-fragment-delay *milli-seconds*
- no max-fragment-delay
- max-links *max-links*
- no max-links
- reassembly-timeout {{100 | 1000} milliseconds}
- no reassembly-timeout
- tunnel *tunnel-name* [create]
- no tunnel *tunnel-name*
  - load-balance-method {per-session | per- tunnel}
  - no load-balance-method
  - mlppp
    - admin-state {down | up}
    - no admin-state
    - endpoint ip *ip-address*
    - endpoint mac *ieee-address*
    - endpoint system-ip
    - endpoint system-mac
    - no endpoint
    - interleave {always | never}
    - no interleave
    - max-fragment-delay *milli-seconds*
    - no max-fragment-delay
    - max-links *max-links*
    - no max-links
    - reassembly-timeout {{100 | 1000} milliseconds}
    - no reassembly-timeout

## 10.5.2 Command Descriptions

### 10.5.2.1 Generic Commands

description

|         |                                                         |
|---------|---------------------------------------------------------|
| Syntax  | description <i>description-string</i><br>no description |
| Context | config>isa>Ins-group<br>config>port-policy              |

---

|                    |                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command creates a text description which is stored in the configuration file to help identify the content of the entity.</p> <p>The <b>no</b> form of the command removes the string from the configuration.</p>                                        |
| <b>Parameters</b>  | <p><i>string</i> — The description character string. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> |

shutdown

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] shutdown</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>isa>Ins-group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the <b>no shutdown</b> command.</p> <p>The <b>shutdown</b> command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.</p> |

10.5.2.2 LNS Commands

Ins-group

|                    |                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>Ins-group</b> <i>Ins-group-id</i> [ <b>create</b> ]<br><b>no Ins-group</b> <i>Ins-group-id</i>                                                                                                                                                                                                  |
| <b>Context</b>     | config>isa                                                                                                                                                                                                                                                                                         |
| <b>Description</b> | <p>This command configures an LNS group.</p> <p>The <b>no</b> form of the command removes the LNS group ID from the configuration.</p>                                                                                                                                                             |
| <b>Default</b>     | none                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | <p><i>Ins-group-id</i> — Specifies the LNS group identifier.</p> <p><b>Values</b>      1 to 4</p> <p><b>create</b> — Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled/disabled in the <b>environment&gt;create</b> context.</p> |



mda

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>mda</b> <i>mda-id</i> [ <b>drain</b> ]<br><b>no mda</b> <i>mda-id</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Context     | config>isa>Ins-group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description | <p>This command configures an ISA LNS group MDA.</p> <p>The no form of the command removes the MDA ID from the LNS group configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Parameters  | <p><i>mda-id</i> — Specifies the MDA identifier.</p> <div><div>Values</div><div><div>mda-id: <i>slot/mda</i></div><div>slot: 1 to 10</div><div>mda: 1, 2</div></div></div> <p><b>drain</b> — Prevents new L2TP sessions being associated with the ISA. If an ISA is removed from the Ins-group or if the Ins-group be shutdown all associated L2TP sessions will be immediately terminated (and L2TP CDN messages sent to the L2TP peer). View show commands to determine which ISA is terminating which session (<b>show router l2tp session</b>).</p> |

port-policy

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax      | <b>port-policy</b> <i>policy-name</i><br><b>no port-policy</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Context     | config>isa>Ins-group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Description | <p>This command enables policies referenced in the <b>config&gt;port-policy</b> context to be created under <b>ports</b>. These are the ports that link the carrier IOM to the ISA, and are hidden within the system (they cannot be created through the CLI). They are created automatically. Use the <b>show port</b> command to view information.</p> <p>Currently only the port scheduler policy is supported. Each Ins-esm port in the Ins-group receives an independent port scheduler instance. The port schedulers are instantiated in the carrier IOM on the Ins-esm ports that carry PPPoE traffic in the downstream direction towards the ISA before the PPPoE traffic is L2TP encapsulated.</p> <p>The <b>no</b> form of the command removes the policy name from the configuration.</p> |
| Default     | no port-policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Parameters  | <p><i>policy-name</i> — Specifies the port policy of this LNS group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## port-policy

|                    |                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>port-policy</b> <i>policy-name</i> [ <b>create</b> ]<br><b>no port-policy</b> <i>policy-name</i>                                                                                                                                                 |
| <b>Context</b>     | config                                                                                                                                                                                                                                              |
| <b>Description</b> | <p>This command instantiates a port policy manager that applies policies (port scheduler) to be hidden, dynamically created ports for WLAN GW/LNS/NAT.</p> <p>The <b>no</b> form of the command removes the policy name from the configuration.</p> |
| <b>Parameters</b>  | <i>policy-name</i> — Specifies the port policy name.                                                                                                                                                                                                |

## egress-scheduler-policy

|                    |                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>egress-scheduler-policy</b> <i>port-sched-plcy</i><br><b>no egress-scheduler-policy</b>                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>port-policy                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b> | <p>This command references a port scheduler policy that is defined under the <b>configure&gt;qos&gt;port-scheduler-policy&gt;</b> hierarchy. Port schedulers are instantiated on carrier IOMs towards all ISAs that are part of the lns-group.</p> <p>The no form of the command removes the port scheduler policy from the configuration.</p> |
| <b>Default</b>     | no egress-scheduler-policy                                                                                                                                                                                                                                                                                                                     |
| <b>Parameters</b>  | <i>port-sched-plcy</i> — Specifies the egress scheduler policy up to 32 characters.                                                                                                                                                                                                                                                            |

### 10.5.2.3 Network Address Translation (NAT) Commands

## nat-group

|                    |                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>nat-group</b> <i>nat-group-id</i> [ <b>create</b> ]<br><b>no nat-group</b> <i>nat-group-id</i>                                |
| <b>Context</b>     | config>isa                                                                                                                       |
| <b>Description</b> | <p>This command configures an ISA NAT group.</p> <p>The <b>no</b> form of the command removes the ID from the configuration.</p> |
| <b>Default</b>     | none                                                                                                                             |

**Parameters**    *nat-group* — Specifies the ISA NAT group ID.

**Values**        1 to 4

active-mda-limit

**Syntax**        **active-mda-limit** *number*  
                  **no active-mda-limit**

**Context**        config>isa>nat-group

**Description**    This command configures the ISA NAT group maximum number of MDA.

                  The **no** form of the command removes the number from the configuration.

**Default**        no active-mda-limit

**Parameters**    *number* — Specifies the active MDA limit.

**Values**        1 to 6

mda

**Syntax**        [**no**] **mda** *mda-id*

**Context**        config>isa>nat-group

**Description**    This command configures an ISA NAT group MDA.

**Parameters**    *mda-id* — Specifies the MDA ID in the *slot/mda* format.

**Values**        slot: 1 to 10

**Values**        mda: 1 to 2

session-limits

**Syntax**        **session-limits**

**Context**        config>isa>nat-group

**Description**    This command configures the ISA NAT group session limits.

reserved

**Syntax**        **reserved** *num-sessions*  
                  **no reserved**

|                    |                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Context</b>     | config>isa>nat-group>session-limits                                                                                     |
| <b>Description</b> | This command configures the number of sessions per block that will be reserved for prioritized sessions.                |
| <b>Default</b>     | no reserved                                                                                                             |
| <b>Parameters</b>  | <i>num-sessions</i> — Specifies the number of sessions reserved for prioritized sessions.<br><b>Values</b> 0 to 4194303 |

watermarks

|                    |                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>watermarks high <i>percentage</i> low <i>percentage</i></b><br><b>no watermarks</b>                                                                                                                                                                                                                    |
| <b>Context</b>     | config>isa>nat-group>session-limits                                                                                                                                                                                                                                                                       |
| <b>Description</b> | This command configures the ISA NAT group watermarks.                                                                                                                                                                                                                                                     |
| <b>Default</b>     | no watermarks                                                                                                                                                                                                                                                                                             |
| <b>Parameters</b>  | <b>high <i>percentage</i></b> — Specifies the high watermark of the number of sessions for each MDA in this NAT ISA group.<br><b>Values</b> 1 to 100<br><b>low <i>percentage</i></b> — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA group.<br><b>Values</b> 0 to 99 |

10.5.2.4 MLPPP on LNS Commands

accept-mrru

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] accept-mrru                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Context</b>     | config>subscr-mgt>ppp-policy>mlppp                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>This command is applicable only to LAC. MRRU option is an indication that the session is of MLPPPoX type. The 7750 SR LAC will never initiate MRRU option in LCP negotiation process. However, it will respond to MRRU negotiation request by the client.</p> <p>This command provides an option to specifically enable or disable negotiation of MLPPPoX on a capture SAP level or on a group-interface level.</p> |
| <b>Default</b>     | no accept-mrru to The MRRU option in LCP will not be negotiated by LAC.                                                                                                                                                                                                                                                                                                                                                |

## admin-state

|                    |                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>admin-state {down   up}</b><br><b>no admin-state</b>                                                                                                                                                                                                                                                                                             |
| <b>Context</b>     | config>router>l2tp>group>tunnel>mlppp<br>config>service>vpn>l2tp>group>tunnel>mlppp                                                                                                                                                                                                                                                                 |
| <b>Description</b> | <p>This command is applicable only to LNS.</p> <p>The tunnel can be explicitly activated (assuming that the parent group is in a no shutdown state) or deactivated by the <b>up</b> and <b>down</b> keywords.</p> <p>If case that there is no admin-state configured, the tunnel will inherit its administrative state from its parent (group).</p> |
| <b>Default</b>     | no admin-state — Tunnel administrative state is inherited from the group.                                                                                                                                                                                                                                                                           |
| <b>Parameters</b>  | <p><b>up</b> — Tunnel is administratively up.</p> <p><b>down</b> — Tunnel is administratively down.</p>                                                                                                                                                                                                                                             |

## encap-offset

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |                                  |            |                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------|------------|-----------------------------|
| <b>Syntax</b>      | <b>encap-offset [type <i>encap-type</i>]</b><br><b>no encap-offset</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |                                  |            |                             |
| <b>Context</b>     | config>subscr-mgmt>loc-user-db>ppp>host>access-loop-encapsulation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |                                  |            |                             |
| <b>Description</b> | <p>This command is applicable within the LAC/LNS context. It provides the last mile link encapsulation information that is needed for proper (shaping) rate calculations and interleaving delay in the last mile.</p> <p>The encapsulation value will be taken from the following sources in the order of priority:</p> <ul style="list-style-type: none"> <li>• Statically provisioned value in local user database (LUDB).</li> <li>• RADIUS</li> <li>• PPPoE tags on LAC or ICRQ message (RFC 5515) on LNS</li> </ul> <p>In case that the encapsulation information is not provided by any of the existing means (LUDB, RADIUS, AVP signaling, PPPoE Tags), then by default pppoea-null encapsulation will be in effect.</p> <p>The following values are supported encapsulation values on LNS in the 7750 SR.</p> <p>encap-type:</p> <table> <tr> <td>pppoa-llc</td><td>LLC (NLPID) PPPoA encapsulation.</td></tr> <tr> <td>pppoa-null</td><td>VC-MUX PPPoA encapsulation.</td></tr> </table> | pppoa-llc | LLC (NLPID) PPPoA encapsulation. | pppoa-null | VC-MUX PPPoA encapsulation. |
| pppoa-llc          | LLC (NLPID) PPPoA encapsulation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |                                  |            |                             |
| pppoa-null         | VC-MUX PPPoA encapsulation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |                                  |            |                             |

|                  |                                                                    |
|------------------|--------------------------------------------------------------------|
| pppoeoa-llc      | LLC/SNAP based bridged Ethernet PPPoEoA encapsulation without FCS. |
| pppoeoa-llc-fcs  | LLC/SNAP based bridged Ethernet PPPoEoA encapsulation with FCS.    |
| pppoeoa-null     | VC-MUX PPPoEoA encapsulation without FCS.                          |
| pppoeoa-null-fcs | VC-MUX PPPoEoA encapsulation with FCS.                             |
| pppoe            | PPPoE encapsulation.                                               |
| pppoe-tagged     | Tagged PPPoE Encapsulation.                                        |

The values are not supported encapsulation values on LNS in the 7750 SR.

pppoeoa-llc-tagged  
pppoeoa-llc-tagged-fcs  
pppoeoa-null-tagged  
pppoeoa-null-tagged-fcs  
ipoa-llc  
ipoa-null  
ipoeoa-llc  
ipoeoa-llc-fcs  
ipoeoa-llc-tagged  
ipoeoa-llc-tagged-fcs  
ipoeoa-null  
ipoeoa-null-fcs  
ipoeoa-null-tagged  
ipoeoa-null-tagged-fcs  
ipoe  
ipoe-tagged

**Default** no encap-offset No offset is configured.

rate-down

|                    |                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>rate-down</b> <i>rate</i><br><b>no rate-down</b>                                                                                                                                  |
| <b>Context</b>     | config>subscr-mgmt>loc-user-db>ppp>host>access-loop-encapsulation                                                                                                                    |
| <b>Description</b> | This command is applicable to LAC and LNS. It provides the last mile link rate in the downstream direction that is needed for proper shaping and calculating the interleaving delay. |

The rate information in the last mile will be taken from the following sources in the order of priority:

- Statically provisioned value in local user database (LUDB).
- RADIUS.
- PPPoE tags on LAC or ICRQ message (RFC 5515) /ICCN message (TX Connect Seed) on LNS.

|                   |                                                                           |
|-------------------|---------------------------------------------------------------------------|
| <b>Default</b>    | no rate-down                                                              |
| <b>Parameters</b> | <i>rate</i> — Specifies last mile link downstream rate in the access loop |
| <b>Values</b>     | 1 to 100000 kb/s                                                          |

## endpoint

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>endpoint ip</b> <i>ip-address</i><br><b>endpoint mac</b> <i>ieee-address</i><br><b>endpoint system-ip</b><br><b>endpoint system-mac</b><br><b>no endpoint</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>router>l2tp>group>mlppp<br>config>router>l2tp>group>tunnel>mlppp<br>config>service>vprn>l2tp>group>mlppp<br>config>service>vprn>l2tp>group>tunnel>mlppp<br>config>subscr-mgt>ppp-policy>mlppp                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b> | <p>When configured under the l2tp hierarchy, this command is applicable to LNS.</p> <p>Within the ppp-policy, this command is applicable only to LAC.</p> <p>The endpoint, according to RFC 1990, represents the system transmitting the packet. It is used during MLPPPoX negotiation phase to distinguish this peer from all others.</p> <p>In the case that the client rejects the endpoint option during LCP negotiation, the LAC and the LNS must be able to negotiate the LCP session without the endpoint option.</p> <p>The <b>no</b> form of this command disables sending endpoint option in LCP negotiation.</p> |
| <b>Default</b>     | no endpoint                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <b>ip</b> <i>ip-address</i> — Specifies the IPv4 address (class 2)<br><b>system-ip</b> — Specifies to use the system IPv4 address (class 2)<br><b>mac</b> <i>ieee-address</i> — Specifies the MAC address of the interface (class 3).<br><b>system-mac</b> — Specifies to use the MAC address of the system (class 3)                                                                                                                                                                                                                                                                                                       |

---

## interleave

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>[no] interleave</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Context</b>     | config>router>l2tp>group>mlppp<br>config>service>vprn>l2tp>group>mlppp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b> | <p>This command is applicable only to LNS. Interleaving is supported only on MLPPPoX bundles that contain a single member link. If more than one link is present in the MLPPPoX bundle, interleaving will be automatically disabled and a TRAP/log (tmnxMlpppBundleIndicatorsChange) will be generated.</p> <p>The minimum supported rate of the link on which interleaving is performed is 1 kb/s.</p> <p>If configured at this level, interleaving will be enabled on all tunnels within the group, unless it is explicitly disable per tunnel.</p> |
| <b>Default</b>     | no interleave — Interleaving per group is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## interleave

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>interleave {always   never}</b><br><b>no interleave</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Context</b>     | config>router>l2tp>group>tunnel>mlppp<br>config>service>vprn>l2tp>group>tunnel>mlppp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>This command is applicable only to LNS. Interleaving is supported only on MLPPPoX bundles that contain a single member link. If more than one link is present in the MLPPPoX bundle, interleaving will be automatically disabled and a TRAP/log (tmnxMlpppBundleIndicatorsChange ) will be generated.</p> <p>The minimum supported rate of the link on which interleaving is performed is 1 kb/s.</p> <p>Interleaving configured on this level will overwrite the configuration option under the group hierarchy. If the no form of the command is configured for interleaving at this level, the interleaving configuration will inherit the configuration option configured under the l2tp group.</p> |
| <b>Default</b>     | no interleave — Interleaving configuration is inherited from the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Parameters</b>  | <p><b>always</b> — Always perform interleaving on single linked MLPPPoX sessions within this tunnel, regardless of the configuration option for interleaving under the group level.</p> <p><b>never</b> — Never perform interleaving on single linked MLPPPoX sessions within this tunnel, regardless of the configuration option for interleaving under the group level.</p>                                                                                                                                                                                                                                                                                                                              |



---

## load-balance-method

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>load-balance-method</b> { <b>per-session</b>   <b>per-tunnel</b> }<br><b>no load-balance-method</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Context</b>     | config>router>l2tp>group<br>config>router>l2tp>group>tunnel<br>config>service>vprn>l2tp>group<br>config>service>vprn>l2tp>group>tunnel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b> | <p>This command is applicable only to LNS. By default traffic load balancing between the BB-ISAs is based on sessions. Each session is individually assigned to an BB-ISA during session establishment phase.</p> <p>By introducing MLPPPoX, all sessions of a bundle must be terminated on the same LNS BB-ISA. This is necessary for two reasons:</p> <ul style="list-style-type: none"><li>• QoS in the carrier IOM has a uniform view of the subscriber</li><li>• a single BB-ISA is responsible for MLPPPoX encapsulation/fragmentation for a given bundle.</li></ul> <p>Therefore, if fragmentation is enabled, load-balancing per tunnel must be configured. In the per tunnel load-balancing mode, all sessions within the same tunnel are terminated on the same LNS BB-ISA.</p> <p>In the case that we have MLPPPoX sessions with a single member link, both load-balancing methods are valid.</p> <p>The <b>no</b> form of this command set the per session load balancing.</p> |
| <b>Default</b>     | load-balance-method session — Per session load balancing is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Parameters</b>  | <b>session</b> — Traffic load balancing between the LNS BB-ISAs is based on individual PPPoE sessions.<br><b>tunnel</b> — Traffic load balancing between the LNS BB-ISAs is based on tunnels.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## max-fragment-delay

|                    |                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>max-fragment-delay</b> <i>milliseconds</i><br><b>no max-fragment-delay</b>                                                                                  |
| <b>Context</b>     | config>router>l2tp>group>mlppp<br>config>router>l2tp>group>tunnel>mlppp<br>config>service>vprn>l2tp>group>mlppp<br>config>service>vprn>l2tp>group>tunnel>mlppp |
| <b>Description</b> | This command is applicable only to LNS. It determines the maximum fragment delay caused by the transmission that will be imposed on a link.                    |

Fragmentation can be used to interleave high priority packet in-between low priority fragments on a MLPPPoX session with a single link or on a MLPPPoX session with multiple links to better load balance traffic over multiple member links.

|                   |                                                                |
|-------------------|----------------------------------------------------------------|
| <b>Default</b>    | no max-fragment-delay — Fragmentation is disabled.             |
| <b>Parameters</b> | <i>milliseconds</i> — Specifies the interval, in milliseconds. |
| <b>Values</b>     | 5 to 1000                                                      |

## max-links

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>max-links</b> <i>max-links</i><br><b>no max-links</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Context</b>     | config>router>l2tp>group>mlppp<br>config>router>l2tp>group>tunnel>mlppp<br>config>service>vprn>l2tp>group>mlppp<br>config>service>vprn>l2tp>group>tunnel>mlppp                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <p>This command is applicable only to LNS. It determines the maximum number of links that can be put in a bundle.</p> <p>Any attempt of a session to join a bundle that is above the max-link limit will be rejected.</p> <p>If interleaving is configured, it is recommended that max-links be set to 1 or a version of the command is used (no max-links). Both have the same effect.</p> <p>The configuration under the tunnel hierarchy will override the configuration under the group hierarchy.</p> <p>The <b>no</b> form of this command limits the number of links in the bundle to 1.</p> |
| <b>Default</b>     | no max-links — A single link per bundle is allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Parameters</b>  | <i>max-links</i> — Specifies the maximum number of links in a bundle.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Values</b>      | 1 to 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## reassembly-timeout

|                |                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>  | <b>reassembly-timeout</b> {{100   1000} <i>milliseconds</i> }<br><b>no reassembly-timeout</b>                                                                  |
| <b>Context</b> | config>router>l2tp>group>mlppp<br>config>router>l2tp>group>tunnel>mlppp<br>config>service>vprn>l2tp>group>mlppp<br>config>service>vprn>l2tp>group>tunnel>mlppp |

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <p>This command is applicable only to LNS. It determines the time during which the LNS keeps fragments of the same packet in the buffer before it discards them. The assumption is that if the fragments do not arrive within certain time, the chance is that they were lost somewhere in the network. In this case the partial packet cannot be reassembled and all fragments that has arrived up to this point and are stored in the buffer will be discarded in order to free up the buffer. Otherwise, a condition will arise in which partial packets will be held in the buffer until the buffer is exhausted.</p> <p>The configuration under the tunnel hierarchy will override the configuration under the group hierarchy.</p> <p>The <b>no</b> form of this command also sets the time-out to 1000ms.</p> |
| <b>Default</b>     | reasembly-timeout 1000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Parameters</b>  | {{100   1000} milliseconds} — Specifies the reassembly timeout value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## short-sequence-numbers

|                    |                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | [no] short-sequence-numbers                                                                                                                                                                                                                                |
| <b>Context</b>     | config>subscr-mgt>ppp-policy>mlppp                                                                                                                                                                                                                         |
| <b>Description</b> | This command enables a peer request to send short sequence numbers. This command is applicable to LAC and LNS. By default, MLPPPoX will negotiate 24bit long sequence numbers. This command allows this to be changed to shorter, 12-bit sequence numbers. |
| <b>Default</b>     | short-sequence-numbers                                                                                                                                                                                                                                     |



## 11 Standards and Protocol Support



**Note:** The information presented is subject to change without notice.

Nokia assumes no responsibility for inaccuracies contained herein.

### Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

### Application Assurance (AA)

3GPP Release 12 (ADC rules over Gx interfaces)

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

### Asynchronous Transfer Mode (ATM)

AF-ILMI-0065.000, *Integrated Local Management Interface (ILMI) Version 4.0*

AF-PHY-0086.001, *Inverse Multiplexing for ATM (IMA) Specification Version 1.1*

AF-TM-0121.000, *Traffic Management Specification Version 4.1*

AF-TM-0150.00, *Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR*

GR-1113-CORE, *Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1*

GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3*

ITU-T I.432.1, *B-ISDN user-network interface - Physical layer specification: General characteristics (02/99)*

ITU-T I.610, *B-ISDN operation and maintenance principles and functions (11/95)*

RFC 1626, *Default IP MTU for use over ATM AAL5*

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

### Bidirectional Forwarding Detection (BFD)

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*

RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

## **Border Gateway Protocol (BGP)**

draft-hares-idr-update-attr-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-guidelines-08, *Best Practices for Advertisement of Multiple Paths in IBGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*

draft-ietf-idr-bgp-flowspec-oid-03, *Revised Validation Procedure for BGP Flow Specifications*

draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*

draft-ietf-idr-bgp-optimal-route-reflection-10, *BGP Optimal Route Reflection (BGP-ORR)*

draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*

draft-ietf-idr-flowspec-interfaceset-03, *Applying BGP flowspec rules on a specific interface set*

draft-ietf-idr-flowspec-path-redirect-05, *Flowspec Indirection-id Redirect (localised ID)*

draft-ietf-idr-flowspec-redirect-ip-02, *BGP Flow-Spec Redirect to IP Action*

draft-ietf-idr-link-bandwidth-03, *BGP Link Bandwidth Extended Community*

draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*

draft-uttaro-idr-bgp-persistence-03, *Support for Long-lived BGP Graceful Restart*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1997, *BGP Communities Attribute*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 2918, *Route Refresh Capability for BGP-4*

RFC 3107, *Carrying Label Information in BGP-4*

RFC 3392, *Capabilities Advertisement with BGP-4*

RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

RFC 4360, *BGP Extended Communities Attribute*

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*

---

RFC 4486, *Subcodes for BGP Cease Notification Message*  
RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*  
RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/  
MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual  
Private Networks (VPNs)*  
RFC 4724, *Graceful Restart Mechanism for BGP (helper mode)*  
RFC 4760, *Multiprotocol Extensions for BGP-4*  
RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge  
Routers (6PE)*  
RFC 4893, *BGP Support for Four-octet AS Number Space*  
RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*  
RFC 5065, *Autonomous System Confederations for BGP*  
RFC 5291, *Outbound Route Filtering Capability for BGP-4*  
RFC 5396, *Textual Representation of Autonomous System (AS) Numbers (asplain)*  
RFC 5549, *Advertising IPv4 Network Layer Reachability Information with an IPv6  
Next Hop*  
RFC 5575, *Dissemination of Flow Specification Rules*  
RFC 5668, *4-Octet AS Specific BGP Extended Community*  
RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4*  
RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*  
RFC 6811, *Prefix Origin Validation*  
RFC 6996, *Autonomous System (AS) Reservation for Private Use*  
RFC 7311, *The Accumulated IGP Metric Attribute for BGP*  
RFC 7607, *Codification of AS 0 Processing*  
RFC 7674, *Clarification of the Flowspec Redirect Extended Community*  
RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE)  
Information Using BGP*  
RFC 7854, *BGP Monitoring Protocol (BMP)*  
RFC 7911, *Advertisement of Multiple Paths in BGP*  
RFC 7999, *BLACKHOLE Community*  
RFC 8092, *BGP Large Communities Attribute*

## **Circuit Emulation**

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet  
(SAToP)*  
RFC 5086, *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation  
Service over Packet Switched Network (CESoPSN)*

---

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

## **Ethernet**

IEEE 802.1AB, *Station and Media Access Control Connectivity Discovery*

IEEE 802.1ad, *Provider Bridges*

IEEE 802.1ag, *Connectivity Fault Management*

IEEE 802.1ah, *Provider Backbone Bridges*

IEEE 802.1ak, *Multiple Registration Protocol*

IEEE 802.1aq, *Shortest Path Bridging*

IEEE 802.1ax, *Link Aggregation*

IEEE 802.1D, *MAC Bridges*

IEEE 802.1p, *Traffic Class Expediting*

IEEE 802.1Q, *Virtual LANs*

IEEE 802.1s, *Multiple Spanning Trees*

IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*

IEEE 802.1X, *Port Based Network Access Control*

IEEE 802.3ab, *1000BASE-T*

IEEE 802.3ac, *VLAN Tag*

IEEE 802.3ad, *Link Aggregation*

IEEE 802.3ae, *10 Gb/s Ethernet*

IEEE 802.3ah, *Ethernet in the First Mile*

IEEE 802.3ba, *40 Gb/s and 100 Gb/s Ethernet*

IEEE 802.3i, *Ethernet*

IEEE 802.3u, *Fast Ethernet*

IEEE 802.3x, *Ethernet Flow Control*

IEEE 802.3z, *Gigabit Ethernet*

ITU-T G.8031/Y.1342, *Ethernet Linear Protection Switching*

ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*

ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

## **Ethernet VPN (EVPN)**

draft-ietf-bess-evpn-ac-df-01, *AC-Influenced Designated Forwarder Election for EVPN*

draft-ietf-bess-evpn-pref-df-01, *Preference-based EVPN DF Election*

draft-ietf-bess-evpn-prefix-advertisement-11, *IP Prefix Advertisement in EVPN*



*draft-ietf-bess-evpn-proxy-arp-nd-04, Operational Aspects of Proxy-ARP/ND in EVPN Networks*  
*draft-ietf-bess-evpn-vpls-seamless-integ-03, (PBB-)EVPN Seamless Integration with (PBB-)VPLS*  
*draft-snr-bess-pbb-evpn-isid-cmacflush-01, PBB-EVPN ISID-based CMAC-Flush*  
*RFC 7432, BGP MPLS-Based Ethernet VPN*  
*RFC 7623, Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*  
*RFC 8214, Virtual Private Wire Service Support in Ethernet VPN*  
*RFC 8317, Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) an Provider Backbone Bridging EVPN (PBB-EVPN)*  
*RFC 8365, A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*

## **Frame Relay**

*ANSI T1.617 Annex D, DSS1 - Signalling Specification For Frame Relay Bearer Service*  
*FRF.1.2, PVC User-to-Network Interface (UNI) Implementation Agreement*  
*FRF.12, Frame Relay Fragmentation Implementation Agreement*  
*FRF.16.1, Multilink Frame Relay UNI/NNI Implementation Agreement*  
*FRF.5, Frame Relay/ATM PVC Network Interworking Implementation*  
*FRF2.2, PVC Network-to-Network Interface (NNI) Implementation Agreement*  
*ITU-T Q.933 Annex A, Additional procedures for Permanent Virtual Connection (PVC) status management*

## **Generalized Multiprotocol Label Switching (GMPLS)**

*draft-ietf-ccamp-rsvp-te-srlg-collect-04, RSVP-TE Extensions for Collecting SRLG Information*  
*RFC 3471, Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*  
*RFC 3473, Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*  
*RFC 4204, Link Management Protocol (LMP)*  
*RFC 4208, Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*  
*RFC 4872, RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*  
*RFC 5063, Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart (helper mode)*

## gRPC Remote Procedure Calls (gRPC)

gnmi.proto, *gRPC Network Management Interface (gNMI), version 0.4.0*

*gRPC Network Management Interface (gNMI), Capabilities, Get, Set, Subscribe  
(ONCE, SAMPLE, ON\_CHANGE)*

## Intermediate System to Intermediate System (IS-IS)

draft-ietf-isis-mi-02, *IS-IS Multi-Instance*

draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*

ISO/IEC 10589:2002, Second Edition, Nov. 2002, *Intermediate system to  
Intermediate system intra-domain routing information exchange protocol for  
use in conjunction with the protocol for providing the connectionless-mode  
Network Service (ISO 8473)*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 2973, *IS-IS Mesh Groups*

RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate  
System to Intermediate System*

RFC 3719, *Recommendations for Interoperable Networks using Intermediate  
System to Intermediate System (IS-IS)*

RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate  
System to Intermediate System (IS-IS)*

RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for  
Advertising Router Information*

RFC 5120, *M-ISIS: Multi Topology (MT) Routing in IS-IS*

RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*

RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*

RFC 5302, *Domain-wide Prefix Distribution with Two-Level IS-IS*

RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*

RFC 5304, *IS-IS Cryptographic Authentication*

RFC 5305, *IS-IS Extensions for Traffic Engineering TE*

RFC 5306, *Restart Signaling for IS-IS (helper mode)*

RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label  
Switching (GMPLS)*

RFC 5308, *Routing IPv6 with IS-IS*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5310, *IS-IS Generic Cryptographic Authentication*

RFC 6213, *IS-IS BFD-Enabled TLV*

RFC 6232, *Purge Originator Identification TLV for IS-IS*

RFC 6233, *IS-IS Registry Extension for Purges*

RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*  
RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*  
RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*  
RFC 8202, *IS-IS Multi-Instance* (single topology)

## **Internet Protocol (IP) — Fast Reroute**

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*  
RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*  
RFC 7431, *Multicast-Only Fast Reroute*  
RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

## **Internet Protocol (IP) — General**

draft-grant-tacacs-02, *The TACACS+ Protocol*  
RFC 768, *User Datagram Protocol*  
RFC 793, *Transmission Control Protocol*  
RFC 854, *Telnet Protocol Specifications*  
RFC 1350, *The TFTP Protocol (revision 2)*  
RFC 2347, *TFTP Option Extension*  
RFC 2348, *TFTP Blocksize Option*  
RFC 2349, *TFTP Timeout Interval and Transfer Size Options*  
RFC 2428, *FTP Extensions for IPv6 and NATs*  
RFC 2784, *Generic Routing Encapsulation (GRE)*  
RFC 2890, *Key and Sequence Number Extensions to GRE*  
RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*  
RFC 4251, *The Secure Shell (SSH) Protocol Architecture*  
RFC 4252, *The Secure Shell (SSH) Authentication Protocol* (publickey, password)  
RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*  
RFC 4254, *The Secure Shell (SSH) Connection Protocol*  
RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*  
RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*  
RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer (ECDSA)*  
RFC 5925, *The TCP Authentication Option*  
RFC 5926, *Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)*  
RFC 6398, *IP Router Alert Considerations and Usage (MLD)*

RFC 6528, *Defending against Sequence Number Attacks*

## Internet Protocol (IP) — Multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast* (version 1)

draft-dolganow-bess-mvpn-expl-track-01, *Explicit Tracking with Wild Card Routes in Multicast VPN*

draft-ietf-bier-mvpn-11, *Multicast VPN Using BIER*

draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*

draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*

draft-ietf-mboned-mtrace-v2-17, *Mtrace Version 2: Traceroute Facility for IP Multicast*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)* (auto-RP groups)

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

RFC 4607, *Source-Specific Multicast for IP*

RFC 4608, *Source-Specific Protocol Independent Multicast in 232/8*

RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*

RFC 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*

RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*

RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*

RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

RFC 6037, *Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6513, *Multicast in MPLS/BGP IP VPNs*

RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/IP VPNs*

RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs*

RFC 6516, *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages*

RFC 6625, *Wildcards in Multicast VPN Auto-Discover Routes*

RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path*

RFC 7246, *Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context*

RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

RFC 7716, *Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures*

RFC 7761, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

RFC 8279, *Multicast Using Bit Index Explicit Replication (BIER)*

RFC 8296, *Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks (MPLS encapsulation)*

RFC 8401, *Bit Index Explicit Replication (BIER) Support via IS-IS*

## **Internet Protocol (IP) — Version 4**

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

RFC 951, *Bootstrap Protocol (BOOTP)*

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery (router specification)*

RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*  
RFC 1534, *Interoperation between DHCP and BOOTP*  
RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*  
RFC 1812, *Requirements for IPv4 Routers*  
RFC 1918, *Address Allocation for Private Internets*  
RFC 2003, *IP Encapsulation within IP*  
RFC 2131, *Dynamic Host Configuration Protocol*  
RFC 2132, *DHCP Options and BOOTP Vendor Extensions*  
RFC 2401, *Security Architecture for Internet Protocol*  
RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*  
RFC 3046, *DHCP Relay Agent Information Option (Option 82)*  
RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*  
RFC 4884, *Extended ICMP to Support Multi-Part Messages (ICMPv4 and ICMPv6 Time Exceeded)*

## **Internet Protocol (IP) — Version 6**

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*  
RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*  
RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*  
RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*  
RFC 3587, *IPv6 Global Unicast Address Format*  
RFC 3596, *DNS Extensions to Support IP version 6*  
RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*  
RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*  
RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*  
RFC 3971, *SEcure Neighbor Discovery (SEND)*  
RFC 3972, *Cryptographically Generated Addresses (CGA)*  
RFC 4007, *IPv6 Scoped Address Architecture*  
RFC 4193, *Unique Local IPv6 Unicast Addresses*  
RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*  
RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*  
RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*  
RFC 4862, *IPv6 Stateless Address Autoconfiguration (router functions)*

---

RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*  
RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*  
RFC 5007, *DHCPv6 Leasequery*  
RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*  
RFC 5722, *Handling of Overlapping IPv6 Fragments*  
RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 (IPv6)*  
RFC 5952, *A Recommendation for IPv6 Address Text Representation*  
RFC 6092, *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service* (Internet Control and Management, Upper-Layer Transport Protocols, UDP Filters, IPsec and Internet Key Exchange (IKE), TCP Filters)  
RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*  
RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*  
RFC 8021, *Generation of IPv6 Atomic Fragments Considered Harmful*  
RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*  
RFC 8201, *Path MTU Discovery for IP version 6*

## **Internet Protocol Security (IPsec)**

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*  
draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*  
RFC 2401, *Security Architecture for the Internet Protocol*  
RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*  
RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*  
RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*  
RFC 2406, *IP Encapsulating Security Payload (ESP)*  
RFC 2407, *IPsec Domain of Interpretation for ISAKMP (IPsec DoI)*  
RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*  
RFC 2409, *The Internet Key Exchange (IKE)*  
RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*  
RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*  
RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*  
RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*  
RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*  
RFC 3947, *Negotiation of NAT-Traversal in the IKE*

---

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*  
RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec ESP*  
RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*  
RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*  
RFC 4301, *Security Architecture for the Internet Protocol*  
RFC 4303, *IP Encapsulating Security Payload*  
RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*  
RFC 4308, *Cryptographic Suites for IPsec*  
RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*  
RFC 4543, *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*  
RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*  
RFC 4945, *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX*  
RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*  
RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*  
RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol*  
RFC 5903, *ECP Groups for IKE and IKEv2*  
RFC 5998, *An Extension for EAP-Only Authentication in IKEv2*  
RFC 6379, *Suite B Cryptographic Suites for IPsec*  
RFC 6380, *Suite B Profile for Internet Protocol Security (IPsec)*  
RFC 6712, *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*  
RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*  
RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*  
RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*  
RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*  
RFC 7427, *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*  
RFC 7468, *Textual Encodings of PKIX, PKCS, and CMS Structures*



---

## Label Distribution Protocol (LDP)

*draft-ietf-mpls-ldp-ip-pw-capability-09, Controlling State Advertisements Of Non-negotiated LDP Applications*

*draft-pdutta-mpls-ldp-adj-capability-00, LDP Adjacency Capabilities*

*draft-pdutta-mpls-ldp-v2-00, LDP Version 2*

*draft-pdutta-mpls-mldp-up-redundancy-00, Upstream LSR Redundancy for Multipoint LDP Tunnels*

*draft-pdutta-mpls-multi-ldp-instance-00, Multiple LDP Instances*

*draft-pdutta-mpls-tldp-hello-reduce-04, Targeted LDP Hello Reduction*

*RFC 3037, LDP Applicability*

*RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol (helper mode)*

*RFC 5036, LDP Specification*

*RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs)*

*RFC 5443, LDP IGP Synchronization*

*RFC 5561, LDP Capabilities*

*RFC 5919, Signaling LDP Label Advertisement Completion*

*RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

*RFC 6512, Using Multipoint LDP When the Backbone Has No Route to the Root*

*RFC 6826, Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

*RFC 7032, LDP Downstream-on-Demand in Seamless MPLS*

*RFC 7552, Updates to LDP for IPv6*

## Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

*draft-mammoliti-l2tp-accessline-avp-04, Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*

*RFC 2661, Layer Two Tunneling Protocol "L2TP"*

*RFC 2809, Implementation of L2TP Compulsory Tunneling via RADIUS*

*RFC 3438, Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*

*RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

*RFC 4719, Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*

*RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

## Management

draft-ietf-snmpv3-update-mib-05, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*

draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*

draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*

draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*

draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*

draft-ietf-vrrp-unified-mib-06, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6 (IPv6)*

ianaaddressfamilynumbers-mib, *IANA-ADDRESS-FAMILY-NUMBERS-MIB*

ianagmplstc-mib, *IANA-GMPLS-TC-MIB*

ianaiftype-mib, *IANAifType-MIB*

ianaiprouteprotocol-mib, *IANA-RTPROTO-MIB*

IEEE8021-CFM-MIB, *IEEE P802.1ag(TM) CFM MIB*

IEEE8021-PAE-MIB, *IEEE 802.1X MIB*

IEEE8023-LAG-MIB, *IEEE 802.3ad MIB*

LLDP-MIB, *IEEE P802.1AB(TM) LLDP MIB*

openconfig-bgp.yang version 3.0.1, *BGP Module*

openconfig-bgp-common.yang version 3.0.1, *BGP Common Module*

openconfig-bgp-common-multiprotocol.yang version 3.0.1, *BGP Common Multiprotocol Module*

openconfig-bgp-common-structure.yang version 3.0.1, *BGP Common Structure Module*

openconfig-bgp-global.yang version 3.0.1, *BGP Global Module*

openconfig-bgp-neighbor.yang version 3.0.1, *BGP Neighbor Module*

openconfig-bgp-peer-group.yang version 3.0.1, *BGP Peer Group Module*

openconfig-bgp-policy.yang version 4.0.1, *BGP Policy Module*

openconfig-if-aggregate.yang version 2.0.0, *Interfaces Aggregated Model*

openconfig-if-ethernet.yang version 2.0.0, *Interfaces Ethernet Model*

openconfig-if-ip.yang version 2.0.0, *Interfaces IP Module*

openconfig-if-ip-ext.yang version 2.0.0, *Interfaces IP Extensions Module*

openconfig-interfaces.yang version 2.0.0, *Interfaces Module*

---

openconfig-isis.yang version 0.3.0, *IS-IS Module*  
openconfig-isis-lsp.yang version 0.3.0, *IS-IS LSP Module*  
openconfig-isis-routing.yang version 0.3.0, *IS-IS Routing Module*  
openconfig-lacp.yang version 1.1.0, *LACP Module*  
openconfig-lldp.yang version 0.1.0, *LLDP Module*  
openconfig-local-routing.yang version 1.0.1, *Local Routing Module*  
openconfig-network-instance.yang version 0.8.0, *Network Instance Module*  
openconfig-routing-policy.yang version 3.0.0, *Routing Policy Module*  
openconfig-vlan.yang version 2.0.0, *VLAN Module*  
RFC 1157, *A Simple Network Management Protocol (SNMP)*  
RFC 1212, *Concise MIB Definitions*  
RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*  
RFC 1215, *A Convention for Defining Traps for use with the SNMP*  
RFC 1724, *RIP Version 2 MIB Extension*  
RFC 1901, *Introduction to Community-based SNMPv2*  
RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*  
RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*  
RFC 2206, *RSVP Management Information Base using SMIv2*  
RFC 2213, *Integrated Services Management Information Base using SMIv2*  
RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*  
RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*  
RFC 2515, *Definitions of Managed Objects for ATM Management*  
RFC 2570, *SNMP Version 3 Framework*  
RFC 2571, *An Architecture for Describing SNMP Management Frameworks*  
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*  
RFC 2573, *SNMP Applications*  
RFC 2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*  
RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*  
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*  
RFC 2579, *Textual Conventions for SMIv2*  
RFC 2580, *Conformance Statements for SMIv2*

---

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3164, *The BSD syslog Protocol*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4)*

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*

---

RFC 4220, *Traffic Engineering Link Management Information Base*  
RFC 4273, *Definitions of Managed Objects for BGP-4*  
RFC 4292, *IP Forwarding Table MIB*  
RFC 4293, *Management Information Base for the Internet Protocol (IP)*  
RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*  
RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*  
RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms (TLS)*  
RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*  
RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*  
RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*  
RFC 5102, *Information Model for IP Flow Information Export*  
RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2 (TLS client, RSA public key)*  
RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*  
RFC 6425, *Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping*  
RFC 6991, *Common YANG Data Types*  
RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*  
RFC 7950, *The YANG 1.1 Data Modeling Language*  
SFLOW-MIB, *sFlow MIB Version 1.3 (Draft 5)*

## **Multiprotocol Label Switching — Transport Profile (MPLS-TP)**

RFC 5586, *MPLS Generic Associated Channel*  
RFC 5921, *A Framework for MPLS in Transport Networks*  
RFC 5960, *MPLS Transport Profile Data Plane Architecture*  
RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*  
RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*  
RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*  
RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*  
RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*  
RFC 6478, *Pseudowire Status for Static Pseudowires*

RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

## **Multiprotocol Label Switching (MPLS)**

draft-ietf-teas-sr-rsvp-coexistence-rec-02, *Recommendations for RSVP-TE and Segment Routing LSP co-existence*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*

RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*

RFC 5332, *MPLS Multicast Encapsulations*

RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

RFC 7510, *Encapsulating MPLS in UDP*

## **Network Address Translation (NAT)**

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6334, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite*

RFC 6887, *Port Control Protocol (PCP)*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7915, *IP/ICMP Translation Algorithm*

## **Network Configuration Protocol (NETCONF)**

RFC 5277, *NETCONF Event Notifications*

RFC 6022, *YANG Module for NETCONF Monitoring*  
RFC 6241, *Network Configuration Protocol (NETCONF)*  
RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*  
RFC 6243, *With-defaults Capability for NETCONF*  
RFC 7895, *YANG Module Library*

## **Open Shortest Path First (OSPF)**

draft-ietf-ospf-ospfv3-lsa-extend-13, *OSPFv3 LSA Extendibility*  
RFC 1586, *Guidelines for Running OSPF Over Frame Relay Networks*  
RFC 1765, *OSPF Database Overflow*  
RFC 2328, *OSPF Version 2*  
RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*  
RFC 3509, *Alternative Implementations of OSPF Area Border Routers*  
RFC 3623, *Graceful OSPF Restart Graceful OSPF Restart (helper mode)*  
RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*  
RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*  
RFC 4222, *Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance*  
RFC 4552, *Authentication/Confidentiality for OSPFv3*  
RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*  
RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*  
RFC 5185, *OSPF Multi-Area Adjacency*  
RFC 5187, *OSPFv3 Graceful Restart (helper mode)*  
RFC 5243, *OSPF Database Exchange Summary List Optimization*  
RFC 5250, *The OSPF Opaque LSA Option*  
RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*  
RFC 5340, *OSPF for IPv6*  
RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*  
RFC 5838, *Support of Address Families in OSPFv3*  
RFC 6987, *OSPF Stub Router Advertisement*  
RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*  
RFC 7770, *Extensions to OSPF for Advertising Optional Router Capabilities*

## OpenFlow

TS-007, *OpenFlow Switch Specification Version 1.3.1* (OpenFlow-hybrid switches)

## Path Computation Element Protocol (PCEP)

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*

draft-ietf-pce-segment-routing-08, *PCEP Extensions for Segment Routing*

draft-ietf-pce-stateful-pce-14, *PCEP Extensions for Stateful PCE*

RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

## Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*

RFC 1661, *The Point-to-Point Protocol (PPP)*

RFC 1662, *PPP in HDLC-like Framing*

RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*

RFC 1989, *PPP Link Quality Monitoring*

RFC 1990, *The PPP Multilink Protocol (MP)*

RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

RFC 2153, *PPP Vendor Extensions*

RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*

RFC 2615, *PPP over SONET/SDH*

RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

RFC 2878, *PPP Bridging Control Protocol (BCP)*

RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*

RFC 5072, *IP Version 6 over PPP*

## Policy Management and Credit Control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points (Gx support as it applies to wireline environment (BNG))*

RFC 3588, *Diameter Base Protocol*

RFC 4006, *Diameter Credit-Control Application*



---

## Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS Interworking*  
MFA Forum 12.0.0, *Multiservice Interworking - Ethernet over MPLS*  
MFA Forum 13.0.0, *Fault Management for Multiservice Interworking v1.0*  
MFA Forum 16.0.0, *Multiservice Interworking - IP over MPLS*  
MFA Forum 9.0.0, *The Use of Virtual trunks for ATM/MPLS Control Plane Interworking*  
RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*  
RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3)*  
RFC 4385, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*  
RFC 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*  
RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*  
RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*  
RFC 4619, *Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*  
RFC 4717, *Encapsulation Methods for Transport Asynchronous Transfer Mode (ATM) over MPLS Networks*  
RFC 4816, *Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service*  
RFC 5085, *Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*  
RFC 5659, *An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*  
RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*  
RFC 6073, *Segmented Pseudowire*  
RFC 6310, *Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*  
RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*  
RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*  
RFC 6718, *Pseudowire Redundancy*  
RFC 6829, *Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6*  
RFC 6870, *Pseudowire Preferential Forwarding Status bit*  
RFC 7023, *MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking*

---

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

## Quality of Service (QoS)

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2598, *An Expedited Forwarding PHB*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3260, *New Terminology and Clarifications for Diffserv*

## Remote Authentication Dial In User Service (RADIUS)

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*

## Resource Reservation Protocol — Traffic Engineering (RSVP-TE)

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions (IF\_ID RSVP\_HOP object with unnumbered interfaces and RSVP-TE graceful restart helper procedures)*

RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*

RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*

RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

## **Routing Information Protocol (RIP)**

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

## **Segment Routing (SR)**

draft-filsfils-spring-segment-routing-policy-05, *Segment Routing Policy for Traffic Engineering*

draft-francois-rtgwg-segment-routing-ti-lfa-04, *Topology Independent Fast Reroute using Segment Routing*

draft-gredler-idr-bgp-ls-segment-routing-ext-03, *BGP Link-State extensions for Segment Routing*

draft-ietf-idr-segment-routing-te-policy-02, *Advertising Segment Routing Policies in BGP*

draft-ietf-isis-segment-routing-extensions-04, *IS-IS Extensions for Segment Routing*

*draft-ietf-mpls-spring-lsp-ping-02, Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane*

*draft-ietf-ospf-segment-routing-extensions-04, OSPF Extensions for Segment Routing*

*draft-ietf-spring-conflict-resolution-05, Segment Routing MPLS Conflict Resolution*

*draft-ietf-spring-segment-routing-ldp-interop-09, Segment Routing interworking with LDP*

## **Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH)**

*ANSI T1.105.03, Jitter Network Interfaces*

*ANSI T1.105.06, Physical Layer Specifications*

*ANSI T1.105.09, Network Timing and Synchronization*

*ITU-T G.703, Physical/electrical characteristics of hierarchical digital interfaces*

*ITU-T G.707, Network node interface for the synchronous digital hierarchy (SDH)*

*ITU-T G.813, Timing characteristics of SDH equipment slave clocks (SEC)*

*ITU-T G.823, The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*

*ITU-T G.824, The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy*

*ITU-T G.825, The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*

*ITU-T G.841, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1, issued in July 2002*

*ITU-T G.957, Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*

## **Time Division Multiplexing (TDM)**

*ANSI T1.403, DS1 Metallic Interface Specification*

*ANSI T1.404, DS3 Metallic Interface Specification*

## **Timing**

*GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005*

*GR-253-CORE, SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000*

IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions*, issued 09/2008

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC)*, issued 03/2003

ITU-T G.8261, *Timing and synchronization aspects in packet networks*, issued 04/2008

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC)*, issued 08/2007

ITU-T G.8264, *Distribution of timing information through packet networks*, issued 10/2008

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization*, issued 10/2010

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network*, issued 07/2014

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

## **Two-Way Active Measurement Protocol (TWAMP)**

RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP) (server, unauthenticated mode)*

RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*

RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*

## **Virtual Private LAN Service (VPLS)**

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

RFC 5501, *Requirements for Multicast Support in Virtual Private LAN Services*

RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

RFC 7041, *Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging*

RFC 7117, *Multicast in Virtual Private LAN Service (VPLS)*

---

## Voice and Video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

ITU-T G.1020 Appendix I, *Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks - Mean Absolute Packet Delay Variation & Markov Models*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550 Appendix A.8, *RTP: A Transport Protocol for Real-Time Applications* (estimating the interarrival jitter)

RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

## Wireless Local Area Network (WLAN) Gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses* (S2a roaming based on GPRS)

# Customer Document and Product Support



## Customer Documentation

[Customer Documentation Welcome Page](#)



## Technical Support

[Product Support Portal](#)



## Documentation Feedback

[Customer Documentation Feedback](#)

