IP Transport

Description

4/1551-LZA 701 6012/1 Uen A2

Contents

1 Introduction

This document describes the management model and concepts for managed area *IP Transport* for Pico Radio Nodes. It provides a description of how the area is modelled, the functions related to the area, and how they are managed.

A managed area represents a group of functions and the corresponding Managed Objects (MO) within the node. The grouping of managed areas defines areas relatively independent of one another.

This managed area represents the basic functions and MOs for IP transport, IP transport security, and IP based Operation and Maintenance (O&M) node access.

1.1 Related Documents

The following documents relate to this managed area:

- *Security for O&M Node Access* describes the functions and MOs used to secure O&M access to the node.
- *Network Synchronization* describes the functions and MOs used to synchronize the nodes of a network to a reference clock.
- For WCDMA, the *WCDMA RAN IP Transport Network Configuration* document describes recommended alternatives for IP transport configurations for all types of logical interfaces in WCDMA RAN.
- For LTE, the *Transport Network Configuration* document describes recommended alternatives for IP transport configurations for all types of logical interfaces in LTE RAN.

2 Functions and Concepts

This section describes the functions and concepts that apply to operation and maintenance.

2.1 Basic Concepts

This section describes the terminology used in this document.

2.1.1 Traffic Types

The following are traffic type definitions used in this document.

O&M Traffic Operation and Maintenance traffic over the WCDMA Mub interface as described in *Node Description* and correspondingly for LTE over the Mul interface as described in *System and Node Description*.

Iub Traffic For WCDMA, User Plane and Control Plane traffic over the Iub interface, as described in *Node Description*. Also referred to as WCDMA traffic in some MO descriptions in the RBS 6402 *Managed Object Model (MOM) RBS*.

S1/X2 Traffic For LTE, User Plane and Control Plane traffic over the S1 and X2 interfaces, as described in *System and Node Description*.

2.1.2 Inner and Outer IP Hosts

An IP host that provides the outer, public, IP address for an IPSec tunnel is called an outer IP host or a public IP host.

An IP host that provides the inner IP address for an IPSec tunnel is called an inner IP host.

2.1.3 DHCP Options

The Dynamic Host Configuration Protocol (DHCP) provides an internal framework for passing configuration information in the network. Configuration parameters are carried in tagged data items called options that are stored in protocol messages exchanged between the DHCP server and its clients. See Table 3.

Standard DHCP options are defined in *RFC 2132*.

2.1.4 IPSec VPN and IPSec tunnel

A Virtual Private Network (VPN) extends a private network across a public network. IPSec is used to build a VPN over an untrusted Radio Access Network (RAN). An IPSec VPN consists of one Internet Key Exchange (IKE) Security Association (SA) and one or more IPSec tunnels.

An IPSec tunnel indicates one bidirectional child SA pair.

For information about re-key time intervals, see *IP Security*.

2.1.5 IPv4 Address

The IPv4 address is used to find the correct recipient in the IPv4 network. It is 32 bits long, composed of four 8-bit octets. The most significant part of the IP address is to address the actual IP network. The least significant part addresses the host on the network. The number of octets used for the network part depends on the size of the network. The larger the network, the fewer octets for the network part.

To use IP addresses in a efficient way, subnetting is used to divide an IP network into subnets, see Figure 1. A subnet mask determines how to divide the address into the network, subnet and host parts. The Network Prefix Length is defined as the subnet mask length, that is, the number of bits in the subnet mask.

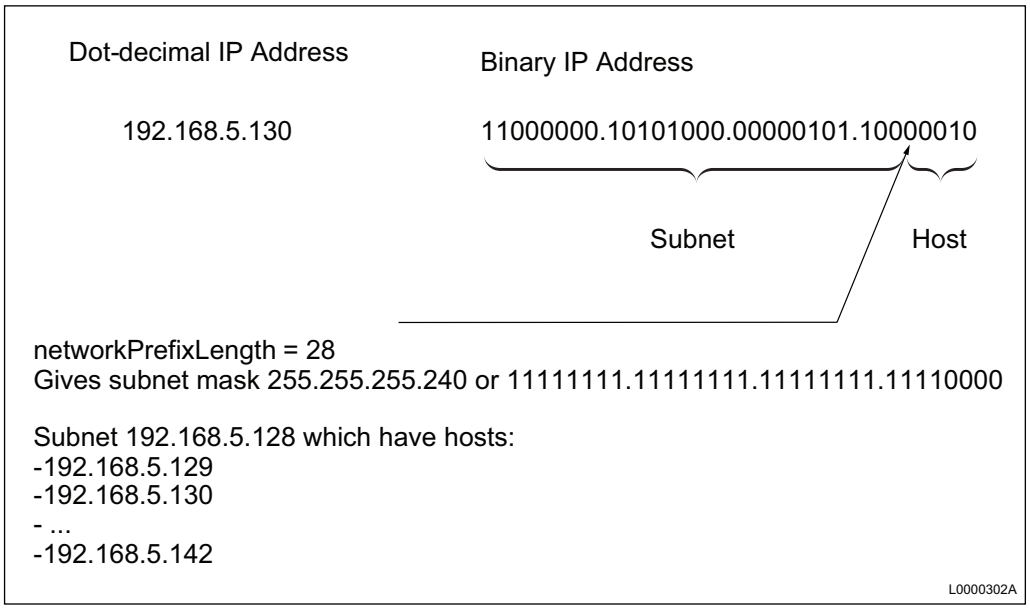

Figure 1 Subnetting

2.1.6 IPv6 Address

This section is valid for LTE only.

The IPv6 address is used to find the correct recipient in the IPv6 network. The address is 128 bits long. There are several address types in IPv6. Two of them are the link local unicast and the global unicast address.

In the majority of the networks, an IPv6 network node has at least one link local unicast address and at least one global unicast address.

The link local address is typically constructed directly from the physical Ethernet interface MAC address. It is only used for communication within the same layer 2 network.

The global unicast address is unique in the layer 3 network and is used for most of the communication. The global unicast address is divided into two parts.

The X most significant bits are termed network prefix. It is divided into one part containing a global routing prefix and another part containing a subnet identity. The 128 minus X least significant bits are termed the interface ID. In the IPv6 addressing architecture, most of the global unicast addresses uses a network prefix length equal to 64.

An IPv6 address is preferably represented as X:X:X:X:X:X:X:X

X represents one to four hexadecimal digits of the eight 16-bit pieces of the address, see page 4.

A special syntax, "::", can be used to simplify writing of addresses containing zeros. The use of "::" indicates one or more groups of 16 bits of zeros. The "::" can only be used once in an address.

```
ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
2001:DB8:0:0:8:800:200C:417A
```

Example 1 IPv6 address

2.2 Network Element Communication

This section gives a high-level description of the communication between the network elements.

2.2.1 Security Gateway

A Security Gateway (SEG) is an IPSec supported device used to encrypt and decrypt data between a Trusted and an Untrusted Transport Network. This section describes general requirements and settings for communication between the SEG and the RBS.

Independent of cell site, the SEG must support the following requirements:

- Required certificates:
  - Root certificate from the Certificate Authority (CA) that issues the Ericsson vendor credentials. This is used to verify that the connecting equipment originates from an Ericsson factory.
  - Root certificate from the CA that issues the operator network elements credentials. This is used to trust the operator-owned cell site equipment.
  - Root certificate from the CA that issues the operator SEG credentials. This is used to verify the correctness of the node's own operator node certificate. Using this certificate, the SEG trusts its own node certificate.
  - OSS-RC operator node certificate with the corresponding private key. This is used to prove to the cell site that the SEG is a genuine operator SEG and must be used during mutual authentication when the permanent IPSec VPN is established.
- Create RSA key pairs and send certificate request according to standard PKCS#10 for certificate signing.
- Diffie-Hellman groups 2 and 14.
- Answer Dead Peer Detection (DPD) messages from cell site.
- Encapsulation Security Payload (ESP) in tunnel mode.

The SEG must support the following Pico Radio Node specific requirements:

- Authentication algorithms (SHA-1,SHA-2).
- Encryption algorithms (AES).
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration Payload (CP) for autointegration. IKEv2 for LMT (Local Maintenance Terminal) integration, on-site configuration.

For detailed information, refer to the vendor's product information.

Figure 2 shows the interaction between the RBS and SEG logical interfaces. The RBS behaves as three logical IPSec boxes, that all use the same IP interface. The boxes connect the temporary O&M, the permanent O&M, and the permanent RAN IPSec VPN. The SEG is configured with three IKE gateways that connect to the three logical RBS IPSec boxes. The three IP pools are configured in the Remote Authentication Dial In User Service (RADIUS) server or in the DHCP server.

Note: Whether the configuration is done in the RADIUS server or the DHCP server depends on the IKEv2 CP implementation of the SEG.

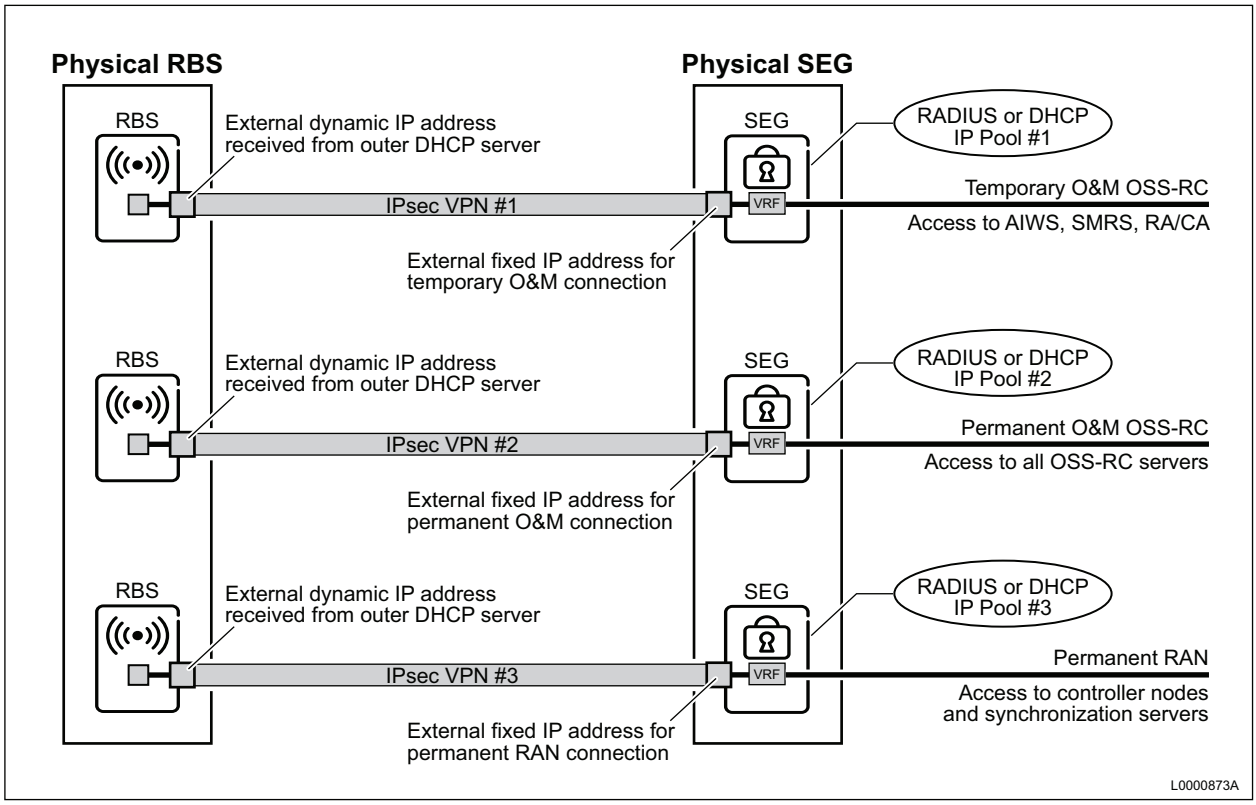

Figure 2 SEG Logical Interfaces

2.2.2 DHCP Server

A DHCP server ensures RBS IP connectivity to the Transport Network and O&M.

Depending on the SEG solution, it is necessary to deploy two DHCP servers, one inner and one outer server in the IPSec solution. In this case, the inner DHCP is located in the Trusted Transport Network and the outer DHCP is located in the Untrusted Transport Network. See Figure 4.

The outer DHCP server must supply the RBS with the following attributes:

- IP attributes for routing in the Transport Network
  - RBS outer IP address
  - RBS own IP subnet
  - RBS default gateway
- SEG IP address, that is the external fixed IP address for temporary O&M connection
  - Alternative 1: DHCP option 241

  - Alternative 2: Domain Name System (DNS) address, option 6 and domain name, option 15

    Note: The SEG IP is only needed when IPSec is an integral part of the auto-integration function.

- Autointegration Web Service (AIWS) address

  - Alternative 1: domain name, option 15

  - Alternative 2: option 72

    Note: The preferred way of resolving the AIWS address is through the inner DNS server. Otherwise the AIWS address must be known in the public or outer DHCP server which is not owned by the operator. The inner DNS address is supplied as an IKEv2 CP attribute by the SEG to the RBS.

The inner DHCP server must supply the RBS with the following attributes:

- RBS inner IP addresses
- RBS inner IP networks
- Inner DNS IP address

Note: Depending on the SEG implementation of IKEv2 CP these attributes can be provided through a RADIUS server instead.

2.2.3 Domain Name System

The SEG gateway address, an external fixed IP address for a temporary O&M connection can be alternatively provisioned through the outer DNS server if the DHCP option 241 is not used or supported by the outer DHCP server. In this case, the outer DHCP server must provide the RBS with the outer DNS address, option 6, together with the domain name, option 15.

The AIWS address is provisioned through the inner DNS server. The RBS is provided with the inner DNS address as an IKEv2 CP attribute. The RBS uses the domain name provided from the outer DHCP server and the inner DNS address to resolve the AIWS address through the inner DNS server.

As a part of the Small Cell Instant Connect (SCIC) service, the Ericsson Global Integration Server (EGIS) address is provisioned through the outer DNS. The RBS uses the EGIS address to send a HTTPS-request to EGIS, when integrating an RBS in an untrusted network, see Section 2.2.5 on page 8.

Note: The DNS is non-OSS-RC equipment.

2.2.4 RADIUS Server

The use of IKEv2 CP by the RBS puts a requirement on the IKE responder (SEG) to provide the RBS with provisioning information. Depending on the SEG implementation this information can either be acquired from a specified source such as a RADIUS server, or it can be returned from a DHCP server through a RADIUS server.

Typically the SEG uses an external RADIUS interface for providing the provisioning information to the RBS, that is the SEG makes a RADIUS access request to an external RADIUS server. The RADIUS server makes a DHCP discover activity for the inner IP address which includes the unique client-ID, based on IKE ID, to an external DHCP server. The RADIUS service is used as the DHCP Relay .

Note: Three different IP pools are used in the inner DHCP server for allocating inner IP addresses. One IP pool is used for allocating the temporary O&M IP addresses, a second pool for allocating permanent O&M IP addresses, and a third pool for allocating permanent RAN IP addresses.

Alternatively, the provisioning information can be provided to the Pico Radio Nodes directly from the RADIUS server through internal IP pools managed by the RADIUS server, if this functionality is supported by the RADIUS server.

For more information about RADIUS server, refer to *RFC 2865* and *RFC 2866*.

2.2.5 Ericsson Global Integration Service

The EGIS provides the FQDN or IP addresses to the SEG and the AIWS server to the RBS. EGIS can be used when integrating an RBS in an untrusted network. The RBS sends an HTTPS request to EGIS and uses the vendor credentials for authentication. The EGIS responds to the request with the IP addresses to the SEG and the AIWS server. To be able to use EGIS during autointegration, the operator must send data for the RBS to EGIS, see *Add RBS*. EGIS makes it possible for operators to use shared outer DHCP servers.

2.3 IP Transport Configuration Variants

This section describes the IP transport configuration variants that are available to meet the varying requirements of transport networks. The main difference between the variants is the use of IPSec to secure IP transport and the use of Virtual Local Area Network (VLAN) tags to separate O&M traffic from Iub (WCDMA) or S1/X2 (LTE) traffic for different subnetworks.

Wi-Fi traffic is either VLAN tagged or untagged in each of the configuration variants.

The RBS integrated IPSec function makes it possible to connect the RBS directly to the Untrusted Transport Network and still protect the O&M and RAN

traffic, see Figure 3. The outer IP address of the RBS is part of the transport network and the inner IP address is part of the overlay VPN. The same outer IP address can be used for both IPSec protected and non-protected traffic.

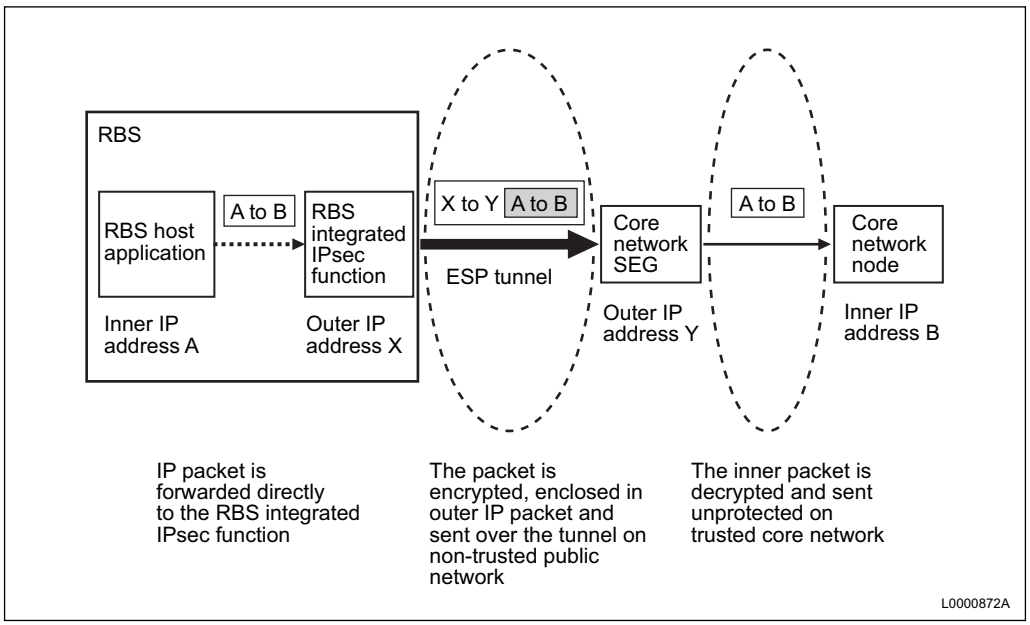

Figure 3 Packet Transfer in the IPSec Solution

The following topology figures are high-level descriptions of the network and some of the integrated network elements. Figure 4 shows an IPSec solution where an IPSec tunnel protects the traffic in the Untrusted Transport Network and where two DHCP servers are used. Figure 5 shows a solution with unprotected traffic in a Trusted Transport Network.

The use of IPSec is highly recommended. However, IPSec can be omitted in exceptional cases if the transport network and the deployment environment is considered secure.

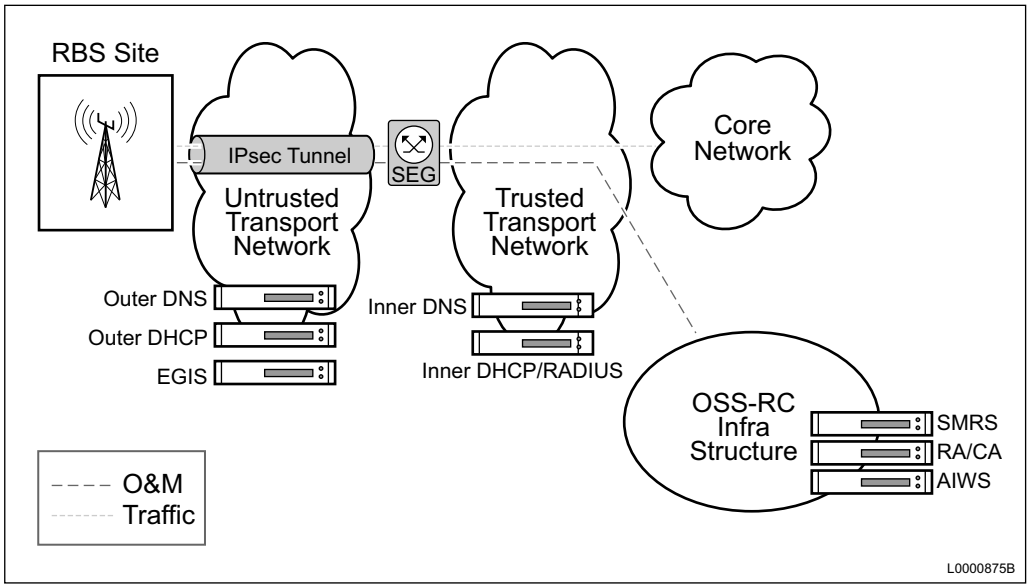

Figure 4 Network Topology - with IPSec

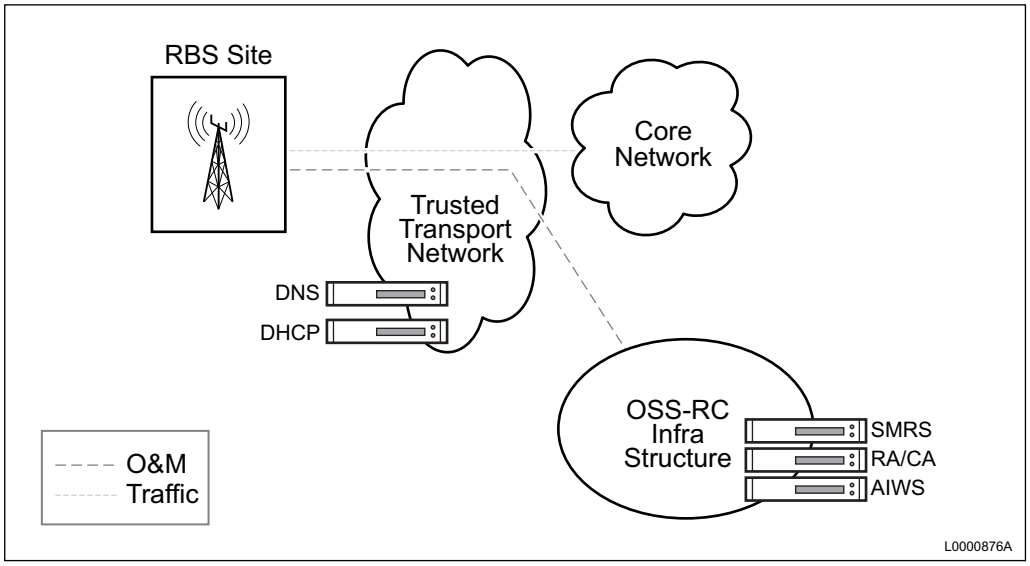

Figure 5 Network Topology - without IPSec

Permanent IPSec tunnels and VLAN tagging is set up during autointegration based on the Initial Configuration File (ICF). The Base Station Integration Manager (BSIM) Operations Support System for Radio and Core (OSS-RC) module generates the ICF based on an ICF template and other data. BSIM uses different ICF templates for the different IP transport configuration variants. Refer to Section 2.5 on page 16 and Section 3.2 on page 32 for more information about the ICF template variants.

To introduce or remove IPSec for a commissioned RBS, that is, an RBS already taken into service, the node must be reset to factory default settings and a new autointegration session must be performed. Refer to Section 4.11

on page 41 for more information. VLAN tagging of a commissioned node can be reconfigured without performing a new autointegration session.

Table 1 provides a configuration variant overview. Transport network requirements are available in Section 2.6 on page 17.

Refer to Section 3.2 on page 32 for information about configuration variant MOs.

O&M, Iub (WCDMA) or S1/X2 (LTE), and Wi-Fi traffic is transported through one Ethernet interface.

For WCDMA, IPv6 is not supported in the current release.

Table 1 IP Transport Configuration Variants

Configuration Variant	IPSec	VLAN Alternatives	Traffic Separation Possible O&M / Iub (WCDMA) or S1/X2 (LTE)
Two Permanent IPSec Tunnels, Untagged or Common VLAN Section 2.3.1 on page 11	Yes	• No VLAN, untagged traffic • One common VLAN ID for O&M traffic and Iub (WCDMA) or S1/X2 (LTE) traffic	Yes, through subnetwork separation
No IPSec, Traffic Separation Section 2.3.2 on page 13	No	• Two separate VLAN IDs for O&M traffic and Iub (WCDMA) or S1/X2 (LTE) traffic	Yes, through VLAN tagging
No IPSec, No Traffic Separation Section 2.3.3 on page 13	No	• No VLAN, untagged traffic • One common VLAN ID for O&M traffic and Iub (WCDMA) or S1/X2 (LTE) traffic	No

2.3.1 Two Permanent IPSec Tunnels, Untagged or Common VLAN

As described in Figure 6 and Figure 7, O&M traffic and Iub (WCDMA) or S1/X2 (LTE) traffic is transported through separate IPSec tunnels, which are terminated in one outer IP host on the RBS. The outer host interface can either be tagged with a VLAN ID or it can be untagged. If the interface is tagged, the same VLAN ID applies to both O&M traffic and Iub (WCDMA) or S1/X2 (LTE) traffic. The two traffic types are terminated in two separate inner IP hosts in the RBS.

Traffic separation is possible. Different subnetworks must be used for the traffic types.

The inner host addresses are allocated from the Security Gateway (SEG) using IKEv2.

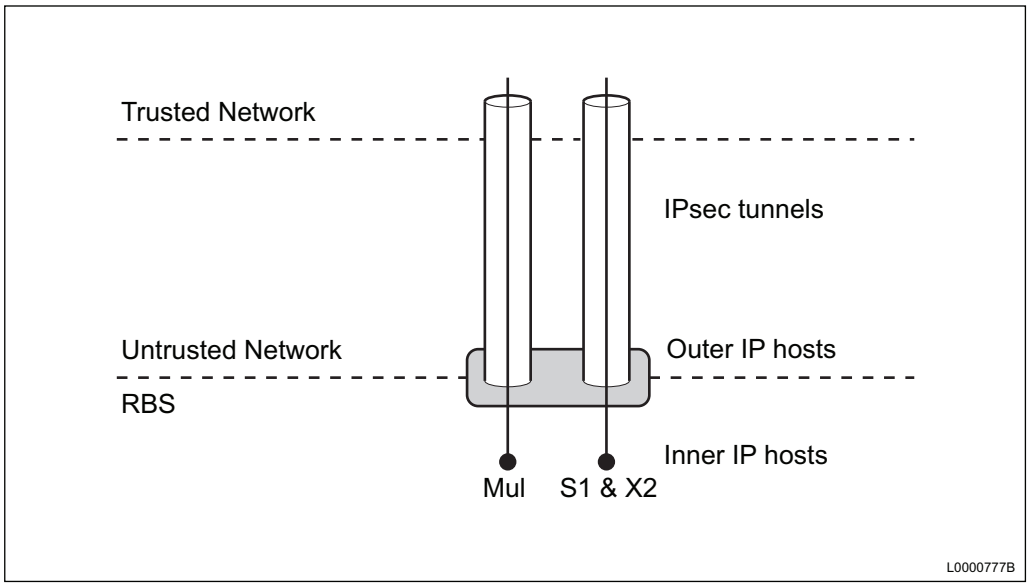

Figure 6 Two Permanent IPSec Tunnels, LTE

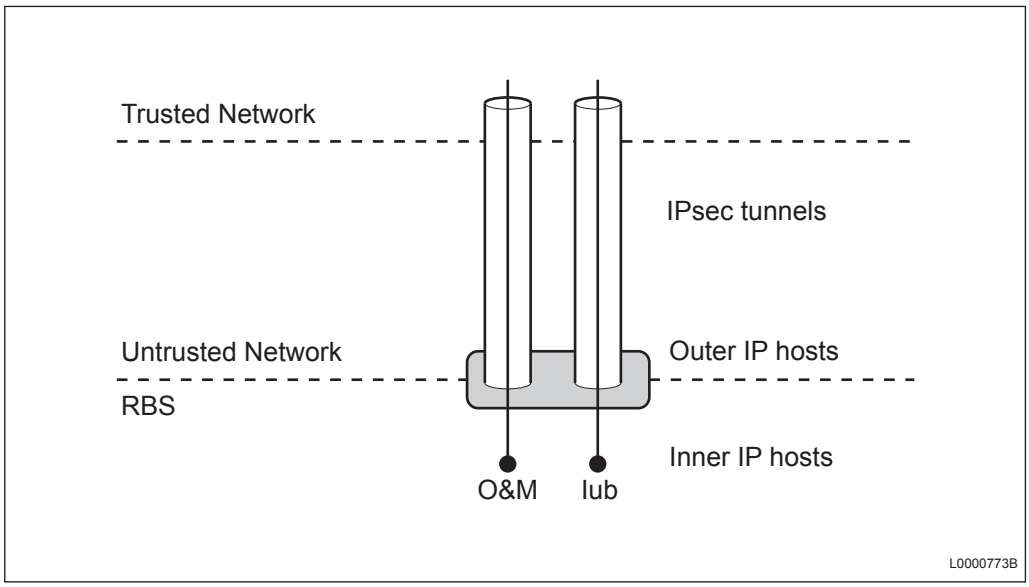

Figure 7 Two Permanent IPSec Tunnels, WCDMA

Refer to Section 2.7 on page 20 for more information about IPSec negotiation.

Refer to Wi-Fi Solution Library for information on how to configure Wi-Fi IPSec.

2.3.2 No IPSec, Traffic Separation

In this configuration variant three IP hosts terminate O&M and Iub (WCDMA) or S1/X2 (LTE), and Wi-Fi traffic respectively. IPSec is not used for either O&M, Iub or S1/X2 traffic.

VLAN IDs are used to separate traffic types for different subnetworks. Wi-Fi traffic may have its own VLAN or use the same VLAN as O&M or Iub traffic for WCDMA and Mul or S1/X2 traffic for LTE.

2.3.3 No IPSec, No Traffic Separation

In this configuration variant three IP hosts terminate O&M, Iub (WCDMA) or S1/X2 (LTE), and Wi-Fi traffic respectively. IPSec is not used for either O&M, Iub or S1/X2 traffic.

All traffic types are either untagged or tagged with one common VLAN ID. No traffic separation is possible.

Note: If this configuration variant is used, the ICF must first be manually edited. See Section 2.5 on page 16.

2.4 IPSec Addressing Options

This section describes how to configure different IPSec addressing options.

2.4.1 High-Level Architecture

IPSec architecture based on two IPSec tunnels are supported. This architecture is defined by the following conditions:

- One public outer IPv4 address
- One IKE SA with one private inner IPv4 address for O&M
- One IKE SA with one private inner IPv4 address for traffic
- Different IKE IDs used for the O&M tunnel and the traffic tunnel to support termination to the same SEG instance

The MOM attributes affect IPSec the following way:

- *Host* =1 is for inner O&M IP address
- *Host* =2 is for inner traffic IP address
- *Host* =3 is for outer IP address

- *Host* =3, *IpSecTunnel* =1 correspond to the tunnel for *Host* =1
- *Host* =3, *IpSecTunnel* =2 correspond to the tunnel for *Host* =2
- *remoteTrafficSelector* (TSr) determines routing for the tunnels
- *localTrafficSelector* (TSi) triggers whether or not IKEv2 CP is used. When TSi is provided, IKEv2 without CP is used. If not provided, IKEv2 CP is used

2.4.2 IKEv2 without Configuration Payload

The following is valid for IKEv2 without CP:

- The node receives proposals for inner IPv4 addresses through the ICF/MOM
- *Host* =3, *IpSecTunnel* =x, *localTrafficSelector* must exist in ICF/MOM and must contain the inner IP address proposal
- *Host* =[1,2], *InterfaceIPv4* =1 must exist in ICF/MOM and must contain the IP address proposal
- The node provides value from *localTrafficSelector*
- The node provides value from *remoteTrafficSelector*
- CP is never included in the IKEv2 handshake procedure

2.4.3 IKEv2 CP with Proposal

The following is valid for IKEv2 with proposal:

- The node receives proposals for inner IPv4 addresses through the ICF/MOM
- *Host* =3, *IpSecTunnel* =x, *localTrafficSelector* must not exist in ICF/MOM
- *Host* =[1,2], *InterfaceIPv4* =1 must exist in ICF/MOM and must contain the IP address proposals
- The node provides `0.0.0.0/0` in TSi and proposal IPv4 address in `CP(CFG_REQUEST)=(INTERNAL_IP4_ADDRESS(a.b.c.d)`
- By default the node provides `0.0.0.0/0` in TSr.

  Optionally, the TSr value can be overridden by providing *Host* =3, *IpSecTunnel* =x, *IpsecPolicy* , *remoteTrafficSelector* for *IpSecTunnel* in the ICF/MOM

- SEG validates the proposals and provides inner IP addresses through `CP(CFG_REPLY)=INTERNAL_IP4_ADDRESS(...)`

  Note: The SEG selects inner IP addresses. Thus, they can differ from those requested in the proposal

2.4.4 IKEv2 without Proposal

The following is valid for IKEv2 without proposal:

- The node does not have any knowledge about inner IP addresses before the IKEv2 negotiation
- *`Host`* =3, *`IpSecTunnel`* =x. *`IpsecPolicy`* , *`localTrafficSelector`* must not exist in ICF/MOM
- *`Host`* =[1,2], *`InterfaceIPv4`* =1 must not exist in ICF/MOM
- The node provides `0.0.0.0/0` in TSi and empty IP address in `CP(CFG_REQUEST)=(INTERNAL_IP4_ADDRESS()`
- By default the node provides `0.0.0.0/0` in TSr

  Optionally, the TSr value can be overridden by *`Host`* =3, *`IpSecTunnel`* =x, *`IpsecPolicy`* , *`remoteTrafficSelector`* for *`IpSecTunnel`* in the ICF/MOM
- The SEG assigns and provides inner IP addresses through `CP(CFG_REPLY)=INTERNAL_IP4_ADDRESS(...)`

2.4.5 IKEv2 Configuration Summary

Table 2 describes the IKEv2 configurations in short.

Table 2 IKEv2 Configuration Variants

Configuration Variant	localTrafficSelector (TSi)	remoteTrafficSelector (TSr)	Host=[1,2], InterfaceIPv4
IKEv2 without Configuration Payload	Mandatory Contains inner IPv4 subnet	Mandatory Contains remote inner IPv4 subnet(s)	Mandatory Contains inner IPv4 address
IKEv2 CP with Proposal	Not provided	Optional Contains TSr proposals	Mandatory Contains inner IPv4 address proposals

Configuration Variant	localTrafficSelector (TSi)	remoteTrafficSelector (TSr)	Host=[1,2], InterfaceIPv4
IKEv2 CP without Proposal	Not provided	Optional Contains TSr proposals	Not provided

2.5 ICF Templates

This section describes the ICF templates used for the different configuration variants.

The following ICF templates are provided:

- Without IPSec. For LTE, see *ICF Template Trusted* and for WCDMA, see *ICF Template Trusted*.
- With IPSec. For LTE, see *ICF Template with IPsec* and for WCDMA, see *ICF Template with IPSec*.
- Without IPSec for LMT integration, on-site configuration. For LTE, see *ICF Template Trusted Semi-AI* and for WCDMA, see *ICF Template Trusted Semi-AI*.
- With IPSec for LMT integration, on-site configuration. For LTE, see *ICF Template IPSec Semi-AI* and for WCDMA, see *ICF Template IPSec Semi-AI*.

For LTE configuration variant *No IPSec, No Traffic Separation*, the *ICF Template Trusted* or the *ICF Template Trusted Semi-AI* must be manually edited.

For WCDMA configuration variant *No IPSec, No Traffic Separation*, the *ICF Template Trusted* or the *ICF Template Trusted Semi-AI* must be manually edited.

The traffic VLAN code sequence in Example 2 must be removed from the template.

If a remote traffic selector is to be defined, the value `addressRange` must be changed in *ICF Template IPSec Semi-AI* (LTE) or *ICF Template IPSec Semi-AI* (WCDMA), see Example 3. This is only valid for configuration variant *Two Permanent IPSec Tunnels, Untagged or Common VLAN* when using LMT integration, on-site configuration. If `addressRange` is not changed in the ICF template the LMT integration, on-site configuration fails.

Note: 0.0.0.0/0 is not an accepted value for `addressRange` .

```
<VlanPort xmlns="urn:com:ericsson:EPIC_T_L2_VlanPort"
xc:operation="create">    <vlanPortId>2</vlanPortId>
```

```
<vlanId>%trafficVlanId%</vlanId>    <userLabel>Traffic
Vlan interface.</userLabel> </VlanPort>
```

Example 2 Traffic VLAN Code Sequence

```
<!--AddressRange must be updated operator value; example
1.2.3.4/5 (IPv4 address/prefix length) <IpsecTunnel
xmlns="urn:com:ericsson:ecim:MSRBS_V1_T_IPsec_Tunnel">
<ipsecTunnelId>1</ipsecTunnelId>
<IpsecPolicy>               <ipsecPoliciyId>1</
ipsecPolicyId>               <remoteTrafficSelector
struct="TrafficSelector">
<addressRange>"Add Operator value here"</
addressRange>               </
remoteTrafficSelector>        </IpsecPolicy> </
IpsecTunnel>
```

Example 3 Defining Remote Traffic Selector

2.6 Transport Network Requirements

This section describes the Transport Network Requirements from a general perspective and for the Untrusted and Trusted Transport Networks.

The following non-OSS-RC nodes are part of the requirements:

- DHCP server
- DNS
- SEG

Refer to *OSS-RC CPI Library* for Pico Radio Node requirements on OSS-RC nodes.

2.6.1 General Transport Network Requirements

This section contains transport network requirements that apply to all configuration variants in Section 2.3 on page 8.

The following rules and requirements apply to all configuration variants:

- The same IP address must not be reused for different IP hosts.
- During autointegration, the AutoIntegration Web Service (AIWS) server address must be provided by an outer DHCP server or an inner DNS server on RBS request:
  - For DHCP the IP address must be provided in option 72, see .

– For DNS the IP address must be paired to `aiws.ai.ericsson` or `aiws.ai.domain`. Replace `domain` with the appropriate domain name. The domain name used must be provided to the node in standard DHCP option 15.

Note: As an option, Fully Qualified Domain Name (FQDN) can be set through the On-Site RBS Integrator (ORI). This setting overrides the hardcoded `aiws.ai` address. See *Integrating RBSs On-Site Using ORI*.

2.6.2 Transport Network Requirements for Untrusted Transport Networks

Use an IPSec solution, that is, the *Two Permanent IPSec Tunnels, Untagged or Common VLAN* configuration variant described in Section 2.3.1 on page 11 for Untrusted Transport Networks.

The transport network requirements for the configuration variant are the following:

- The external fixed SEG address for the temporary O&M IPSec tunnel must be provided by EGIS, the outer DHCP server or the outer DNS on the RBS request:

  – EGIS provides the SEG address when responding to the HTTPS request sent by the RBS.

  – For the outer DHCP server, the SEG address must be provided in option 241. If VLAN is used, the DHCP server must reside within the same VLAN as the RBS.

    The DHCP server provides a SEG address for creating an initial temporary IPSec VPN with one IPSec tunnel. SEG addresses for permanent IPSec tunnels are defined in the ICF.

  – For the outer DNS, the SEG address must be paired to `secgw.ai.ericsson` or `secgw.ai.domain`. Replace `domain` with the appropriate domain name. The domain name used must be provided to the node in standard DHCP option 15.

    Note: As an option, Fully Qualified Domain Name (FQDN) can be set through the On-Site RBS Integrator (ORI). This setting will override the hardcoded `secgw.ai` address. See *Integrating RBSs On-Site Using ORI*.

- If EGIS is used the RBS must receive the EGIS address from the outer DNS. EGIS provides the RBS with the SEG address and the AIWS server address in response to an HTTPS request, see Section 2.2.5 on page 8.

- If the AIWS server address is requested from a DNS, it must be requested from the inner DNS. That is, the server must reside in the Trusted

Transport Network, as the address is requested after the IPSec tunnels are established. It is recommended for Untrusted Transport Networks that the AIWS is resolved through EGIS or the inner DNS.

- For WCDMA, the SEG needs to support multiple traffic selectors deployed in multiple IP subnets.

Note: Due to limitations in OSS-RC and in the RBS (LTE) or RNC (WCDMA), the permanent inner IP addresses for O&M and S1/X2 (LTE) or Iub (WCDMA) traffic must not change as this results in lost connections with the RBS. Due to this, the inner DHCP must guarantee that the assigned IP addresses do not change. The inner IP addresses allocated to the RBS must therefore be mapped to specific IP addresses defined in the RADIUS or DHCP pools, based on IKE ID.

Refer to Section 2.7 on page 20 for more information about IPSec negotiation.

2.6.3 Transport Network Requirements for Trusted Transport Networks

The use of IPSec is highly recommended since the RBS site can be located at an untrusted location. The IPSec is used to authenticate the RBS as a remote peer in this case, since the RBS can be exposed and tampered with, even if it connects to a trusted transport network. However, IPSec can be omitted in exceptional cases if the transport network and the deployment environment is considered secure. For such cases, use configuration variant *No IPSec, Traffic Separation* or *No IPSec, No Traffic Separation*, described in Section 2.3.2 on page 13 and Section 2.3.3 on page 13.

The RBS expects to receive unique IP addresses for O&M and Iub (WCDMA) or S1/X2 (LTE) hosts as replies to requests with the following DHCP client identifiers:

- `<RBS serial number>-rbs-wcdma` for Iub (WCDMA)
- `<RBS serial number>-rbs-lte` for S1/X2 (LTE)
- `<RBS serial number>-rbs-oam` for O&M

Mapping to inner IP addresses is performed in the inner DHCP based on client-IDs.

The RBS expects to receive IP addresses in the DHCP options described in Table 3.

Table 3 DHCP Options

DHCP option	Usage
Option 1	Subnetwork mask

DHCP option	Usage
Option 3	Default router
Option 6 (optional)(1)	DNS server address
Option 15(optional)(1)	Domain name
Option 43	The Wi-Fi Controller (WIC) IP address(2)
Option 72	AIWS server address
Option 241 (optional)(1)	Initial O&M IPSec tunnel address(3)

(1) Either option 6 and 15 are used to provide the SEG IP address (used for the initial O&M IPSec tunnel) or option 241.

(2) Only required if RBS is equipped with optional Wi-Fi unit and if the address is not configured in DNS

(3) This IPSec tunnel is consistent.

When Iub (WCDMA) or S1/X2 (LTE) and O&M are in different subnetworks, they each have their own default gateway. The RBS makes a separate DHCP request for each IP address.

The RBS resolves DNS queries after receiving an IP address from the DHCP server. Thus, option 72 can be exchanged to the DNS query described in Section 2.6.1 on page 17.

During autointegration, the RBS fetches the IP addresses for the permanent IPSec tunnels from the DHCP server once only and continues to statically use the given IP addresses. That is, the RBS does not act as a DHCP client. The result of this is that re-provisioning new IP addresses through DHCP requires an RBS factory reset.

For configuration variant *No IPSec, Traffic separation*, IP address allocation requires one DHCP instance per VLAN ID. Also, the IP addresses for O&M and Iub (WCDMA) or S1/X2 (LTE) traffic must belong to different subnetworks.

For configuration variant *No IPSec, No Traffic separation* IP addresses are allocated from one DHCP server.

Note: One physical DHCP server runs multiple DHCP services. Each service issues IP addresses from a specific IP subnet.

2.7 IPSec Negotiation

The RBS uses certificate-based authentication. During autointegration, the RBS first uses both the factory-installed Ericsson vendor credentials, which is a node-unique certificate and the corresponding private key. These are then used for authentication of the RBS by the SEG while establishing the temporary O&M IPSec tunnel. The RBS then performs certificate enrollment using Certificate Management Protocol Version 2 (CMPv2) to acquire a certificate from the operator OSS-RC Certification Authority (CA) server,

through the temporary O&M IPSec tunnel. This certificate is then used for all subsequent IPSec tunnels.

Because the RBS acts as an IKE initiator during the IKEv2 handshake, all requests are proposals to the responder. The IKE responder (SEG) chooses the configuration used in the negotiated IPSec connections.

The proposal amongst other attributes includes a request for an inner IP address. If an inner IP address is changed through the Managed Object Model (MOM), after autointegration, the new address is not used unless the new proposal is accepted by the responder.

The RBS uses the following IKE ID when setting up the IPSec tunnel:

- For the temporary O&M IPSec tunnel established with the vendor credentials, certificate subject (DN) in format `C=<country>, O=Ericsson, CN=<RBS serial number>.ericsson.com` in the subject string is used as IKE ID.
- For the permanent O&M IPSec tunnel established with the operator credentials, subject CN is used as IKE ID:`<OSS-RC name>:<RBS6402-NE-name>`
- For the permanent RAN (WCDMA) or S1/X2 (LTE) IPSec tunnel, `subjectAltName` matches the Common Name (CN) of the subject. The Subject Alternative Name is used as IKE ID: `<RBS serial number>.<customer>.com`

The SEG assigns one inner IP address to the RBS for each IPSec tunnel. At the end of the autointegration sequence, the RBS reports to the OSS-RC which IP addresses it has acquired for O&M and Iub (WCDMA) or S1/X2 (LTE) traffic by sending the SNMP trap, an alarm.

At the initial IKEv2 handshake, the Pico radio Node uses any IP range traffic selector as the remote subnet, when establishing the permanent O&M and Traffic IPSec connections. SEGs must be provisioned to narrow down the selector as follows:

- **O&M SEG:** Remote subnet(s) defined for all destination IP addresses that the RBS makes a connection with, for example DNS or OSS-RC. For WCDMA, there can be single or several subnets.
- **Traffic SEG:** For WCDMA, remote subnets should be defined, except for IP addresses of the controller nodes (RNC). Remote subnet should be defined, not including any IP addresses of nodes that reside in the public network, for example NTP server, and to which the RBS attempts to connect.

For WCDMA, when multiple subnets are defined, the traffic SEG can provide connections to more than one RNC without knowing which RNC will be used for the RBS 6402. A traffic selector that uses multiple subnets also enables the RNC to be provisioned with IP-addresses for more than one subnet.

Refer to *RFC 5996* for more information about the IKEv2 protocol.

2.7.1 Default Settings for Cryptographic Algorithm Negotiation

Table 4 describes the default settings for the IKEv2 and Encapsulating Security Payload (ESP) algorithm suite and their respective priority in the cryptographic algorithm negotiation. The settings can not be changed.

Table 4 Default settings for the IKEv2 and ESP Algorithm Suite

Priority in Negotiation	Cipher	Integrity Protection Algorithm	Diffie-Hellman Group
1	AES128 CBC	SHA1	Group 14 - 2048-bit MODP
2	AES128 CBC	SHA1	Group 2 - 1024-bit MODP

2.8 Ethernet Capabilities

The Pico Radio Node supports a single Gigabit Ethernet (GE) physical interface for transport or backhaul purposes. This section discusses the following Ethernet capabilities:

- Automatic negotiation
- Flow control

Ethernet automatic negotiation allows the devices at both ends of an Ethernet link segment to do the following:

- Advertise abilities.
- Acknowledge receipt and understanding of a common operating mode that both devices share.
- Reject the use of operating modes that are not shared by both devices.

Note: Automatic negotiation (AN) as defined by IEEE802.3 for 1000Base-X is not supported by the RBS 6402. To establish a 1000Base-X link with RBS 6402 the link partner must implement AN as defined by the Cisco SGMII (Serial Gigabit Media Independent Interface) specification, or use forced mode.

The operating mode specifies the link speed, the duplex setting and the master or slave state. Ethernet automatic negotiation of the operating mode is enabled by default and cannot be disabled. Half duplex mode is not supported and is excluded during ethernet automatic negotiation. Refer to Section 4.10 on page 41 for information about how to find the operating mode of a node.

There are two standard Ethernet flow control mechanisms: pause and Priority-Flow Control (PFC). They are intended to regulate traffic flows to avoid dropping frames during periods of congestion on a point-to-point full duplex link. Ethernet flow control mechanisms are not supported. The Pico Radio Node does not generate outgoing pause and PFC frames and it ignores incoming pause and PFC frames.

2.9 TWAMP Light Responder

The Two Way Active Measurement Protocol (TWAMP) specified in *RFC 5357* is a protocol that enables measurements of network delay and lost packets between two nodes in an IP network. The RBS implements a TWAMP light responder, all settings are predefined and are not visible in the MOM.

TWAMP sessions are identified by the following information:

- The local and remote IP addresses
- The local and remote ports
- The Differentiated Services Code Point (DSCP) value

The following are default settings that cannot be changed:

- The TWAMP light responder is enabled by default.
- The TWAMP communication is sent through UDP port 863.

2.10 Default SCTP Settings

This section describes the default settings for the Stream Control Transmission Protocol (SCTP). For WCDMA, the settings cannot be changed. For LTE, see the *SctpProfile* MO in the *Managed Object Model (MOM) RBS*for more information about SCTP settings.

For WCDMA, the following SCTP port numbers are used for the Node B Application Protocol (NBAP):

- 5113 (NBAP Common)
- 5114 (NBAP Dedicated)

For LTE, the following SCTP endpoint port numbers are used for S1 and X2:

- 36412 for S1
- 36422 for X2

Table 5 describes the default SCTP settings for WCDMA.

Table 5 Default SCTP Settings

Setting	Value
Association.Max.Retrans, as defined in *RFC 4960*, section 8.1	12 attempts
The SCTP heartbeat interval (HB.interval), as defined in *RFC 4960*, section 8.3	1 second
HB.MaxBurst, as defined in *RFC 4960*, section 5.4	1 heartbeat
The time interval for probing heartbeat path	200 milliseconds
RTO.Initial, as defined in *RFC 4960*, section 6.3.1	200 milliseconds
RTO.Max, as defined in *RFC 4960*, section 6.3.1	400 milliseconds
RTO.Min, as defined in *RFC 4960*, section 6.3.1	100 milliseconds
The maximum number of consecutive retransmissions on an IP path (defined by local IP address and remote IP address)	12 retransmissions
The time delay between receiving the DATA chunk to sending the SACK chunk	10 milliseconds
The value of the initial advertised receiver window credit (a_rwnd sent in the INIT message)	16384 bytes
The maximum user data size (1)	556 bytes

(1) This setting prevents situations where fragmentation of IP packets or SCTP packets will occur. The user data size plus the IP header will not exceed the Maximum Transmission Unit (MTU) size. 556 bytes is also recommended for the peer to ensure that no fragments arrive at the RBS if the network MTU is not known. If the MTU size used in the network is known and it can be ensured that fragmentation is avoided, a higher value (up to 1480 bytes without IPSec protection and 1416 bytes with IPSec protection) can be used.

Note: Typically, the control plane application monitors S1 (LTE) or Iub (WCDMA) link based on the SCTP association state and considers the link being down if all related SCTP associations towards the peer node are closed, in which case Pico will attempt to recover via triggering a reset.

Note that the attributes `RTO.init`, `RTO.min`, `RTO.max`, `RTO.alpha`, `RTO.beta`, `assocMaxRtx` and `pathMaxRtx` contributes to the decision to close down a single SCTP association, and consequently, the round-trip-time and link break duration Pico is able to withstand. The current RTO is computed according to RFC-4960, Ch 6.3.1.

2.11 IP QoS and Traffic Shaping

This section describes the default settings that are related to IP Quality of Service (QoS) and IP traffic shaping.

IP traffic shaping can be used to improve the characteristics of the transport network. Egress shaping in RBS is a way to avoid IP packets to be lost higher up in the network in cases where the transport network only provides limited QoS handling. Egress shaping can also be used to match the egress traffic with link capacity in the transport network.

2.11.1 Traffic Shaping Profiles

The RBS has three predefined setting profiles for traffic shaping. Each profile contains preset values for the following settings:

- Number of queues
- Mapping between Differentiated Services Code Point (DSCP) values and queues
- Scheduling algorithm for each queue, one of the following:
  - Strict Priority (SP)
  - Deficit Weighted Round Robin (DWRR)
- Buffer weights for DWRR queues
- Queue length
- Drop profile

The attribute *`trafficShapingProfile`* is common for both LTE, WCDMA and Wi-Fi.

Detailed information about the traffic shaping profiles is available in the enumeration description of the *trafficShapingProfile* attribute in the *Managed Object Model (MOM) RBS*.

2.11.2 Main Attributes for Traffic Shaping

In addition to the traffic shaping profiles, the `egressCir` attribute sets the Committed Information Rate (CIR) of the traffic scheduler. The `egressCbs` attribute sets the Committed Burst Size (CBS). Also, the `rbsUlPolicingFactor` attribute specifies the ratio of the uplink data rate for the RBS data and control plane traffic to the uplink data rate of the Wi-Fi traffic.

Note: The attribute `rbsUlPolicingFactor` is not supported by RBS 6402 in current release.

There exist three predefined Traffic Shaping Profiles. These profiles are common for both LTE, WCDMA and Wi-Fi and are configurable in the ICF.

2.11.3 Starvation of LTE Traffic due to Wi-Fi Traffic

This section is valid for LTE only.

There is a risk of Wi-Fi traffic causing starvation of 3GPP traffic either in the downlink or uplink direction. Generally, the overall QoS design at network level should always be considered. This includes, for instance, proper DSCP and P-bit marking, packet classification and traffic shaping configuration at any QoS aware node in the network. As for AP 6402 specific configurations to mitigate such issues, consider the following:

- In case of downlink starvation, it is recommended to use bandwidth contracts for AP 6402. This AC feature provides an upper limit to downstream bandwidth utilized by clients in a role. The role can be defined as per AP group or per user. Furthermore, bandwidth contracts can be used to limit traffic for individual applications (or categories of applications).
- In case of uplink starvation, make sure proper Wi-Fi DSCP and P-bit configuration is in place and does not conflict with 3GPP. The used QoS parameters in RBS 6402 should be taken into consideration due to common uplink traffic shaping.

Please refer to the AOS User Guide for configuration details.

2.11.4 Default DSCP Values

Table 6 specifies services and the respective default DSCP values.

Table 6 Default DSCP Values of Services

Service	DSCP value
Synchronization	54
SCTP	40
SNMP(1)	32 (Cannot be changed)
Other O&M services	16 (Cannot be changed)

(1) Simple Network Management Protocol

If Wi-Fi is enabled, user must configure proper DSCP and Pbit values at integration time via AC. By default, AC sets DSCP 0 and Pbit 0 for all traffic. Wi-Fi AP supports configurable marking of DSCP for control plane, OAM and user data.

It is recommended to use the following values:

- DSCP 40 for Control plane
- DSCP 16 for OAM
- DSCP 14 for User data

As for P-bit marking, it is recommended to follow the DSCP to Pbit mapping in Table 7.

The overall QoS design for LTE and Wi-Fi should always be considered when deviating from recommended values.

Refer to *Network Synchronization* for information about how to change the DSCP value for synchronization.

Refer to Section 4.9 on page 40 for information about how to change the DSCP value for SCTP.

For WCDMA, the RNC assigns Transport Network Layer (TNL) QoS for the user plane during radio link setup.

2.11.5 Default DCSP to VLAN Priority Bit Mapping

Table 7 specifies the IP DSCP to VLAN priority bit mapping.

Table 7 IP DSCP to VLAN Priority Bit Mapping

VLAN Priority Bit	DSCP Value
7	54, 51
6	48, 40, 32
5	46, 38, 36, 34, 24

VLAN Priority Bit	DSCP Value
4	28, 26, 16, 8
3	22, 20, 18
2	14, 12, 10
1	All other DSCP values

3 Managed Object Model (MOM)

This section describes the management model defined for the managed area.

Note: Setting an unsupported value may affect traffic. A few MOs, parameters, counters, and value ranges may be visible in the *Managed Object Model (MOM) RBS* even though they are not yet supported. This is due to consideration of future system aspects.

For LTE, refer to *Parameter and Counter Limitations* for a list of limitations to the MOM included in this library.

Refer to the *Managed Object Model (MOM) User Guide* for information about the managed object model concept.

3.1 Managed Object Overview

The IP Transport area represents a subset of the MOM. The MOs contained in the area are shown in Figure 8 (WCDMA) and Figure 9 (LTE). The MOs `ManagedElement` and `Transport` belong to the managed area described in *Managed Element*.

All MOs, except the `VlanPort` MO, are created by the RBS during autointegration (AI), as specified in the ICF. The applicable `VlanPort` MOs must also be specified in the ICF. However, they can be created and deleted after autointegration to account for transport network changes.

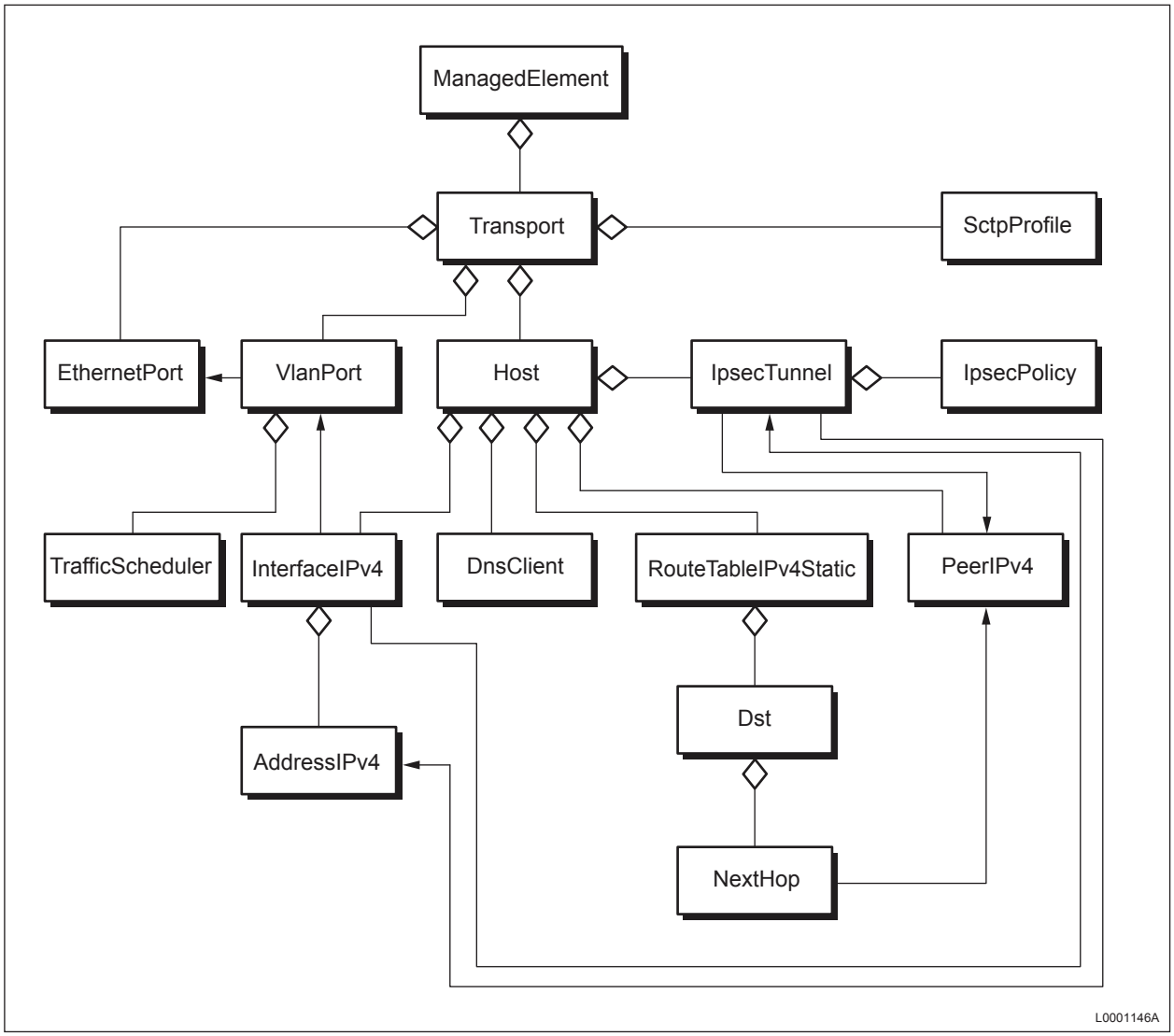

Figure 8 IP Transport MO Overview, WCDMA

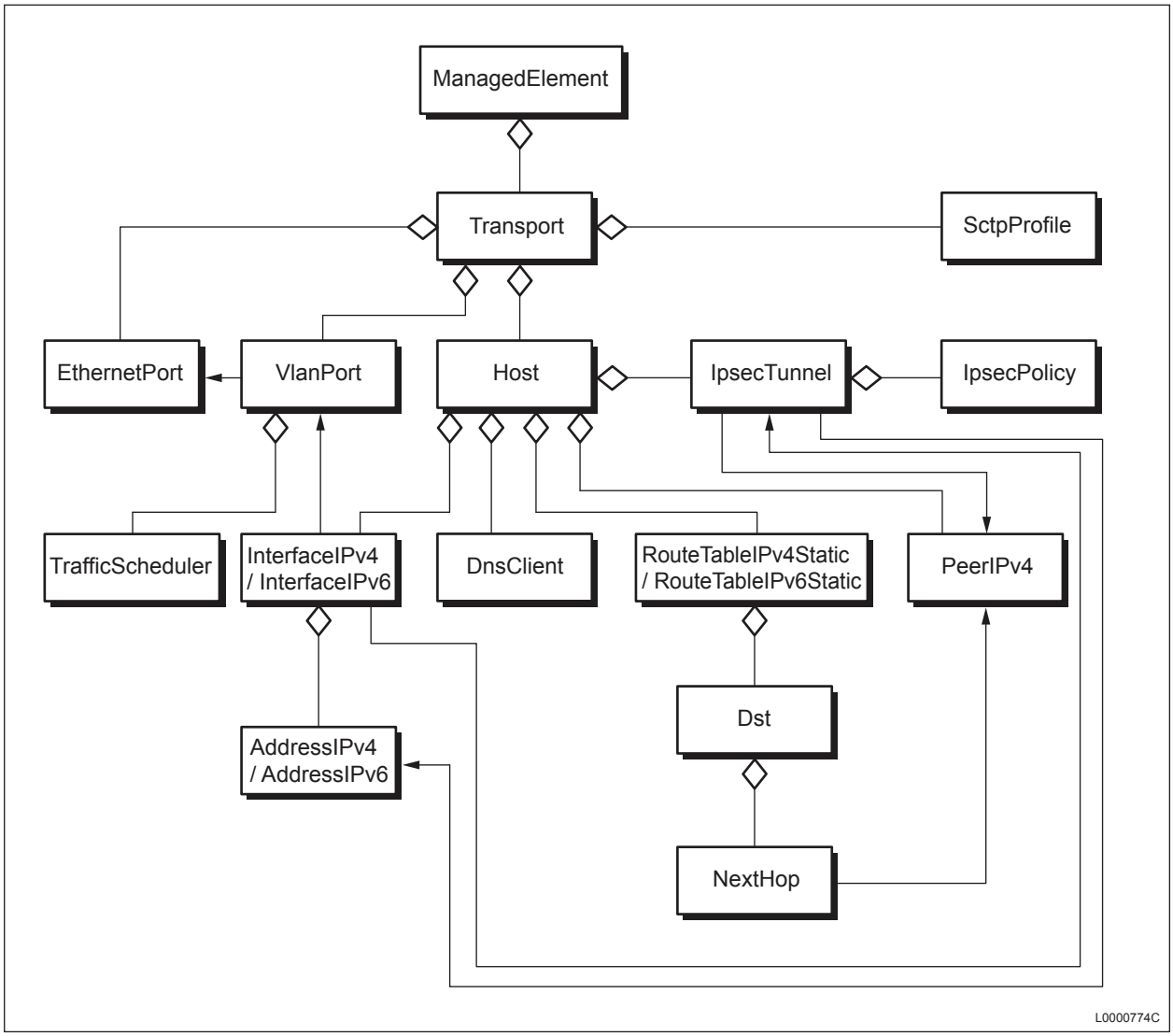

Figure 9 IP Transport MO Overview, LTE

Table 8 describes the MO classes in the IP Transport managed area. Refer to the *Managed Object Model (MOM) RBS* for more information.

Note: LTE only - for boxes with two MO classes, for example InterfaceIPv4/ InterfaceIPv6, two parallel classes exist. That is, one for IPv4, and another for IPv6.

Table 8 IP Transport MO Classes

MO Class	Description
AddressIPv4	IPv4 assigned address including information about the subnet it is residing on

MO Class	Description
AddressIPv6	LTE only. IPv6 assigned address including information about the subnet it is residing on
DnsClient	Represents the DNS client and specifies the address to the DNS server
Dst	Represents a destination network of a routing table
EthernetPort	Represents a physical port that provides an Ethernet-like MAC service access point
Host	Represents an IP domain for traffic termination
InterfaceIPv4	IPv4-addressed termination point: interface on an IPv4 Routing Function
InterfaceIPv6	LTE only. IPv6-addressed termination point: interface on an IPv6 Routing Function
NextHop	Represents next hop information, which describes how to reach a destination network
PeerIPv4	IPv4 peer information
RouteTableIPv4Static	Table of manually defined IPv4 static routes represented by MOs Dst and its children NextHop
RouteTableIPv6Static	LTE only. Table of manually defined IPv6 static routes represented by MOs Dst and its children NextHop
TrafficScheduler	Provides functions for traffic scheduling and traffic shaping
Transport	Contains all MOs that represent the transport functions of the managed element
VlanPort	Represents a single aware port of a VLAN

3.2 MOs for Configuration Variants

This section describes a selection of system created MOs, that is, MOs created by the RBS during autointegration.

3.2.1 MOs for Configuration Variant "Two Permanent IPSec Tunnels, Untagged or Common VLAN"

This section describes a selection of system created MOs for the IP transport configuration variant in Section 2.3.1 on page 11.

Table 9 Selection of System Created MO RDNs, Configuration Variant Two Permanent IPSec Tunnels, Untagged or Common VLAN

MO Description	RDN
Inner IP host, O&M traffic	`ManagedElement=1, Transport=1, Host=1`
Inner IP host, Iub (WCDMA) or S1/X2 (LTE) traffic	`ManagedElement=1, Transport=1, Host=2`
RBS outer IP host	`ManagedElement=1, Transport=1, Host=3`
RBS outer IP host, IPv4 address	`ManagedElement=1, Transport=1, Host=3, InterfaceIPv4=3, AddressIPv4=3`
O&M SEG, peer IPv4 address	`ManagedElement=1, Transport=1, Host=3, PeerIPv4=1`
Iub (WCDMA) or S1/X2 (LTE) SEG, peer IPv4 address	`ManagedElement=1, Transport=1, Host=3, PeerIPv4=2`
Default gateway, peer IPv4 address	`ManagedElement=1, Transport=1, Host=3, PeerIPv4=3`
Common VLAN interface for O&M and Iub (WCDMA) or S1/X2 (LTE) traffic (optional)	`ManagedElement=1, Transport=1, VlanPort=1`
Wi-Fi VLAN ID (optional)	`ManagedElement=1, Transport=1, VlanPort=3`

3.2.2 MOs for Configuration Variant "No IPSec, Traffic Separation"

This section describes a selection of system created MOs for the IP transport configuration variant in Section 2.3.2 on page 13.

Table 10 Selection of System Created MO RDNs, Configuration Variant No IPSec, Traffic Separation

MO Description	RDN
IP host, O&M traffic	`ManagedElement=1, Transport=1, Host=1`
IP host, Iub (WCDMA) or S1/X2 (LTE) traffic	`ManagedElement=1, Transport=1, Host=2`
O&M default gateway, peer IPv4 address	`ManagedElement=1, Transport=1, Host=1,PeerIPv4=1`
DNS client for O&M traffic	`ManagedElement=1, Transport=1, Host=1,DNSClient=1`

MO Description	RDN
VLAN interface, O&M traffic	`ManagedElement=1, Transport=1, VlanPort=1`
VLAN interface, Iub (WCDMA) or S1/X2 (LTE) traffic	`ManagedElement=1, Transport=1, VlanPort=2`
Wi-Fi VLAN ID (optional)	`ManagedElement=1, Transport=1, VlanPort=3`

3.2.3 MOs for Configuration Variant "No IPSec, No Traffic Separation"

This section describes a selection of system created MOs for the IP transport configuration variant in Section 2.3.3 on page 13.

Table 11 Selection of System Created MO RDNs, Configuration Variant No IPSec, Traffic Separation

MO Description	RDN
IP host, O&M traffic	`ManagedElement=1, Transport=1, Host=1`
IP host, Iub (WCDMA) or S1/X2 (LTE) traffic	`ManagedElement=1, Transport=1, Host=2`
Default gateway, peer IPv4 address	`ManagedElement=1, Transport=1, Host=1,PeerIPv4=1`
DNS client for O&M traffic	`ManagedElement=1, Transport=1, Host=1,DNSClient=1`
Common VLAN interface for O&M and Iub (WCDMA) or S1/X2 (LTE) traffic (optional)	`ManagedElement=1, Transport=1, VlanPort=1`
Wi-Fi VLAN ID (optional)	`ManagedElement=1, Transport=1, VlanPort=3`

4 Configuration Management

This section describes configuration management aspects related to IP Transport. It describes the changes and additions that can be made to the basic configuration that is set up during autointegration.

Attention!

Risk of data loss or data corruption.

Attention!

Risk of system malfunction or traffic disturbance.

Note: Setting an unsupported value can affect traffic. A few MOs, parameters, counters, and value ranges may be visible in the MOM even though they are not yet supported. This is due to consideration of future system aspects.

For LTE, refer to *Parameter and Counter Limitations* for a list of limitations to the MOM included in this library.

Note: Parameters with indication "Takes effect: At node restart" in the *Managed Object Model (MOM) RBS* require a node restart:

To restart the node, see *Restart Node*.

4.1 Changing the IP Address for Iub (WCDMA) or S1/X2 (LTE) Traffic

Note:

- The RBS will use DHCP again in case of factory restart. The following external nodes might be impacted due to the change: RNC, MME, SEG, DHCP, default GW.
- With IPSec, user should also choose whether the defined inner IP-address is static without IKEv2 CP or proposal via IKEv2 CP towards the SEG. See Section 2.4 on page 13.

Steps

Do the following to change the IP address for Iub (WCDMA) or S1/X2 (LTE) traffic:

1. Set the *address* attribute of MO `ManagedElement=1, Transport=1, Host=2, InterfaceIPv4=2, AddressIPv4=2`
2. Restart the node.

   LTE only - for IPv6, the MOs `InterfaceIPv6=2` and `AddressIPv6=2` are used in step 1 on page 36.

   Refer to *Restart Node* for information on how to restart the node.

4.2 Changing the Node O&M IP Address

Note:
- The RBS will use DHCP again in case of factory restart. The following external nodes might be impacted due to the change: OSS-RC, SEG, DHCP, default GW.
- With IPSec, user should also choose whether the defined inner IP-address is static without IKEv2 CP or proposal via IKEv2 CP towards the SEG. See Section 2.4 on page 13.

Steps

Do the following to change the node O&M IP address:

1. Set the *address* attribute of MO `ManagedElement=1, Transport=1, Host=1, InterfaceIPv4=1, AddressIPv4=1`
2. Restart the node.

   LTE only - for IPv6, the MOs `InterfaceIPv6=1` and `AddressIPv6=1` are used in step 1 on page 36.

   Refer to *Restart Node* for information on how to restart the node.

   Note: Changing the IP address causes an interruption of the communication between the node and the network management tool. If the assigned IP address is incorrect, then the IP connection is lost.

4.3 Changing the Outer IP Addresses of an IPSec Tunnel

This section describes how to change the local and remote outer IP addresses of an IPSec tunnel.

4.3.1 Changing the Outer RBS IP Address of an IPSec Tunnel

Note: The RBS will use DHCP again in case of factory restart.

Do the following to change the outer RBS IP address:

Steps

1. Navigate to MO `ManagedElement=1, Tranport=1, Host=3, InterfaceIPv4=3, AddressIPv4=3`.
2. Set the *`address`* attribute.
3. Restart the node.

   Refer to *Restart Node* for information on how to restart the node.

4.3.2 Changing the SEG IP Address of an IPSec Tunnel

Note: In case of factory restart, the RBS will use the SEG addresses in ICF that is retrieved from AIWS.

Do the following to change a SEG IP address:

Steps

1. Navigate to the appropriate child *`PeerIPv4`* MO of the outer IP host. (Refer to Section 3.2.1 on page 32.)
2. Set the *`address`* attribute.
3. Restart the node.

   Refer to *Restart Node* for information on how to restart the node.

4.4 Changing Default Gateway Address

Note: The RBS will use DHCP again in case of factory restart.

Steps

Do the following to change the default gateway address:

1. Navigate to the child `PeerIPv4` MO of the appropriate `Host` MO.
2. Set the *`address`* attribute.

3. Restart the node.

   Note: The above is valid only in the case when O&M traffic and Iub (WCDMA) or S1/X2 (LTE) traffic IP addresses reside in different subnets.

   Refer to *Restart Node* for information on how to restart the node.

4.5 Changing the DNS Server Addresses

Note: In case of factory restart, the RBS will use DHCP options or IKEv2 CP to retrieve DNS server addresses.

To change the DNS server addresses set the *serverAddress* attribute of MO `ManagedElement=1, Transport=1, Host=1, DnsClient=1`. The `serverAddress` attribute can store three DNS server addresses.

4.6 Configuring VLAN IDs

This section describes configuration management of VLAN IDs.

4.6.1 Changing VLAN ID for Iub (WCDMA) or S1/X2 (LTE) Traffic

Note:
- In case of factory restart, the RBS will use VLAN ID in ICF that is retrieved from AIWS.
- The following external nodes might be impacted due to the change: DHCP, AIWS, NTP, PTP/IP, default GW.

Steps

To change an existing VLAN ID, do the following:

1. Navigate to MO `ManagedElement=1, Transport=1, Host=2, InterfaceIPv4=2`
2. Find out what *VlanPort* MO is referred to in attribute *encapsulation*.
3. Navigate to that `VlanPort` MO and set the *vlanId* attribute.
4. Restart the node.

   LTE only - for IPv6, the MO `InterfaceIPv6=2` is used in step 1 on page 38.

   Refer to *Restart Node* for information on how to restart the node.

4.6.2 Adding VLAN ID for Iub (WCDMA) or S1/X2 (LTE) Traffic

Steps

To add a VLAN ID, do the following:

1. Create a *VlanPort* MO according to the information in Section 3.2 on page 32.
2. Set the *encapsulation* attribute of the new VlanPort MO to `ManagedElement=1, Transport=1, EthernetPort=1`
3. Restart the node.

   Refer to *Restart Node* for information on how to restart the node.

4.6.3 Changing VLAN ID for O&M Traffic

Note:
- In case of factory restart, the RBS will perform VLAN-scan to search for the DHCP server.
- The following external nodes might be impacted due to the change: DHCP, NTP ToD, default GW.

Steps

To change an existing VLAN ID, do the following :

1. Navigate to MO `ManagedElement=1, Transport=1, VlanPort=1`
2. Set the *vlanId* attribute.
3. Restart the node.

   Refer to *Restart Node* for information on how to restart the node.

4.6.4 Adding VLAN ID for O&M Traffic

Steps

To add a VLAN ID, do the following:

1. Create MO `ManagedElement=1, Transport=1, VlanPort=1.`
2. Set the *encapsulation* attribute of the new VlanPort MO to `ManagedElement=1,Transport=1,EthernetPort=1`

3. Restart the node.

   Refer to *Restart Node* for information on how to restart the node.

4.7 Configuring IP Traffic Shaping

The following attributes of MO class *TrafficScheduler* relate to IP traffic shaping:

- *egressCbs*
- *egressCir*
- *rbsULPolicingFactor*
- *trafficShapingProfile*

  Restart the node after setting the trafficShapingProfile attribute. Refer to *Restart Node* for information on how to restart the node.

4.8 Changing the Maximum Transmission Unit of the Ethernet Interface

Steps

Do the following to change the MTU of the Ethernet interface:

1. Set attribute *mtu* of MO ManagedElement=1, Transport=1, EthernetPort=1.
2. Restart the node.

   Refer to *Restart Node* for information on how to restart the node.

4.9 Configuring the DSCP Value for SCTP

Steps

Do the following to set the DSCP value for SCTP:

1. Set attribute *dscp* of MO ManagedElement=1, Transport=1, SctpProfile=1.
2. Restart the node.

Refer to *Restart Node* for information on how to restart the node.

4.10 Reading the Ethernet Operating Mode

Refer to attribute *operOperatingMode* of MO `ManagedElement=1, Transport=1, EthernetPort=1` for information about the operational operating mode, which specifies the link speed, the duplex setting and the master or slave state.

4.11 Introducing or Removing IPSec

To introduce IPSec to an already commissioned node the RBS must first be reset to factory default settings and then configured with an appropriate ICF. The same procedure is required to remove IPSec from an already commissioned node.

For instructions on how to reset an RBS to factory settings, see *Recovering a Node on Site*.

For ICF templates, see Section 2.5 on page 16.

5 Fault Management

This section describes Fault Management (FM) aspects related to IP Transport.

Refer to *Alarm and Event List* for information about alarms and FM events.

6 Performance Management

This section describes Performance Management (PM) aspects related to IP Transport.

For WCDMA, refer to *WCDMA RAN Counter List* and for LTE to *Counter List* for information about PM counters.

Note: Setting an unsupported value may affect traffic. A few MOs, parameters, counters, and value ranges may be visible in the MOM even though they are not yet supported due to system design considering future aspects.

For LTE, refer to *Parameter and Counter Limitations* for a list of limitations to the MOM included in this library.