BayRS Version 14.20

Part No. 308603-14.20 Rev 00
September 2000

600 Technology Park Drive
Billerica, MA 01821-4130

Reference for BCC IP show Commands

NORTEL
NETWORKS™

Copyright © 2000 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

ASN, BayRS, BayStack, and BCC are trademarks of Nortel Networks.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Chapter 1
IP show Commands

Chapter 2
BGP show Commands

Chapter 3
DVMRP show Commands

Chapter 4
GRE show Commands

Chapter 5
IGMP show Commands

Chapter 6
NAT show Commands

Chapter 7
OSPF show Commands

Index

Preface

This guide describes the Bay Command Console (BCC™) show commands for the following services:

- Internet Protocol (IP)
- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Generic Routing Encapsulation (GRE)
- Internet Group Management Protocol (IGMP)
- Network Address Translation (NAT)
- Open Shortest Path First (OSPF)

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network).*

Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is:
ping <*ip_address*>, you enter:
ping 192.32.10.12

bold text

Indicates command names and options and text that you need to enter.

Example: Enter **show ip** {**alerts** | **routes**}.

Example: Use the **dinfo** command.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is:
show ip {**alerts** | **routes**}, you must enter either:
show ip alerts or **show ip routes**, but not both.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is:
show ip interfaces [**-alerts**], you can enter either:
show ip interfaces or **show ip interfaces -alerts**.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
AS	autonomous system
ASBR	AS boundary router
ASE	autonomous system external
BGP	Border Gateway Protocol
DDN	Defense Data Network
DNS	domain name server
DVMRP	Distance Vector Multicast Routing Protocol
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
IBGP	Internal BGP
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol

IGP	Interior Gateway Protocol
IP	Internet Protocol
LSA	link state advertisement
LSDB	link state database
MAC	media access control
MIB	management information base
NAT	Network Address Translation
NSSA	not-so-stubby area
OSPF	Open Shortest Path First
PDN	Public Data Network
PIM	Protocol Independent Multicast
RIP	Routing Information Protocol
RIPSO	Revised IPSO
RSVP	Resource Reservation Protocol
SNAP	Subnetwork Access Protocol
SVC	switched virtual circuit
TCP	Transmission Control Protocol
TTL	time to live
UDP	User Datagram Protocol

Related Publications

For more information about using IP services, refer to the following publications:

- *Configuring IP, ARP, RARP, RIP, and OSPF* (Nortel Networks part number 308627-14.20 Rev 00)

  Provides a description of IP, ARP, RARP, RIP, and OSPF services and instructions for configuring them.

- *Configuring IP Exterior Gateway Protocols (BGP and EGP)* (Nortel Networks part number 308628-14.00 Rev 00)

  Provides a description of Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP) services and instructions for configuring them.

- *Configuring GRE, NAT, RIPSO, and BFE Services* (Nortel Networks part number 308625-14.20 Rev 00)

  Provides a description of Generic Routing Encapsulation (GRE), Network Address Translation (NAT), Revised IP Security Option (RIPSO), and Blacker front-end services and instructions for configuring them.

- *Configuring IP Multicasting and Multimedia Services* (Nortel Networks part number 308629-14.00 Rev 00)

  Provides a description of Internet Group Management Protocol (IGMP), IGMP Relay, Distance Vector Multicast Routing Protocol (DVMRP), Multicasting Extensions to OSPF (MOSPF), Resource Reservation Protocol (RSVP), and Protocol Independent Multicast (PIM) services and instructions for configuring them.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the support.baynetworks.com/library/tpubs/ URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at www.adobe.com to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
IP show Commands

This chapter describes how to use the BCC **show ip** command to display routing, configuration, interface, and statistical data about the Internet Protocol (IP) from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show ip adjacent-hosts

The **show ip adjacent-hosts** command displays a table of configured adjacent hosts. The output includes the following information:

Host Address	IP address of the adjacent host (applies to both single and expanded).
Interface	Address of the IP interface through which packets reach the host.
Encaps	Encapsulation method used: ENET (Ethernet), SNAP (Subnetwork Access Protocol), PDN (Public Data Network), or DDN (Defense Data Network).
Valid ?	Validity of the configuration. If this field displays No, you should check the adjacent host's configuration.
State	Status of the adjacent host: enabled or disabled.
Mac Address	Media access control (MAC) address of the host.
WAN Address	Physical address of the adjacent host.
Sub-address	Subaddress used to establish a switched virtual circuit (SVC) to the adjacent host.
Type of Number	Type of number used to establish an SVC to the adjacent host.

show ip alerts

The **show ip alerts** command displays the circuit name and IP address of interfaces whose state does not match their configuration, for example, an interface configured as enabled but whose state is not up. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
Circuit #	Number of the circuit in the router's active MIB.
State	Status of the IP interface: up or down.
IP Address	IP address of the interface.
Mask	Subnet mask of the IP interface.

show ip arp

The **show ip arp** command displays the IP Address Resolution Protocol (ARP) table. This table shows the mapping between the host IP address and its MAC address and shows how the IP address was learned. The output includes the following information about each host listed:

IP Address	IP address of the host.
Physical address	MAC address of the host.
Type	How the IP address was resolved to the MAC address: dynamic means that ARP resolved it; static means that it was configured through an adjacent host entry.

show ip disabled

The **show ip disabled** command displays information about disabled IP interfaces. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
Circuit #	Number of the circuit in the router’s active MIB.
State	Status of the IP interface: up or down.
IP Address	IP address of the interface.
Mask	Subnet mask of the IP interface.

show ip enabled

The **show ip enabled** command displays information about enabled IP interfaces. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
Circuit #	Number of the circuit in the router's active MIB.
State	Status of the IP interface: up or down.
IP Address	IP address of the interface. IP address 0.0.0.0 indicates that the circuit is associated with an unnumbered interface.
Mask	Subnet mask of the IP interface.
MAC Address	Layer 2 address of the IP interface.

show ip icmp

The **show ip icmp** command displays statistical information about Internet Control Message Protocol (ICMP) packets and messages.

This command supports the following subcommand options:

client	out
in	server
misc	

In addition, you can specify the following argument with any subcommand option:

<ip_address>	Displays information about the specified IP address only.

show ip icmp client

The **show ip icmp client** command displays echo, timestamp, and address mask statistics about ICMP packets for all IP addresses or for a specific IP address. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Echo Requests	Number of ICMP echo request messages received.
Echo Replies	Number of ICMP echo reply messages received.
Timestamp Reqs	Number of ICMP timestamp request messages received.
Timestamp Repls	Number of ICMP timestamp reply messages received.
Address Mask Requests	Number of ICMP address request messages received.
Address Mask Replies	Number of ICMP address reply messages received.

show ip icmp in

The **show ip icmp in** command displays statistics about ICMP packets received for all IP addresses or for a specific IP address. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
ICMP Received	Total number of ICMP messages received, including errors.
ICMP In Errors	Number of ICMP messages received that had errors (bad ICMP checksums).
Destn. Unreachable	Number of ICMP destination unreachable messages received.
Receive Time Exceeded	Number of ICMP time exceeded messages received.
Receive Param Problem	Number of ICMP parameter problem messages received.

show ip icmp misc

The **show ip icmp misc** command displays statistics about ICMP source, quench, redirect, and prohibit messages for all IP addresses or for a specific IP address. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
SrcQunch In/Out	Number of ICMP source quench messages received and sent.
Redirect Messages In/Out	Number of ICMP redirect messages received and sent.
Prohibit In/Out	Number of ICMP destination unreachable or communication administratively prohibited messages received and sent.

show ip icmp out

The **show ip icmp out** command displays statistics about ICMP packets that the router generates on each IP address or on a specific IP address. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
ICMP Sent	Total number of ICMP messages sent, including errors.
ICMP In Errors	Number of ICMP messages sent that had errors (bad ICMP checksums).
Destn. Unreachable	Number of ICMP destination unreachable messages sent.
Sent Time Exceeded	Number of ICMP time exceeded messages sent.
Sent Param Problem	Number of ICMP parameter problem messages sent.

show ip icmp server

The **show ip icmp server** command displays statistics about ICMP messages that the router generates for all IP addresses or for a specific IP address. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Echo Requests	Number of ICMP echo request messages sent.
Echo Replies	Number of ICMP echo reply messages sent.
Timestamp Reqs	Number of ICMP timestamp request messages sent.
Timestamp Repls	Number of ICMP timestamp reply messages sent.
Address Mask Requests	Number of ICMP address request messages sent.
Address Mask Replies	Number of ICMP address reply messages sent.

show ip interfaces

The **show ip interfaces** command displays a list of all IP interfaces currently configured on the router. This command allows for the following command filters and arguments:

-alerts	Displays information about disabled IP interfaces only.
-enabled	Displays information about enabled IP interfaces only.
-name <*circuit_name*>	Displays information about the specified circuit only.
<*ip_address*>	Displays information about the specified IP address only.

The output includes the following information:

Circuit	The name of the circuit that the IP interface is configured on.
Circuit #	The number of this circuit. The circuit count is assigned in the order that each circuit is created.
State	Current state of the interface: up, down, or not present.
IP Address	The IP address assigned to this interface.

Mask	The subnet mask associated with the interface's IP address.
MAC Address	The media access control (MAC) address associated with this interface.

show ip rip

The **show ip rip** command displays information about the Routing Information Protocol (RIP) configuration on IP interfaces.

This command supports the following subcommand options:

alerts	enabled
auth	summary
disabled	timers

show ip rip alerts

The **show ip rip alerts** command displays information about the IP interfaces that have RIP configured but the state of RIP is down. The output includes the following information:

IP Interface	IP interface to which the RIP configuration applies.
Circuit #	Number of the IP interface circuit in the router's active MIB.
State	Operational state of the IP interface: up or down.
RIP Sup/Lis	Allow this RIP interface to announce/accept RIP routes.
Def. Rt. Sup/Lis	Allow this RIP interface to announce/accept the default RIP route.
Poison Reverse	Method used to readvertise routes out the interface on which they were learned: poison (poisoned reverse), actual (actual cost), or split (split horizon).
RIP Mode	Type of updates RIP sends: rip1 (Version 1 updates), rip2 (Version 2 updates with no aggregation of subnets), or aggr (Version 2 updates with subnet aggregation).

Trig. Updates	Send RIP updates when routing changes occur over 5-second intervals.
TTL	IP time to live for RIP updates.

show ip rip auth

The **show ip rip auth** command displays information about IP interfaces on which RIP performs authentication. You can configure authentication when you set the RIP version to RIP2. The output includes the following information:

IP Interface	IP interface to which the RIP configuration applies.
Circuit #	Number of the IP interface circuit in the router’s active MIB.
Type	Specifies the way RIP handles simple authentication in RIP2 mode.
Password	Valid password string up to 16 characters.

show ip rip disabled

The **show ip rip disabled** command displays the IP interfaces that have RIP configured but disabled. The output includes the following information:

IP Interface	IP interface to which the RIP configuration applies.
Circuit #	Number of the IP interface circuit in the router’s active MIB.
State	Operational state of the IP interface: up or down.
RIP Sup/Lis	Allow this RIP interface to announce/accept RIP routes.
Def. Rt. Sup/Lis	Allow this RIP interface to announce/accept the default RIP route.
Poison Reverse	Method used to readvertise routes out the interface on which they were learned: poison (poisoned reverse), actual (actual cost), or split (split horizon).
RIP Mode	Type of updates RIP sends: rip1 (Version 1 updates), rip2 (Version 2 updates with no aggregation of subnets), or aggr (Version 2 updates with subnet aggregation).

Trig. Updates	Send RIP updates when routing changes occur over 5-second intervals.
TTL	IP time to live for RIP updates.

show ip rip enabled

The **show ip rip enabled** command displays the IP interfaces that have RIP enabled on them. The output includes the following information:

IP Interface	IP interface to which the RIP configuration applies.
Circuit #	Number of the IP interface circuit in the router’s active MIB.
State	Operational state of the IP interface: up or down.
RIP Sup/Lis	Allow this RIP interface to announce/accept RIP routes.
Def. Rt. Sup/Lis	Allow this RIP interface to announce/accept the default RIP route.
Poison Reverse	Method used to readvertise routes out the interface on which they were learned: poison (poisoned reverse), actual (actual cost), or split (split horizon).
RIP Mode	Type of updates RIP sends: rip1 (Version 1 updates), rip2 (Version 2 updates with no aggregation of subnets), or aggr (Version 2 updates with subnet aggregation).
Trig. Updates	Send RIP updates when routing changes occur over 5-second intervals.
TTL	IP time to live for RIP updates.

show ip rip summary

The **show ip rip summary** command displays the IP interfaces on which RIP is configured. The output includes the following information:

IP Interface	IP interface to which the RIP configuration applies.
Circuit #	Number of the IP interface circuit in the router’s active MIB.
State	Operational state of the IP interface: up or down.
RIP Sup/Lis	Allow this RIP interface to announce/accept RIP routes.

Def. Rt. Sup/Lis	Allow this RIP interface to announce/accept the default RIP route.
Poison Reverse	Method used to readvertise routes out the interface on which they were learned: poison (poisoned reverse), actual (actual cost), or split (split horizon).
RIP Mode	Type of updates RIP sends: rip1 (Version 1 updates), rip2 (Version 2 updates with no aggregation of subnets), or aggr (Version 2 updates with subnet aggregation).
Trig. Updates	Send RIP updates when routing changes occur over 5-second intervals.
TTL	IP time to live for RIP updates.

show ip rip timers

The **show ip rip timers** command displays the RIP timer values that you can use to control periodic RIP updates (broadcast), when RIP declares a route invalid (timeout), and the length of time a route is advertised with an infinite metric (holddown). The output includes the following information:

IP Interface	IP interface to which the time interval is applied.
Circuit #	Number of the IP interface circuit in the router’s active MIB.
Broadcast Timer	Time interval between RIP updates.
Timeout Timer	Amount of time after which a route is no longer considered valid.
Hold Down Timer	Amount of time an unused route is held and advertised as unreachable.

show ip routes

The **show ip routes** command displays IP routes. This command allows for the following command filters and arguments:

<ip_address>	Displays the routes that match the specified IP address.
<*ip_address/prefix*>	Displays the routes that match the specified range.
-A	Displays the entire routing table; routes marked with an asterisk (*) are routes in the normal routing table.
-s	Displays the slot. If the address is 255.255.255.255, the cache will be the internal cache for this slot.

The output includes the following information:

Destination/Mask	Destination IP address for this route. 0.0.0.0 indicates a default route. The subnet mask is combined with the destination address and then compared with the value in Destination. If the value of Destination is 0.0.0.0 (a default route), the value of Mask is also 0.0.0.0.
Proto	Routing method through which the router learned this route: local, RIP, or OSPF.
Age	Number of seconds since this route was last updated or verified to be correct. The meaning of “too old” depends on the routing protocol specified under Proto.
Cost	Number of hops to reach the destination.
NextHop	IP address of the next hop of this route. If the next hop is an unnumbered interface, the output includes 0.0.0.*n*, where *n* is the number of the circuit on which the interface has been configured.
AS	Autonomous system identifier for destination IP interfaces running the OSPF protocol.

show ip static

The **show ip static** command displays all statically configured routes on the router. The output includes the following information:

IP Destination	IP address of this static route.
Network Mask	Subnet mask for this static route.
Cost	Number of hops to reach the destination.
Next Hop	IP address of the next hop on the route. If the next hop is an unnumbered interface, the Next Hop field displays the circuit number associated with the unnumbered interface.
Valid	Value that indicates whether or not the configuration is valid.
Enabled	State (active or inactive) of the static route record in the IP routing tables.

show ip stats

The **show ip stats** command displays IP statistical information.

This command supports the following subcommand options:

cache	interface
datagrams	security in
fragments	security out

In addition, you can specify the following filter and arguments with the above subcommand options:

-name *<circuit_name>*	Displays information about the specified circuit only.
<ip_address>	Displays information about the specified IP address only.

show ip stats cache

The **show ip stats cache** command displays statistics about the cached forwarding tables that IP uses for forwarding traffic for all IP addresses or for a specific IP address or circuit. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Cache Networks	Number of entries in the forwarding table.
Cache Misses	Number of times that the forwarding table did not contain information about a destination and IP had to look up the route.
Cache Removes	Number of entries removed from the forwarding table because they timed out.

show ip stats datagrams

The **show ip stats datagrams** command displays error statistics about IP datagrams that IP has processed for all IP addresses or for a specific IP address or circuit. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Header Errors	Number of IP packets received with header errors.
Address Errors	Number of IP packets received with address errors.
Unknown Protocol	Number of IP packets received locally that IP discarded because the router did not implement the protocol.
In Discards	Number of packets that IP received but discarded because of lack of resources, for example, insufficient buffers.
Out Discards	Number of packets given to IP to transmit but discarded because of lack of resources, for example, insufficient buffers.
No Routes	Number of packets with unknown destination addresses that an upper-layer protocol gave to IP to transmit.

show ip stats fragments

The **show ip stats fragments** command displays all information about fragmented IP packets for all IP addresses or for a specific IP address or circuit. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Frag Receives	Number of IP fragments received that this router had to reassemble.
Success Reassemblies	Number of fragmented datagrams that this router successfully reassembled.
Failed Reassemblies	Number of fragmented datagrams that this router failed to reassemble (not necessarily a count of discarded IP fragments).
Frags Sent	Number of IP datagrams that this router fragmented.
Frags Failed	Number of IP datagrams that this router discarded because it could not fragment them properly, for example, could not set the Don’t Fragment bit.
Total Frags	Total number of fragments that this router sent and received.

show ip stats interface

The **show ip stats interface** command displays statistical information about the IP interface configured on the router. This command allows for the following argument:

<*ip_address*>	Displays information about the specified IP address only.

The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP address	IP address of the interface.
In Receives	Number of packets received on the interface, including errors.

Out Requests	Number of packets that local clients, including ICMP, supplied to IP for transmitting.
Forwards	Number of packets forwarded through this interface; included in the In Receives count.
In Discards	Number of packets that IP received but discarded because of lack of resources, for example, insufficient buffers.
Out Discards	Number of packets given to IP to transmit but discarded because of lack of resources, for example, insufficient buffers.

show ip stats security in

The **show ip stats security in** command displays statistics associated with IP security for received packets on each IP address or on a specific IP address or circuit. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Drop Rx Authority	Number of received packets dropped because the authority flag was not sufficient.
Drop Rx Formats	Number of received packets dropped because the security option format was invalid.
Drop Rx Levels	Number of received packets dropped because the classification level was out of range.
Drop Rx No IPSOS	Number of received packets dropped because they did not have an IP security label.
Drop Rx Prohibit	Number of ICMP destination unreachable or communication administratively prohibited messages received.

show ip stats security out

The **show ip status security out** command displays statistics associated with IP security for transmitted packets on each IP address or on a specific IP address or circuit. The output includes the following information:

Circuit	Name of the circuit associated with the IP interface.
IP Address	IP address of the interface.
Drop Tx Authority	Number of transmitted packets dropped because the authority flag was not sufficient.
Drop Tx Levels	Number of transmitted packets dropped because the classification level was out of range.
Drop Tx No IPSOS	Number of transmitted packets dropped because they did not have an IP security label.
No IPSOS ROOMS	Number of packets dropped because the IP header lacked the space to insert an IP security option.
Out Admin Prohibit	Number of ICMP destination unreachable or communication administratively prohibited messages sent.

show ip summary

The **show ip summary** command displays the state of IP, whether it is up and in forwarding mode or in host mode only. The base record controls IP for the entire system.

This command allows for the following command filter and arguments:

-name *<circuit_name>*	Displays information about the specified circuit only.
<ip_address>	Displays information about the specified IP address only.

The output includes the following information:

Configured State	The configured state of IP: enabled or disabled.
Current State	State of IP: down, init (initializing), not pres (enabled but not yet started), or up.

All Subnets	Determines the state of the subnets configured on the router: enabled or disabled.
Number of Routes	Total number of routes configured on the router.
Number of Hosts	Total number of ARP entries that the router requires in its ARP table.
Time-to-Live	Value that determines how long IP retains routes before discarding them.
Maximum Policy Rules	Configured value for the maximum allowable number of policy rules per type (accept or announce) for each protocol.
RIP Diameter	Value or hop count that RIP uses to denote the largest valid metric.
Route Cache Interval	Interval at which routing entries are flushed from the forwarding cache.
Estimated networks	Estimated number of networks that the router will need to keep in its routing table.
Estimated hosts	Estimated number of hosts that the router will need to keep in its host table.
Classless	Applies the default route for unknown subnets, as well as unknown natural class networks.
Forwarding mode	Status of forwarding. Forwarding indicates that the IP host is an IP gateway and is forwarding datagrams received but not addressed to it. Not Forwarding indicates that this IP host is not a gateway.
Route filters	Determines whether route filters are supported: enabled or disabled. If enabled, route filters are supported.

show ip traffic-filter

The **show ip traffic-filter** command displays information about IP traffic filters, such as whether they are enabled, what their status is, and what filter template the router is using.

This command allows for the following command filters and filter arguments:

-circuit <*circuit_name*>	Displays only filters for the specified circuit.
-interface <*name*>	Displays only filters for the specified interface.
-name <*filter_name*>	Displays only the specified filter.
-state {**enabled** | **disabled**}	Displays whether filters are enabled or disabled.
-status {**active** | **inactive** | **error**}	Displays information about filters in the following states: • *active* -- shows only filters that are active. • *inactive* -- shows only filters that are inactive. • *error* -- shows only filters where an error occurred.

The output contains the following information:

Circuit	Circuit to which this traffic filter applies.
IP Interface	Name of the interface using the traffic filter.
Filter Name	Name of the traffic filter.
State	State of the traffic filter: enabled or disabled.
Status	Displays the status of a filter. The state can be: • *active* -- the filter is active. • *inactive* -- the filter is inactive. • *error* -- the filters contain an error.
Hits	Number of matches against this filter.
Prec	Filter precedence.
Type	Specifies that the filter is an inbound filter.

Chapter 2
BGP show Commands

This chapter describes how to use the BCC **show bgp** command to display routing, configuration, interface, and statistical data about the Border Gateway Protocol (BGP) from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show bgp damped-routes

The **show bgp damped-routes** command displays information about BGP damped routes.

This command allows for the following command filters and arguments:

<ip_address>	Displays BGP damped routes for the specified IP address.
<ip_address/prefix>	Displays BGP damped routes for IP addresses with the specified address mask.
-A	Displays the entire routing table. Routes marked with an asterisk (*) are routes in the normal routing table.
-d	Displays the BGP routing pool, including community information.
-i	Displays routes to and from specified BGP peer IDs.
-N	Displays the announce pool.
-p	Displays routes to and from specified BGP peers (local peer address/remote peer address).
-R	Displays the regular expression for AS pattern-matching.
-s	Displays the slot. If the address is 255.255.255.255, the cache will be the internal cache for this slot.

For each damped route, the output depends on the command filters and arguments that you specify.

show bgp errors

The **show bgp errors** command displays error messages generated the last time that a connection between a router and its BGP peer failed. These messages were either received from or sent to the BGP peer. The output includes the following information:

Local Address	IP address of the local interface.
Remote Address	IP address of the peer.
Last Error Code	Last error code and subcode seen by this peer on this connection. If no error occurred, the value of this field is 0. Otherwise, the first byte of this 2-byte octet string contains the error code; the second contains the subcode.
Last error source	Last error source seen by this peer on this connection.

show bgp peers

The **show bgp peers** command displays information about all BGP peers. The output includes the following information:

Local Address/Port	The local interface address and TCP port number.
Remote Address/Port	The peer’s IP address and TCP port number.
Remote AS	Number of the autonomous system (AS) in which the remote peer is located.
Peer Mode	Route server mode of the BGP peer: • 1 -- not a route server connection. • 5 -- peer is a route reflector client. • 6 -- peer is a route reflector in the same RR cluster. • 7 -- peer is a route reflector in a different RR cluster.
State	Current state of the BGP peer: up, down, init (initializing), invalid, or not pres (enabled but not yet started).
BGP Ver	The version of BGP that the BGP peers use to exchange routing information (BGP3 or BGP4).
Routes	Total number of BGP routes received from the peer.

show bgp routes

The **show bgp routes** command displays the BGP routing table.

This command allows for the following command filters and arguments:

<ip_address>	Displays BGP routes for the specified IP address.
<ip_address/prefix>	Displays BGP routes for IP addresses with the specified address mask.
-A	Displays the entire routing table. Routes marked with an asterisk (*) are routes in the normal routing table.
-D	Displays routes damped by route flap damping.
-d	Displays the BGP routing pool, including community information.
-i	Displays routes to and from specific BGP peer IDs.
-N	Displays the announce pool.
-p	Displays routes to and from specific BGP peers (local peer address/remote peer address).
-R	Displays the regular expression for AS pattern-matching.
-s	Displays the slot. If the address is 255.255.255.255, then the cache will be the internal cache for this slot.

The output includes the following information:

Prefix/Length	IP address of the destination subnetwork and the length (in bits) of the IP address prefix.
Peer Address	IP address of the interface on the remote side of this BGP peer connection.
Next Hop Address	Address of the border router that should be used as the next hop for the destination network.
Org	Origin code used to calculate preference: IGP, EGP, Incomplete.
LocPref	Originating BGP speaker’s degree of preference for the advertised route (from -1 through 2,147,483,647). If this attribute has not been provided for this route, the value is -1.

B/U	Best/used indication. Best means that the route is the best BGP route to the destination; used means that the route is in the IP routing table.
I/E	Internal or external BGP route.
Sl	Slot number.

show bgp stats

The **show bgp stats** command displays BGP statistical information. The output includes the following information:

Local Address	IP address of the local interface.
Remote Address	IP address of the remote interface.
Messages Rx	Number of BGP notification messages received.
Messages Tx	Number of BGP notification messages sent.
Updates Rx	Number of BGP update messages received.
Updates Tx	Number of BGP update messages sent.

show bgp summary

The **show bgp summary** command displays a brief summary of BGP information. The output includes the following information:

BGP Information	
BGP State	State of BGP: not pres, disabled, down, init, invalid, or up.
ID	Local BGP identifier.
AS	Local autonomous system number.
Confed ID	Identifier for the BGP confederation to which this peer belongs.
Confed Peers	List of peers of this BGP speaker that are members of other member sub-ASs within the same confederation.
Intra AS Routing	Whether Intra-AS IBGP routing is enabled or disabled.
Dynamic Policy Change	Whether policy change is enabled or disabled.
Multi-hop	Whether multihop is enabled or disabled.
Detect Redundant connections	Whether redundant connections are enabled or disabled.
Cluster ID	Associate the IBGP route server with a cluster.
Injection-time [sec]	Minimum interval (in seconds) between route injections into the routing table.
Max Redundant Routes	Maximum number of redundant routes that BGP received and used, and the total number of redundant routes.
Soloist Slot	Indicates whether BGP is running as a soloist on the specified slot.

BGP3 Information	State of BGP3: configured, not configured, enabled, or disabled.
BGP4 Information	State of BGP4: configured, not configured, enabled, or disabled.

show bgp timers

The **show bgp timers** command displays BGP timer values. The output includes the following information:

Local Address	IP address of the local interface.
Remote Address	IP address of the remote interface.
Hold Cfg Act	Amount of time (in seconds) that either peer waits for a keepalive or update message before declaring the connection down.
Keep Cfg Act	How often (in seconds) BGP issues a keepalive message on this peer-to-peer session.
Up/Down Time (hh:mm:ss)	Length of time since the last reboot of this router.
Last Update (hh:mm:ss)	Time the last BGP update message was received from the peer.

Chapter 3
DVMRP show Commands

This chapter describes how to use the BCC **show dvmrp** command to display routing, configuration, interface, and statistical data about the Distance Vector Multicast Routing Protocol (DVMRP) from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show dvmrp cache

The **show dvmrp cache** command displays the cache forwarding information in each slot on the router.

This command allows for the following command filter and arguments:

-slot *<slot>*	Displays DVMRP routing caches for the specified slot only. If you do not specify a slot, the current slot is used.
<group_address/prefix>	Displays DVMRP cache information for the group addresses specified.

The output includes the following information:

Group Source/Mask	Identifies the group and source/mask of the cache to which the interface belongs.
Interface Name	Name of the interface on which routing cache information is created. The interface name is truncated to 6 characters. Also indicates whether the route is: • I -- Inbound • O -- Outbound
IP Address or Tunnel ID (local/remote)	The IP address of an interface or the tunnel ID (local and remote interface addresses) for which route information is being reported. If you configure this interface as a tunnel, then a tunnel ID (local and remote interface address) is displayed. Otherwise, the IP address of the interface is displayed.
Out State	Indicates whether the interface is active or inactive.
Prune State	The state can be one of the following: • P -- Pruned with timer • N/P -- Not pruned

show dvmrp interfaces

The **show dvmrp interfaces** command displays information about the configured DVMRP interfaces.

This command allows for the following command filters and arguments:

-disabled	Displays information about disabled DVMRP interfaces only.
-enabled	Displays information about enabled DVMRP interfaces only.
<*ip_address*> or <*ip_address_search_pattern*>	Displays information about the DVMRP interfaces of the specified IP address only.

The output includes the following information:

Interface	IP address of the DVMRP interface.
Circuit	Name of the circuit associated with the DVMRP interface.
State	Operational state of the DVMRP interface: up or down.
Metric	Cost (sum of hop metrics along shortest path) of the routes to cross this interface.
TTL Threshold	Minimum IP time to live (TTL) required for a multicast datagram to be forwarded out the interface.
Route Enabled	Whether this circuit is used to propagate routing information, and whether information about the source network associated with this circuit is incorporated into routing updates. The status of this feature is one of the following: • Yes -- Multicast datagrams are forwarded on this circuit in “native mode” (that is, as multicast datagrams). You can configure tunnels on this circuit. • No -- This circuit exists only to support unicast tunnels. The source network associated with this circuit is not incorporated into the routing updates.
Advertise Self	Whether the router advertises its own local networks over this interface: enabled or disabled.

show dvmrp neighbors

The **show dvmrp neighbors** command displays all DVMRP neighbor information or neighbor information for a specified circuit.

This command allows for the following command filter and argument:

-name <*circuit_name*>	Displays information about the specified circuit only.

The output includes the following information:

Circuit	Circuit name of this interface.
Local Tunnel IP	Unicast IP address of the local end of the tunnel. If it is a DVMRP interface, this field indicates “physical.” If it is a tunnel interface, the local IP address of the tunnel is displayed.
Neighbor IP	Unicast IP address of the neighboring router. If it is a DVMRP interface, this field displays the IP address of the first neighbor it learns. If it is a tunnel interface, the IP address of the remote tunnel interface is displayed.
Neighbor Timer	Number of seconds that the router waits to receive a report from a neighbor before considering the connection inactive.

show dvmrp routes detail

The **show dvmrp routes detail** command displays routing information maintained on all DVMRP interfaces (both physical and tunnel).

This command allows for the following command filter and arguments:

-slot <*slot*>	Displays route information for the specified slot only.
<*ip_address/prefix*>	Displays information about the routes for the specified IP addresses.

The output includes the following information:

Source Network	IP address of the source of multicast datagrams.
State	State of the route, as follows: • C -- Child • L -- Leaf • H -- Holddown • l -- Loop neighbor
Local IP	IP address of the local end of the tunnel.
Remote Tunnel	IP address of the remote end of the tunnel.
Dominant Router	Dominant router address for a virtual interface.
Sub Router	Subordinate router address for a virtual interface.

show dvmrp routes main

The **show dvmrp routes main** command displays the main DVMRP routing table. You can specify routes that match an IP address or routes with a source network number that matches a portion of an IP address (for example, 192.34.3.3 or 192.34.0.0/16).

This command allows for the following command filter and arguments:

-slot <*slot*>	Displays routing information for the specified slot only. If no slot is specified, the current slot is used.
<*ip_address*/*prefix*>	Displays information about the routes for the specified IP addresses.

The output includes the following information:

Network/Mask	IP address and mask of the route.
Next Hop Address	If the route is generated from the local interface, the IP address of the local interface is displayed. Otherwise, the IP address of the source that sends this route is displayed.
Slot	Slot number on which this route is learned.
Next Hop CCT	Number of the next-hop circuit on which this route is learned.

Age	Number of seconds since this route was last updated or verified to be correct.
Cost	Cost (sum of hop metrics along shortest path) of the route.
State	State of the main route: • L -- local interface • T -- timed route • G -- garbage route

show dvmrp summary

The **show dvmrp summary** command displays current configuration information for DVMRP. The output includes the following information:

State	State of the DVMRP interface: up or down.
Pruning	Status of the pruning function: enabled or disabled.
Full Update Interval	How often (in seconds) routing messages containing complete routing tables are sent.
Trigger Update Interval	Minimum amount of time (in seconds) between triggered updates.
Leaf Timeout	Value (in seconds) of the leaf timeout (virtual interface holddown) timer.
Neighbor Timeout	Duration of time (in seconds) that a connection with a neighbor is considered active without receiving a subsequent probe or report from the neighbor.
Neighbor Probe Interval	How often (in seconds) DVMRP sends a probe out an interface.
Switch Timeout	Duration of time (in seconds) that DVMRP waits, without receiving a subsequent route update from the original neighbor, before switching to a different neighbor advertising equal cost for this route.
Route Expiration Timeout	Duration of time (in seconds) that a route is considered valid without the receipt of a subsequent update indicating that the route is reachable. This value represents the duration of time that this route will be used. Upon expiration of this timer, this route is advertised as unreachable until it is refreshed or deleted.

Unconfirmed Route Timeout	Duration of time (in seconds) that this route is included in routing updates without the receipt of a subsequent update indicating that the route is reachable. The difference between this value and the Route Expiration Timeout value represents the duration of time that the route will be advertised as unreachable without subsequent updates.
Estimated Routes	Estimated number of routes per slot.
Actual Routes	Number of entries currently in the route table.

show dvmrp tunnels

The **show dvmrp tunnels** command displays DVMRP tunnel configuration information for all circuits, a specified circuit, enabled circuits, or disabled circuits.

This command allows for the following command filters and arguments:

-enabled	Displays information about enabled DVMRP tunnels.
-disabled	Displays information about disabled DVMRP tunnels.
-local <*ip_address*> or <*ip_address_search_pattern*>	Displays information about DVMRP tunnels with the specified local tunnel end point.
-remote <*ip_address*> or <*ip_address_search_pattern*>	Displays information about DVMRP tunnels with the specified remote tunnel end point.
<*ip_address*> or <*ip_address_search_pattern*>	Displays information about the specified IP address.

The output includes the following information:

Local IP	Unicast IP address of the local end point of the tunnel.
Remote IP	Unicast IP address of the remote end point of the tunnel.
State	State of the tunnel: enabled or disabled.
Metric	Cost (sum of hop metrics along shortest path) of the tunnel.
Threshold	Minimum IP time to live (TTL) value for the tunnel (in hops).

Data Encapsulation

Mode that DVMRP uses to encapsulate a tunneled multicast datagram:

- IP-in-IP -- DVMRP encapsulates the tunneled multicast datagram in an IP unicast datagram (ip-in-ip).
- LSSR -- DVMRP loosely encapsulates multicast datagrams using the LSSR option.

Control Encapsulation

Encapsulation mode for IGMP control packets:

- No-encaps -- IGMP sends control messages in regular IGMP packets with the IP protocol type set to IP_PROTOCOL_IGMP.
- Encaps -- IGMP encapsulates control messages inside IP packets with the IP protocol type set to IP_PROTOCOL_IPINIP.

Chapter 4
GRE show Commands

This chapter describes how to use the BCC **show gre** command to display routing, configuration, interface, and statistical data about Generic Routing Encapsulation (GRE) from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show gre logical-ip-tunnels

The **show gre logical-ip-tunnels** command displays information about the logical IP connections configured on a GRE tunnel. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tunnels only.
-enabled	Displays information about enabled tunnels only.
-address <*address*>	Displays information for tunnels configured with the specified IP address only.
-name <*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, displays both the filter flag and value (that is, long notation).
<*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, displays a value only (that is, short notation).

The output includes the following information:

Tunnel Name	Name assigned to the GRE tunnel.
Local Address	IP address of the host interface on the local end of the GRE tunnel connection.
Local State	State of the local host interface: enabled or disabled.
Remote Endpoint Name	Name assigned to the host interface on the remote end of the GRE tunnel connection.
Remote Endpoint Host Address	IP address assigned to the host interface on the remote end of the GRE tunnel connection.

show gre logical-ipx-tunnels

The **show gre logical-ipx-tunnels** command displays information about the logical IPX connections configured on a GRE tunnel. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tunnels only.
-enabled	Displays information about enabled tunnels only.
-address <*address*>	Displays information for tunnels configured with the specified IP address only.
-name <*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, displays both the filter flag and value (that is, long notation).
<*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, displays a value only (that is, short notation).

The output includes the following information:

Tunnel Name	Name assigned to the GRE tunnel.
Local Network Address	Address of the host interface on the local end of the GRE tunnel connection.
Local State	State of the local host interface: enabled or disabled.
Remote Endpoint Name	Name assigned to the host interface on the remote end of the GRE tunnel connection.
Remote Endpoint Host	Name of the host on the remote end of the GRE tunnel connection.

show gre physical-tunnels

The **show gre physical-tunnels** command displays information about the router interfaces at either end of the physical GRE tunnel. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tunnels only.
-enabled	Displays information about enabled tunnels only.
-address <*address*>	Displays information for tunnels configured with the specified IP address only.
-name <*name*>	Displays information for tunnels configured with the specified name only. When you specify this filter, displays both the filter flag and value (that is, long notation).
<*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, displays a value only (that is, short notation).

The output includes the following information:

Tunnel Name	Name assigned to the GRE tunnel.
Encaps Protocols	Protocol that the tunnel is configured for.
Local Address	IP address of the router interface on which the GRE tunnel is configured.
Local State	State of the router interface: enabled or disabled.
Remote Endpoint Name	Name assigned to the interface at the tunnel’s remote end point.
Remote Endpoint Address	IP address of the interface at the tunnel’s remote end point.

Chapter 5
IGMP show Commands

This chapter describes how to use the BCC **show igmp** command to display routing, configuration, interface, and statistical data about the Internet Group Management Protocol (IGMP) from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show igmp base

The **show igmp base** command displays basic configuration information about IGMP. The output includes the following information:

Protocol	The IGMP protocol running on this interface.
State	Current state of IGMP: up, down, init (initializing), or not present (enabled but not yet started).
Estimated Groups	Initial memory allocated to the total number of configured groups.

show igmp groups

The **show igmp groups** command displays information about the IGMP groups registered per interface on the router.

This command allows for the following command filter and argument:

-name <*circuit_name*>	Displays IGMP group information for the specified circuit only.

The output includes the following information:

Group Address	IP address of the IGMP group.
Circuit	Name of the circuit on which the IGMP group has subscribed.
Timer Value	Amount of time, in seconds, until the group subscription times out.

show igmp interfaces

The **show igmp interfaces** command displays information about all configured IGMP interfaces.

This command allows for the following command filter and argument:

-name <*circuit_name*>	Displays IGMP interface information for the specified circuit only.

The output includes the following information:

Circuit	Name of the circuit on which IGMP is configured.
State	State of the IGMP interface: up or down.
Query Rate	How often (in seconds) the router sends general queries on the interface.
DR Timeout	Designated router timeout value (in seconds). This value specifies the amount of time from the last host query message that will be used to determine the loss of the IGMP designated router.
Membership Timeout	Amount of time (in seconds) that a local group membership is valid without the receipt of a subsequent report for that group.
Designated Router	IP address of the current IGMP designated router. If there are multiple routers on a multiaccess network, this value specifies the router sending the IGMP host queries.
Net Version	Version of IGMP that the router is running on this network. A value of 1 means IGMPv1 (the older version of IGMP); a value of 2 means IGMPv2 (the newer version of IGMP).
Relay Type	How the circuit is configured: primary (for primary upstream), backup (for backup upstream), or dwnstream (for downstream).

show igmp stats

The **show igmp stats** command displays statistical information for all IGMP circuits. The output includes the following information:

Circuit
Circuit name on which IGMP is configured.

Designated Router
IP address of the current IGMP designated router. If there are multiple routers on a multiaccess network, this value specifies the router sending the IGMP host queries.

Local Address
IP address currently in use on this circuit. This is the IP address that is being used to generate multicast traffic.

In Datagrams
Total number of datagrams received on this interface.

In Queries
Number of host membership query messages received on this interface.

Out Queries
Number of host membership query messages sent from this interface.

Discards
Number of IGMP messages received on this interface that were discarded due to errors such as bad checksums, illegal message types, and bad values in fields.

Chapter 6
NAT show Commands

This chapter describes how to use the BCC **show nat** command to display data about the Network Address Translation (NAT) protocol from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show nat domains

The **show nat domains** command displays address translations for the domains used in NAT. The output includes the following information:

Original IP Address	Original IP address.
Translated IP Address	Translated IP address.
Inbound Domain	The domain that contains the original address.
Outbound Domain	The domain that contains the translated address.

This **show nat domains** command allows for the following command filters and arguments:

-in-domain <*dname*>	Displays information for the specified domain.
-out-domain <*dname*>	Displays information for the specified domain.
-address <*IP_address*>	Displays domain information for the specified address.

show nat filters

The **show nat filters** command displays statistics about configured NAT source address filters. The output includes the following information:

Starting Address	First IP address for the range of private IP addresses that NAT translates.
Ending Address	Last IP address for the range of private addresses that NAT translates.
Prefix Length	IP address mask that, in conjunction with the base address, defines the address range for the source address filter.
State	State of the source address filter: enabled or disabled.
Domain Name	The domain name to which this source address filter is applied.

This **show nat filters** command allows for the following command filters and arguments:

-address <*IP_address*>	Displays NAT source address filter information for the specified address.
-state {**enabled** | **disabled**}	Displays information for either enabled or disabled NAT source address filters for the domain.
<*dname*>	Displays NAT source address filter information for the specified domain.

show nat interfaces

The **show nat interfaces** command displays statistics for all router interfaces configured for NAT. The output includes the following information:

IP Address	IP address of the NAT interface.
Circuit Name	Name of the Ethernet circuit that the IP interface is configured on.
Domain Name	For unidirectional translations, indicates whether this NAT interface is private or public. For bidirectional translations, indicates the DNS domain name associated with this NAT interface.
Packets TX	Number of NAT translation packets translated on this interface.
Packets RX	Number of NAT translation packets received on this interface.
Drop Count	Number of NAT translation packets dropped by this interface.

The **show nat interfaces** command allows for the following command filters and arguments:

-address <*IP_address*>	Displays interface information for the specified address.
<*dname*>	Displays information for this domain name.

show nat mappings

The **show nat mappings** command displays statistics for all current address mappings in the NAT table on the router. The output includes the following information:

Original IP Address	Original address in a NAT translation.
Translated IP Address	Translated address in a NAT translation.
IP Protocol	IP protocol (UDP or TCP) of this mapping.
Original Port	UDP or TCP port associated with the original IP address.
Translated Port	UDP or TCP port associated with the translated IP address.
Packets TX	Number of packets translated for this address mapping.
Packets RX	Number of packets received for this address mapping.
Last Used	Amount of time (in seconds) since this NAT address mapping generated packet activity.

This **show nat mappings** command allows for the following command filters and arguments:

-in-domain <*dname*>	Displays information for the specified domain.
-out-domain <*dname*>	Displays information for the specified domain.
-address <*IP_address*>	Displays NAT mapping information for the specified address.
type	Displays mapping information for this NAT type: 1-to-1, static, or n-to-1.

show nat pools

The **show nat pools** command displays statistics about configured NAT translation pools. The output includes the following information:

Starting Address	First IP address for the range of public IP addresses that NAT translates.
Ending Address	Last IP address for the range of public addresses that NAT translates.
Prefix Length	IP address mask that, in conjunction with the base address, defines the address range in the translation pool.
State	State of the translation pool: enabled or disabled.
Domain Name	Domain name associated with this translation pool.

This **show nat pools** command allows for the following command filters and arguments:

-address <*IP_address*>	Displays NAT translation pool information for the specified address.
-state {**enabled | disabled**}	Displays information for either enabled or disabled NAT translation pool for the domain.
<*dname*>	Displays NAT translation pool information for the specified domain.

show nat summary

The **show nat summary** command displays the current configuration for NAT parameters set globally on the router. The output includes the following information:

NAT State	Administrative status of NAT on the router: enabled or disabled.
Soloist Slot	Mask value indicating the preferred soloist slot on this router.
Dynamic Aging	Whether the dynamic mapping table entries are timed out when unused: enabled or disabled.
Dynamic Timer	Maximum time (in seconds) before unused NAT mapping table entries are deleted.
Translations Dynamic	Total number of dynamic address mappings in the router's mapping table.
Translations N-to-1	Total number of N-to-1 address mappings in the router's mapping table.
Translations FTP	Number of address mappings in the router's mapping table using FTP.
Install Private Addresses	Whether a private route is visible to public networks (enabled) or not (disabled).

The **show nat summary** command allows for the following command filters and arguments:

-address <*IP_address*>	Displays information for the specified address range.
-state {enabled | disabled}	Displays information for either enabled or disabled interfaces on the router.

Chapter 7
OSPF show Commands

This chapter describes how to use the BCC **show ospf** command to display routing, configuration, interface, and statistical data about the Open Shortest Path First (OSPF) protocol from the management information base (MIB). This chapter includes descriptions of the following **show** commands:

show ospf area

The **show ospf area** command displays a list of configured OSPF areas on the router. For each area, the output includes the following information:

Area ID	Area identifier.
Area State	State of the area: up or down.
Area Type	Specifies whether the area is nonstub, stub, or NSSA.
Authentication	Authentication type for the area: None or Simple Password.

show ospf ase

The **show ospf ase** command displays information about autonomous system external (ASE) advertisements. You can display information for all link state IDs on your router. The output includes the following information:

Area Id Tag	OSPF area ID that receives and generates ASE advertisements.
Link State Id	Network number that this ASE advertisement represents.
Originating Router	Router that generated the advertisement.
Age	Age of the advertisement in seconds.
Metric	Metric of the advertisement; the cost of the external route.
Forwarding Address	Address used to get to this network. If the address is 0, traffic is forwarded to the originating router.
LS Type	Type of OSPF link state advertisement, which can be one of the following: • 0 -- stub • 1 -- router • 2 -- network • 3 -- summary link, IP network • 4 -- summary link, ASBR • 5 -- external • 6 -- group • 7 -- NSSA • 15 -- opaque • 16 -- resource

show ospf base

The **show ospf base** command displays global information for the OSPF router. The base record controls OSPF for the entire router. The output includes the following information:

Router ID	Router identifier, which is unique among all OSPF routers.
State	Whether the OSPF protocol is enabled or disabled on the router.
Area Border Router	Whether the router is an area border router. Valid values are true or false.
AS Boundary Router	Whether the router is an autonomous system boundary router. Valid values are true or false.
NSSA Border Router	Whether the router is an NSSA border router. Valid values are yes or no.
Slot Running Primary	The slot on which the OSPF soloist is running.
Slot Running Backup	The slot on which the backup OSPF soloist is running.

show ospf interface

The **show ospf interface** command displays a table of OSPF interfaces followed by a table of OSPF virtual interfaces. The output includes the following information:

OSPF Interfaces	
IP Address	IP address of the OSPF interface.
Area ID	Area identifier of the interface.
Interface Type	Type of interface link, as follows: • PtoP -- point-to-point interface • BCAST -- broadcast network • NBMA -- nonbroadcast multiaccess network • DFLT -- not configured appropriately • P to MPs -- point-to-multipoint proprietary • IETF -- point-to-multipoint standard • PASSIVE -- passive interface

Interface State	State of the interface, as follows: • Enabled -- interface is operational, allowing neighbor relationships to be formed • Disabled -- interface is not operational
Metric Cost	Cost of using this interface.
Priority	Router priority on this interface; used in multiaccess networks (broadcast or NBMA) for electing the designated router. If the value is 0, this router is not eligible to become the designated router on this network.
Designated Router	IP address of the designated router on the network.
OSPF Virtual Interfaces	
Area ID	Identifier of the transit area that the virtual link traverses.
Virtual Neighbor	Router ID of the virtual neighbor.
State	State of the virtual interface: down or point-to-point.

show ospf io

The **show ospf io** command displays the number and types of OSPF packets that the router has sent and received. The output includes the following information:

Interface	IP address of the OSPF interface.
Hellos Rx	Number of OSPF Hello messages received.
Hellos Tx	Number of OSPF Hello messages sent.
DBs Rx	Number of OSPF database description messages received.
DBs Tx	Number of OSPF database description messages sent.
LS Req Rx	Number of OSPF link state request messages received.
LS Req Tx	Number of OSPF link state request messages sent.
Ls Upd Rx	Number of OSPF link state update messages received.
LS Upd Tx	Number of OSPF link state update messages sent.
LS Ack Rx	Number of OSPF link state acknowledgments received.
LS Ack Tx	Number of OSPF link state acknowledgments sent.
Drop	Number of OSPF messages dropped.

show ospf lsdb

The **show ospf lsdb** command displays information from the OSPF link state database (LSDB).

This command allows for the following command filters and arguments:

<*ip_address*>	Displays OSPF link state data for the specified IP address.
<*ip_address/prefix*>	Displays OSPF link state data for IP addresses with the specified address mask.
-a	Displays the OSPF area.
-A	Displays the entire link state advertisement.
-C	Displays the LSDB count.
-t	Displays the type of OSPF link state advertisement.

The output includes the following information:

Area ID	Identifier of the area from which the LSA was received.
Router ID	Identifier for the originating router in the autonomous system.
Link State ID	Router ID or IP address of the routing domain that the ASE advertisement represents.
LS Type	Type of OSPF link state advertisement, which can be one of the following: • 0 -- stub • 1 -- router • 2 -- network • 3 -- summary link, IP network • 4 -- summary link, ASBR (AS boundary router) • 5 -- external • 6 -- multicast • 7 -- NSSA (not-so-stubby area) • 15 -- opaque • 16 -- resource
Forward Address	Address used to get to this network. If the address is 0, traffic is forwarded to the originating router.
Age	Age of the advertisement in seconds.

show ospf neighbors

The **show ospf neighbors** command displays information about all OSPF neighbors. The output includes the following information:

IP Interface
IP address of the interface for the neighbor (OSPF dynamic and configured neighbors only).

Area ID
Area identifier of the transit area (OSPF virtual neighbors only).

Router ID
Router identifier.

Neighbor IP Address
IP address of the neighbor.

State
State of the neighbor, which is one of the following:

- Down -- Neighbor is not operational. This state can occur only if the neighbor is configured for nonbroadcast multiaccess networks.
- Attempt -- Router is trying to establish communication with the neighbor; can occur only if the neighbor is configured for nonbroadcast multiaccess networks.
- Init -- Router has received the neighbor’s Hello packet, but the packet does not include this router in its list.
- Two Way -- Router and neighbor receive each other’s Hello packets.
- Exch Start -- Router and neighbor are negotiating a master/slave relationship for the database exchange process.
- Exchange -- Router and neighbor are exchanging their link state databases.
- Loading -- Router and neighbor are synchronizing their link state databases.
- Full -- Router and neighbor have fully synchronized databases.

Type
Type of neighbor:

- Dynamic -- Router and neighbor learn about each other on broadcast or point-to-point networks.
- Cfg. -- Static configuration of neighbors, which occurs on nonbroadcast multiaccess networks.
- Virtual -- Configured neighbor over a virtual link.

show ospf nssa-range

The **show ospf nssa-range** command displays a list of configured OSPF NSSA address ranges on the router. For each NSSA address range, the output includes the following information:

Network Address	Single IP address for a group of NSSA subnets. The network address, together with the network mask, specifies the subnets to be grouped in this NSSA range.
Network Mask	Network mask for a group of NSSA subnets.
Action	Indicates whether the NSSA border router advertises type 5 LSAs for the NSSA address range. Valid options are advertise or block.
External Route Tag	Indicates the value to be inserted in the external route tag field of translated type 5 LSAs configured for a type 7 address range.

Index