

Edition

06/2023

Configuration Manual

# SIMATIC NET

**Rugged Multi Service Platforms**

RUGGEDCOM ROX II v2.16 Web Interface

For RX5000, MX5000, MX5000RE

<https://www.siemens.com/ruggedcom>

## SIMATIC NET

### Rugged Multi Service Platforms RUGGEDCOM ROX II v2.16 Web Interface

Configuration Manual

For RX5000, MX5000, MX5000RE

Preface	
Introduction	1
Using RUGGEDCOM ROX II	2
Getting Started	3
Device Management	4
System Administration	5
Security	6
IP Address Assignment	7
Layer 2	8
Layer 3	9
Serial Server	10
Tunneling and VPNs	11
Unicast and Multicast Routing	12
Network Redundancy	13
Network Discovery and Management	14
Traffic Control and Classification	15
Time Services	16

Continued on next page



Applications

**17**

Troubleshooting

**18**

Reference

**19**

## SIMATIC NET

### Rugged Multi Service Platforms RUGGEDCOM ROX II v2.16 Web Interface

Configuration Manual





For RX5000, MX5000, MX5000RE



## Legal information

### Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 <b>DANGER</b>
indicates that death or severe personal injury will result if proper precautions are not taken.
 <b>WARNING</b>
indicates that death or severe personal injury may result if proper precautions are not taken.
 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
 <b>NOTICE</b>
indicates that property damage can result if proper precautions are not taken.


If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

### Qualified personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

### Proper use of Siemens products

Note the following:

 <b>WARNING</b>
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

### Trademarks

All names identified by ® are registered trademarks of Siemens Canada Ltd.. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

### Disclaimer of liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.



# Table of contents

<b>Preface</b> .....	<b>xxxvii</b>
Security information .....	xxxvii
Firmware/software support model .....	xxxviii
SIMATIC NET glossary .....	xxxviii
System Requirements .....	xxxviii
Accessing documentation .....	xxxix
License conditions .....	xxxix
Registered trademarks .....	xxxix
Warranty .....	xxxix
Training .....	xl
Customer support .....	xl
Contacting Siemens .....	xl
<b>1 Introduction</b> .....	<b>1</b>
1.1 Features and Benefits .....	1
1.2 Feature Keys .....	6
1.3 Security Recommendations .....	8
1.4 Available Services by Port .....	12
1.5 User Permissions .....	13
1.6 Removable Memory .....	16
1.7 Logged Events .....	16
1.7.1 Structure of a Syslog Event .....	16
1.7.2 Syslog Event Types .....	17
1.7.3 Logged Security Events .....	17
<b>2 Using RUGGEDCOM ROX II</b> .....	<b>23</b>
2.1 Default User Names and Passwords .....	23
2.2 Logging In .....	23
2.3 Logging Out .....	24
2.4 Navigating the Interface .....	25
2.4.1 Screen Layout .....	25
2.4.2 Tabs .....	26
2.4.3 Locator Tooltips .....	26
2.4.4 UI Controls .....	27
2.5 Configuring the Device .....	29
2.5.1 Using Tables .....	29
2.5.1.1 Selecting Entries in a Table .....	30
2.5.1.2 Adding and Deleting Table Entries .....	31
2.5.1.3 Editing Table Cells .....	32
2.5.1.4 Changing the Priority of Table Entries .....	32



2.5.1.5	Scrolling Between Table Pages .....	33
2.5.2	Using the Info Button .....	33
2.5.3	Exporting Data to Excel .....	34
2.6	Managing Changes .....	34
2.6.1	Viewing Configuration Changes .....	34
2.6.2	Validating Configuration Changes .....	35
2.6.3	Committing a Change .....	37
2.6.4	Discarding a Change .....	37
2.7	Using Network Utilities .....	39
2.7.1	Pinging an IPv4 Address or Host .....	39
2.7.2	Pinging an IPv6 Address or Host .....	40
2.7.3	Pinging MPLS Endpoints .....	40
2.7.4	Pinging VRF Endpoints .....	41
2.7.5	Tracing a Route to an IPv4 Host .....	41
2.7.6	Tracing a Route to an IPv6 Host .....	42
2.7.7	Tracing a Route to an MPLS Endpoint .....	42
2.7.8	Tracing a Route to a VRF Endpoint .....	42
2.7.9	Capturing Packets from a Network Interface .....	43
2.7.10	Capturing Packets from a VRF Network Interface .....	44
2.8	Using the Command Line Interface .....	45
2.9	Accessing Different Modes .....	45
2.9.1	Enabling/Disabling SSH Access in Maintenance Mode .....	45
2.9.2	Managing Maintenance Mode Authorization .....	46
2.9.2.1	Temporarily Enabling Maintenance Mode Authorization .....	47
2.9.2.2	Permanently Enabling Maintenance Mode Authorization .....	47
2.9.2.3	Disabling Maintenance Mode Authorization .....	48
<b>3</b>	<b>Getting Started .....</b>	<b>49</b>
3.1	Connecting to RUGGEDCOM ROX II .....	49
3.1.1	Default IP Address .....	49
3.1.2	Connecting Directly via a Port .....	49
3.1.3	Connecting Remotely via a Web Browser .....	50
3.2	Configuring a Basic Network .....	51
3.2.1	Configuring a Basic IPv4 Network .....	51
3.2.2	Configuring a Basic IPv6 Network .....	52
<b>4</b>	<b>Device Management .....</b>	<b>53</b>
4.1	Displaying Device and Software Information .....	53
4.2	Viewing Chassis Information and Status .....	54
4.2.1	Viewing the Slot Hardware .....	54
4.2.2	Viewing Module Information .....	54
4.2.3	Viewing Flash Card Storage Utilization .....	55
4.2.4	Viewing CPU/RAM Utilization .....	55
4.2.5	Viewing the Slot Status .....	56
4.2.6	Viewing the Slot Sensor Status .....	56
4.2.7	Viewing the Power Controller Status .....	57

4.3	Shutting Down the Device .....	58
4.4	Rebooting the Device .....	58
4.5	Restoring Factory Defaults .....	58
4.6	Decommissioning the Device .....	59
4.7	Managing Feature Keys .....	60
4.7.1	Installing Feature Keys .....	60
4.8	Managing Files .....	61
4.8.1	Installing Files .....	62
4.8.2	Backing Up Files .....	63
4.9	Managing Logs .....	64
4.9.1	Viewing Logs .....	65
4.9.2	Deleting Logs .....	66
4.9.3	Configuring Secure Remote Syslog .....	66
4.9.3.1	Enabling/Disabling Secure Remote Syslog .....	66
4.9.3.2	Viewing a List of Permitted Peers .....	67
4.9.3.3	Adding a Permitted Peer .....	67
4.9.3.4	Deleting a Permitted Peer .....	67
4.9.3.5	Configuring a Source IP Address for Remote Syslog Messages .....	68
4.9.4	Managing Diagnostic Logs .....	68
4.9.4.1	Enabling/Disabling the Developer's Log .....	68
4.9.4.2	Enabling/Disabling the SNMP Log .....	69
4.9.4.3	Enabling/Disabling the NETCONF Summary Log .....	70
4.9.4.4	Enabling/Disabling the NETCONF Trace Log .....	70
4.9.4.5	Enabling/Disabling the XPATH Trace Log .....	71
4.9.4.6	Enabling/Disabling the WebUI Trace Log .....	72
4.9.4.7	Enabling/Disabling the JSON-PRC Log .....	72
4.9.5	Managing Remote Syslog Servers .....	73
4.9.5.1	Viewing a List of Remote Servers .....	73
4.9.5.2	Adding a Remote Server .....	73
4.9.5.3	Deleting a Remote Server .....	74
4.9.6	Managing Remote Server Selectors .....	74
4.9.6.1	Viewing a List of Remote Server Selectors .....	74
4.9.6.2	Adding a Remote Server Selector .....	74
4.9.6.3	Deleting a Remote Server Selector .....	76
4.10	Managing the Software Configuration .....	76
4.10.1	Backing Up the Software Configuration .....	76
4.10.2	Saving the Configuration .....	77
4.10.3	Loading a Configuration .....	78
4.10.4	Managing Automatic Configuration Loading .....	78
4.10.4.1	Enabling/Disabling Automatic Configuration Loading .....	78
4.10.4.2	Automatically Loading a Configuration File from a Removable Drive .....	79
4.10.4.3	Overriding Factory Settings Using a Removable Drive .....	80
4.10.4.4	Deleting an Automatic Configuration File .....	80
4.11	Managing Upgrade Servers .....	80
4.11.1	Understanding Upgrade Servers .....	81

4.11.2	Configuring the Upgrade Server .....	81
4.12	Managing Software Versions .....	82
4.12.1	Understanding Upgrades/Downgrades .....	83
4.12.2	Upgrading/Downgrading Software .....	83
4.12.2.1	Determining the Current Software Partition and Version .....	84
4.12.2.2	Obtaining a Software Release .....	84
4.12.2.3	Stopping/Declining a Software Upgrade .....	85
4.12.2.4	Upgrading the Software and Retaining the Configuration .....	85
4.12.2.5	Upgrading the Software and Resetting the Configuration .....	88
4.12.2.6	Downgrading Software .....	90
4.12.2.7	Rolling Back a Software Upgrade .....	92
4.12.2.8	Monitoring Software Upgrades/Downgrades .....	92
4.13	Monitoring Firmware Integrity .....	92
4.13.1	Enabling/Disabling the Boot Time Firmware Integrity .....	93
4.13.2	Checking the Firmware Integrity .....	93
4.13.3	Scheduling a Recurring Firmware Integrity Check .....	94
4.13.4	Viewing the Status of the Firmware Integrity Check .....	94
4.14	Managing the Fan Controller .....	94
4.14.1	Viewing the Fan Controller Status .....	94
4.14.2	Configuring the Activation Temperature .....	96
4.15	Managing Fixed Modules .....	96
4.15.1	Viewing a List of Fixed Module Configurations .....	97
4.16	Managing Line Modules .....	97
4.16.1	Removing a Line Module .....	97
4.16.2	Installing a New Line Module .....	97
4.16.3	Viewing a List of Line Module Configurations .....	98
4.16.4	Configuring a Line Module .....	98
4.17	Managing SFP Transceivers (RUGGEDCOM RX5000 Only) .....	99
4.17.1	SFP Transceiver Support .....	99
4.17.2	Viewing SFP Information .....	100
4.17.3	Enabling/Disabling Smart SFP Mode (RUGGEDCOM RX5000 Only) .....	100
4.18	Managing Routable Ethernet Ports .....	101
4.18.1	Viewing a List of Routable Ethernet Ports .....	101
4.18.2	Configuring a Routable Ethernet Port .....	101
4.18.3	Managing VLANs for Routable Ethernet Ports .....	102
4.18.3.1	Viewing a List of VLANs for Routable Ethernet Ports .....	103
4.18.3.2	Adding a VLAN to a Routable Ethernet Port .....	103
4.18.3.3	Deleting a VLAN for a Routable Ethernet Port .....	104
<b>5</b>	<b>System Administration .....</b>	<b>105</b>
5.1	Configuring the System Name and Location .....	105
5.2	Configuring the Host Name .....	105
5.3	Customizing the Welcome Screen .....	106
5.4	Setting the Maximum Number of Sessions .....	107

---

5.5	Enabling and Configuring WWW Interface Sessions .....	107
5.6	Enabling/Disabling Remote Access Through a VRF Interface .....	108
5.7	Managing Alarms .....	110
5.7.1	Pre-Configured Alarms .....	110
5.7.2	Viewing a List of Active Alarms .....	113
5.7.3	Clearing and Acknowledging Alarms .....	113
5.7.3.1	Clearing Alarms .....	114
5.7.3.2	Acknowledging Alarms .....	114
5.7.4	Configuring an Alarm .....	114
5.7.5	List of Alarms .....	115
5.8	Managing Users .....	116
5.8.1	Viewing a List of Users .....	117
5.8.2	Adding a User .....	117
5.8.3	Deleting a User .....	118
5.8.4	Monitoring Users .....	118
5.8.4.1	Logging Out Users from a Session .....	118
5.8.4.2	Sending Messages to Users .....	118
5.9	Managing Passwords and Passphrases .....	118
5.9.1	Configuring Password/Passphrase Complexity Rules .....	119
5.9.2	Setting a User Password/Passphrase .....	120
5.9.3	Setting the Boot Password/Passphrase .....	121
5.9.4	Setting the Maintenance Password/Passphrase .....	122
5.9.5	Resetting Passwords and Passphrases .....	123
5.10	Scheduling Jobs .....	123
5.10.1	Viewing a List of Scheduled Jobs .....	123
5.10.2	Adding a Scheduled Job .....	123
5.10.3	Deleting a Scheduled Job .....	126
<b>6</b>	<b>Security .....</b>	<b>127</b>
6.1	Enabling and Configuring CLI Sessions .....	127
6.2	Enabling/Disabling Brute Force Attack Protection .....	128
6.3	Enabling/Disabling Compact Flash Card Removal Detection .....	130
6.4	Enabling/Disabling SYN Cookies .....	130
6.5	Managing Cipher Suites .....	130
6.5.1	Viewing Active SSH Server Algorithms .....	130
6.5.2	Enabling SSH Server and NETCONF Algorithms .....	131
6.5.3	Enabling TLS Algorithms .....	132
6.5.4	Configuring the Diffie-Hellman Key Exchange Length .....	133
6.6	Managing SFTP Sessions .....	134
6.6.1	Enabling and Configuring SFTP Sessions .....	134
6.6.2	Adding an SFTP Server's Public Key .....	135
6.7	Managing Port Security .....	135
6.7.1	Port Security Concepts .....	136
6.7.1.1	Static MAC Address-Based Authentication .....	136

6.7.1.2	Static MAC Address-Based Authentication in an MRP Ring .....	136
6.7.1.3	IEEE 802.1x Authentication .....	137
6.7.1.4	IEEE 802.1X Authentication with MAC Address-Based Authentication .....	138
6.7.1.5	Assigning VLANs with Tunnel Attributes .....	138
6.7.2	Configuring Port Security .....	139
6.7.3	Viewing the Security Status of Switched Ethernet Ports .....	142
6.8	Managing User Authentication .....	142
6.8.1	Setting the User Authentication Mode .....	142
6.8.2	Managing User Authentication Keys .....	143
6.8.2.1	Determining Which Keys are Associated to a User .....	143
6.8.2.2	Adding a User Authentication Key .....	144
6.8.2.3	Deleting a User Authentication Key .....	145
6.8.2.4	Associating/Disassociating a User Authentication Key .....	145
6.8.3	Managing RADIUS Authentication .....	145
6.8.3.1	Configuring RADIUS Authentication for LOGIN Services .....	147
6.8.3.2	Configuring RADIUS Authentication for PPP Services .....	148
6.8.3.3	Configuring RADIUS Authentication for Switched Ethernet Ports .....	149
6.8.4	Configuring TACACS+ Authentication .....	150
6.9	Managing Certificates and Keys .....	152
6.9.1	Viewing the Local Host SSH/RSA Public Key .....	152
6.9.2	Configuring Session Security .....	152
6.9.3	Managing the Trusted Certificate Store .....	153
6.9.3.1	Configuring the Trusted Certificate Store .....	153
6.9.3.2	Enabling/Disabling the Trusted Certificate Store .....	154
6.9.3.3	List of Root Certificates in the Trusted Certificate Store .....	154
6.9.4	Managing CA Certificates for the Trusted Certificate Store .....	177
6.9.4.1	Viewing a List of CA Certificates Added to the Trusted Certificate Store .....	177
6.9.4.2	Adding a CA Certificate to the Trusted Certificate Store .....	177
6.9.4.3	Deleting a CA Certificate from the Trusted Certificate Store .....	178
6.9.5	Managing CA Certificates and CRLs .....	178
6.9.5.1	Viewing a List of CA Certificates and CRLs .....	178
6.9.5.2	Viewing the Status of a CA Certificate and CRL .....	178
6.9.5.3	Adding a CA Certificate and CRL .....	179
6.9.5.4	Deleting a CA Certificate and CRL .....	180
6.9.6	Managing Private Keys .....	180
6.9.6.1	Viewing a List of Private Keys .....	180
6.9.6.2	Adding a Private Key .....	180
6.9.6.3	Deleting a Private Key .....	181
6.9.7	Managing Public Keys .....	182
6.9.7.1	Viewing a List of Public Keys .....	182
6.9.7.2	Adding a Public Key .....	182
6.9.7.3	Adding an IPSec-Formatted Public Key .....	183
6.9.7.4	Deleting a Public Key .....	183
6.9.8	Managing Certificates .....	184
6.9.8.1	Viewing a List of Certificates .....	184
6.9.8.2	Viewing the Status of a Certificate .....	184
6.9.8.3	Adding a Certificate .....	184
6.9.8.4	Deleting a Certificate .....	185

6.9.9	Managing Known Hosts .....	185
6.9.9.1	Viewing a List of Known Hosts .....	186
6.9.9.2	Adding a Known Host .....	186
6.9.9.3	Deleting a Known Host .....	187
6.9.10	Managing SCEP .....	187
6.9.10.1	Understanding SCEP .....	187
6.9.10.2	Configuring SCEP .....	189
6.9.10.3	Configuring the SCEP Client .....	190
6.9.10.4	Configuring the SCEP Certificate Signing Requests .....	191
6.9.10.5	Retrieving an SCEP CA Certificate .....	192
6.9.10.6	Retrieving an SCEP Certificate .....	193
6.9.10.7	Configuring Automatic Certificate Renewal .....	193
6.9.10.8	Renewing an Expired SCEP Certificate .....	194
6.9.10.9	Renewing an SCEP CA Certificate .....	194
6.10	Managing Firewalls .....	195
6.10.1	Firewall Concepts .....	195
6.10.1.1	Stateless vs. Stateful Firewalls .....	195
6.10.1.2	Linux netfilter .....	196
6.10.1.3	Network Address Translation .....	196
6.10.1.4	Port Forwarding .....	197
6.10.1.5	Protecting Against a SYN Flood Attack .....	197
6.10.1.6	Protecting Against IP Spoofing .....	198
6.10.1.7	Active and Working Firewall Configurations .....	198
6.10.2	Viewing a List of Firewalls .....	198
6.10.3	Adding a Firewall .....	198
6.10.4	Deleting a Firewall .....	200
6.10.5	Working with Multiple Firewall Configurations .....	200
6.10.6	Configuring the Firewall for a VPN .....	200
6.10.7	Configuring the Firewall for a VPN in a DMZ .....	202
6.10.8	Configuring Netfilter .....	202
6.10.9	Managing Zones .....	203
6.10.9.1	Viewing a List of Zones .....	203
6.10.9.2	Adding a Zone .....	203
6.10.9.3	Deleting a Zone .....	204
6.10.10	Managing Interfaces .....	204
6.10.10.1	Viewing a List of Interfaces .....	205
6.10.10.2	Adding an Interface .....	205
6.10.10.3	Associating an Interface with a Zone .....	206
6.10.10.4	Configuring a Broadcast Address .....	207
6.10.10.5	Deleting an Interface .....	207
6.10.11	Managing Hosts .....	207
6.10.11.1	Viewing a List of Hosts .....	208
6.10.11.2	Adding a Host .....	208
6.10.11.3	Deleting a Host .....	209
6.10.12	Managing Policies .....	209
6.10.12.1	Viewing a List of Policies .....	210
6.10.12.2	Adding a Policy .....	210
6.10.12.3	Configuring the Source Zone .....	211
6.10.12.4	Configuring the Destination Zone .....	211

6.10.12.5	Deleting a Policy .....	211
6.10.13	Managing Network Address Translation Settings .....	212
6.10.13.1	Viewing a List of NAT Settings .....	212
6.10.13.2	Adding a NAT Setting .....	212
6.10.13.3	Deleting a NAT Setting .....	213
6.10.14	Managing Masquerade and SNAT Settings .....	213
6.10.14.1	Viewing a List of Masquerade and SNAT Settings .....	213
6.10.14.2	Adding Masquerade or SNAT Settings .....	214
6.10.14.3	Deleting a Masquerade or SNAT Setting .....	215
6.10.15	Managing Rules .....	215
6.10.15.1	Viewing a List of Rules .....	215
6.10.15.2	Adding a Rule .....	215
6.10.15.3	Configuring the Source Zone .....	218
6.10.15.4	Configuring the Destination Zone .....	218
6.10.15.5	Deleting a Rule .....	219
6.10.16	Validating a Firewall Configuration .....	219
6.10.17	Enabling/Disabling a Firewall .....	219
6.11	Restricting Management Access to Specific Interfaces .....	220
<b>7</b>	<b>IP Address Assignment .....</b>	<b>223</b>
7.1	Managing IP Addresses for Routable Interfaces .....	223
7.1.1	Configuring Costing for Routable Interfaces .....	223
7.1.2	Viewing Statistics for Routable Interfaces .....	223
7.1.3	Managing IPv4 Addresses .....	225
7.1.3.1	Viewing a List of IPv4 Addresses .....	225
7.1.3.2	Adding an IPv4 Address .....	225
7.1.3.3	Deleting an IPv4 Address .....	226
7.1.4	Managing IPv6 Addresses .....	226
7.1.4.1	Viewing a List of IPv6 Addresses .....	226
7.1.4.2	Adding an IPv6 Address .....	226
7.1.4.3	Deleting an IPv6 Address .....	227
7.1.5	Configuring IPv6 Neighbor Discovery .....	227
7.1.6	Managing IPv6 Network Prefixes .....	229
7.1.6.1	Adding an IPv6 Network Prefix .....	229
7.1.6.2	Deleting an IPv6 Network Prefix .....	230
7.2	Managing the DHCP Relay Agent .....	230
7.2.1	Configuring the DHCP Relay Agent .....	231
7.2.2	Assigning a DHCP Server Address .....	231
7.2.3	Viewing a List of DHCP Client Ports .....	232
7.2.4	Adding a DHCP Client Port .....	232
7.2.5	Deleting a DHCP Client Port .....	232
7.2.6	Example: Configuring the Device as a Relay Agent .....	232
7.3	Managing the DHCP Server .....	234
7.3.1	Viewing a List of Active Leases .....	234
7.3.2	Configuring the DHCP Server .....	234
7.3.3	Enabling/Disabling the DHCP Server .....	235
7.3.4	Configuring DHCP Server Options .....	236
7.3.5	Managing DHCP Client Configuration Options .....	237

7.3.5.1	Configuring Standard DHCP Client Configuration Options (IPv4)	237
7.3.5.2	Configuring Standard DHCP Client Configuration Options (IPv6)	239
7.3.5.3	Viewing a List of Custom DHCP Client Configuration Options	240
7.3.5.4	Adding a Custom DHCP Client Configuration Option	241
7.3.5.5	Deleting a Custom DHCP Client Configuration Option	241
7.3.6	Managing DHCP Listen Interfaces	242
7.3.6.1	Viewing a List of DHCP Listen Interfaces	242
7.3.6.2	Adding a DHCP Listen Interface	242
7.3.6.3	Deleting a DHCP Listen Interface	243
7.3.7	Managing Shared Networks	243
7.3.7.1	Viewing a List of Shared Networks	243
7.3.7.2	Adding a Shared Network	244
7.3.7.3	Configuring Shared Network Options	244
7.3.7.4	Deleting a Shared Network	245
7.3.8	Managing Subnets	246
7.3.8.1	Viewing a List of Subnets	246
7.3.8.2	Adding a Subnet	246
7.3.8.3	Configuring Subnet Options	247
7.3.8.4	Deleting a Subnet	249
7.3.9	Managing Host Groups	249
7.3.9.1	Viewing a List of Host Groups	249
7.3.9.2	Adding a Host Group	250
7.3.9.3	Configuring Host Group Options	250
7.3.9.4	Deleting a Host Group	252
7.3.10	Managing DHCP Hosts	252
7.3.10.1	Viewing a List of Hosts	252
7.3.10.2	Adding a Host	252
7.3.10.3	Configuring Host Options	253
7.3.10.4	Deleting Hosts	255
7.3.11	Managing Address Pools (IPv4)	255
7.3.11.1	Viewing a List of Address Pools (IPv4)	255
7.3.11.2	Adding an Address Pool (IPv4)	255
7.3.11.3	Deleting an Address Pool (IPv4)	256
7.3.12	Managing Address Pools (IPv6)	257
7.3.12.1	Viewing a List of Address Pools (IPv6)	257
7.3.12.2	Adding an Address Pool (IPv6)	257
7.3.12.3	Deleting an Address Pool (IPv6)	258
7.3.13	Managing IP Ranges (IPv4)	258
7.3.13.1	Viewing a List of IP Ranges (IPv4)	258
7.3.13.2	Adding an IP Range (IPv4)	259
7.3.13.3	Deleting an IP Range (IPv4)	259
7.3.14	Managing IP Ranges (IPv6)	260
7.3.14.1	Viewing a List of IP Ranges (IPv6)	260
7.3.14.2	Adding an IP Range (IPv6)	260
7.3.14.3	Deleting an IP Range (IPv6)	261
7.3.15	Managing IPv6 Prefixes	261
7.3.15.1	Viewing a List of IPv6 Prefixes	262
7.3.15.2	Adding an IPv6 Prefix	262
7.3.15.3	Deleting an IPv6 Prefix	263



7.3.16	Managing Temporary Subnets .....	263
7.3.16.1	Viewing a List of Temporary Subnets .....	263
7.3.16.2	Adding a Temporary Subnet .....	263
7.3.16.3	Deleting a Temporary Subnet .....	264
7.3.17	Managing IPv6 Subnets .....	264
7.3.17.1	Viewing a List of IPv6 Subnets .....	264
7.3.17.2	Adding a IPv6 Subnet .....	265
7.3.17.3	Deleting an IPv6 Subnet .....	265
7.3.18	Managing Option 82 Classes for Address Pools .....	265
7.3.18.1	Viewing a List of Option 82 Classes for Address Pools .....	266
7.3.18.2	Adding an Option 82 Class to an Address Pool .....	266
7.3.18.3	Deleting an Option 82 Class From an Address Pool .....	267
7.3.19	Example: Configuring the Device as a DHCP Server to Support a Relay Agent .....	267
7.4	Managing Static DNS .....	271
7.4.1	Managing Domain Names .....	272
7.4.1.1	Viewing a List of Domain Names .....	272
7.4.1.2	Adding a Domain Name .....	272
7.4.1.3	Deleting a Domain Name .....	272
7.4.2	Managing Domain Name Servers .....	272
7.4.2.1	Viewing a List of Domain Name Servers .....	273
7.4.2.2	Adding a Domain Name Server .....	273
7.4.2.3	Deleting a Domain Name Server .....	273
<b>8</b>	<b>Layer 2 .....</b>	<b>275</b>
8.1	Configuring Link Detection .....	275
8.2	Managing Switched Ethernet Ports .....	276
8.2.1	Viewing a List of Switched Ethernet Ports .....	276
8.2.2	Configuring a Switched Ethernet Port .....	276
8.2.3	Configuring RMON Threshold Alerts .....	281
8.2.4	Viewing Switched Ethernet Port Statistics .....	283
8.2.5	Viewing the Status of a Switched Ethernet Port .....	284
8.2.6	Viewing RMON Port Statistics .....	285
8.2.7	Clearing Switched Ethernet Port Statistics .....	287
8.2.8	Resetting a Switched Ethernet Port .....	287
8.2.9	Testing Switched Ethernet Port Cables .....	288
8.2.9.1	Running a Cable Diagnostic Test .....	288
8.2.9.2	Viewing Cable Diagnostic Statistics .....	289
8.2.9.3	Clearing Cable Diagnostic Statistics .....	290
8.3	Managing Ethernet Trunk Interfaces .....	290
8.3.1	Viewing a List of Ethernet Trunk Interfaces .....	290
8.3.2	Adding an Ethernet Trunk Interface .....	290
8.3.3	Deleting an Ethernet Trunk Interface .....	293
8.3.4	Managing Ethernet Trunk Ports .....	293
8.3.4.1	Viewing a List of Ethernet Trunk Ports .....	293
8.3.4.2	Adding an Ethernet Trunk Port .....	294
8.3.4.3	Deleting an Ethernet Trunk Port .....	294
8.4	Managing MAC Addresses .....	294

8.4.1	Viewing a Dynamic List of MAC Addresses .....	294
8.4.2	Purging the Dynamic MAC Address List .....	295
8.4.3	Configuring MAC Address Learning Options .....	295
8.4.4	Managing Static MAC Addresses .....	296
8.4.4.1	Viewing a List of Static MAC Addresses .....	296
8.4.4.2	Adding a Static MAC Address .....	296
8.4.4.3	Deleting a Static MAC Address .....	297
8.5	Managing Multicast Filtering .....	298
8.5.1	Multicast Filtering Concepts .....	298
8.5.1.1	IGMP .....	298
8.5.1.2	GMRP (GARP Multicast Registration Protocol) .....	302
8.5.2	Enabling and Configuring GMRP .....	305
8.5.3	Managing IGMP Snooping .....	306
8.5.3.1	Configuring IGMP Snooping .....	306
8.5.3.2	Viewing a List of Router Ports .....	307
8.5.3.3	Adding a Router Port .....	307
8.5.3.4	Deleting a Router Port .....	307
8.5.4	Managing the Static Multicast Group Table .....	307
8.5.4.1	Viewing a List of Static Multicast Group Entries .....	307
8.5.4.2	Adding a Static Multicast Group Entry .....	308
8.5.4.3	Deleting a Static Multicast Group Entry .....	308
8.5.5	Managing Egress Ports for Multicast Groups .....	309
8.5.5.1	Viewing a List of Egress Ports .....	309
8.5.5.2	Adding an Egress Port .....	309
8.5.5.3	Deleting an Egress Port .....	309
8.5.6	Viewing a Summary of Multicast Groups .....	309
8.5.7	Viewing a List of IP Multicast Groups .....	310
8.6	Managing VLANs .....	311
8.6.1	VLAN Concepts .....	311
8.6.1.1	Tagged vs. Untagged Frames .....	311
8.6.1.2	Native VLAN .....	311
8.6.1.3	Edge and Trunk Port Types .....	312
8.6.1.4	Ingress Filtering .....	312
8.6.1.5	Forbidden Ports List .....	313
8.6.1.6	VLAN-Aware Mode of Operation .....	313
8.6.1.7	GARP VLAN Registration Protocol (GVRP) .....	313
8.6.1.8	PVLAN Edge .....	315
8.6.1.9	Restricted VLANs .....	315
8.6.1.10	VLAN Advantages .....	316
8.6.2	Configuring the Internal VLAN Range .....	318
8.6.3	Enabling/Disabling Ingress Filtering .....	319
8.6.4	Managing VLANs for Switched Ethernet Ports .....	320
8.6.4.1	Viewing VLAN Assignments for Switched Ethernet Ports .....	320
8.6.4.2	Configuring VLANs for Switched Ethernet Ports .....	320
8.6.5	Managing Static VLANs .....	321
8.6.5.1	Viewing a List of Static VLANs .....	321
8.6.5.2	Adding a Static VLAN .....	321
8.6.5.3	Deleting a Static VLAN .....	322

8.6.6	Managing Forbidden Ports .....	322
8.6.6.1	Viewing a List of Forbidden Ports .....	322
8.6.6.2	Adding a Forbidden Port .....	323
8.6.6.3	Deleting a Forbidden Port .....	323
8.6.7	Managing VLANs for Interfaces and Tunnels .....	323
<b>9</b>	<b>Layer 3 .....</b>	<b>325</b>
9.1	Layer 3 Switching Concepts .....	325
9.1.1	Layer 3 Switch Forwarding Table .....	325
9.1.2	Static Layer 3 Switching Rules .....	326
9.1.3	Dynamic Learning of Layer 3 Switching Rules .....	326
9.1.4	Layer 3 Switch ARP Table .....	327
9.1.5	Multicast Cross-VLAN Layer 2 Switching .....	327
9.1.6	Size of the Layer 3 Switch Forwarding Table .....	328
9.1.7	Interaction with the Firewall .....	328
9.1.8	Layer 3 Switching Summary .....	328
9.2	Configuring Layer 3 Switching .....	329
9.3	Enabling/Disabling IPsec Hardware Acceleration .....	331
9.4	Managing Static ARP Table Entries .....	331
9.4.1	Viewing a List of ARP Table Entries .....	332
9.4.2	Adding a Static ARP Table Entry .....	332
9.4.3	Deleting a Static ARP Table Entry .....	332
9.5	Viewing a Static and Dynamic ARP Table Summary .....	333
9.6	Viewing Routing Rules .....	333
9.7	Flushing Dynamic Hardware Routing Rules .....	334
<b>10</b>	<b>Serial Server .....</b>	<b>335</b>
10.1	Managing Serial Ports .....	335
10.1.1	Viewing Serial Port Statistics .....	335
10.1.2	Viewing Transport Connection Statistics .....	336
10.1.3	Viewing DNP Device Table Statistics .....	337
10.1.4	Restarting the Serial Server .....	337
10.2	Managing Serial Port Protocols .....	338
10.2.1	Serial Port Protocol Concepts .....	338
10.2.1.1	Raw Socket Applications .....	338
10.2.1.2	Modbus TCP Applications .....	339
10.2.1.3	DNP Applications .....	340
10.2.1.4	MicroLok Applications .....	341
10.2.1.5	Incoming/Outgoing Serial Connections .....	343
10.2.2	Viewing a List of Serial Port Protocols .....	343
10.2.3	Adding a Serial Port Protocol .....	344
10.2.4	Configuring the DNP Protocol .....	344
10.2.5	Configuring the Modbus TCP Protocol .....	345
10.2.6	Configuring the Raw Socket Protocol .....	346
10.2.7	Configuring the MicroLok Protocol .....	348
10.2.8	Deleting a Serial Port Protocol .....	348

---

10.3	Managing DNP Device Address Tables .....	348
10.3.1	Viewing a List of DNP Device Address Tables .....	349
10.3.2	Adding a DNP Device Address Table .....	349
10.3.3	Deleting a Device Address Table .....	350
10.4	Managing MicroLok Device Address Tables .....	350
10.4.1	Viewing a List of MicroLok Device Address Tables .....	350
10.4.2	Adding a MicroLok Device Address Table .....	350
10.4.3	Deleting a MicroLok Device Address Table .....	351
10.5	Managing Serial Multicast Streaming .....	352
10.5.1	Understanding Serial Multicast Streaming .....	352
10.5.1.1	Sink vs. Source Ports .....	352
10.5.1.2	Multicast Streaming Examples .....	352
10.5.2	Configuring Serial Multicast Streaming .....	353
10.5.3	Example: Serial Interfaces Configured as a Sink for Multicast Streams .....	353
10.5.4	Example: Serial Interfaces Configured as a Source for Multicast Streams .....	355
10.5.5	Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams ..	357
10.6	Managing Remote Hosts .....	360
10.6.1	Viewing a List of Remote Hosts .....	360
10.6.2	Adding a Remote Host .....	360
10.6.3	Deleting a Remote Host .....	361
10.7	Managing Local Hosts .....	361
10.7.1	Viewing a List of Local Hosts .....	361
10.7.2	Adding a Local Host .....	361
10.7.3	Deleting a Local Host .....	362
10.8	Managing Remote Host Interfaces .....	362
10.8.1	Viewing a List of Remote Host Interfaces .....	363
10.8.2	Adding a Remote Host Interface .....	363
10.8.3	Deleting a Remote Host Interface .....	363
10.9	Managing Local Host Interfaces .....	364
10.9.1	Viewing a List of Local Host Interfaces .....	364
10.9.2	Adding a Local Host Interface .....	364
10.9.3	Deleting a Local Host Interface .....	364
<b>11</b>	<b>Tunneling and VPNs .....</b>	<b>365</b>
11.1	Configuring L2TP Tunnels .....	365
11.2	Managing Virtual Switches .....	366
11.2.1	Viewing a List of Virtual Switches .....	368
11.2.2	Adding a Virtual Switch .....	368
11.2.3	Deleting a Virtual Switch .....	369
11.2.4	Managing Virtual Switch Interfaces .....	370
11.2.4.1	Viewing a List of Virtual Switch Interfaces .....	370
11.2.4.2	Adding a Virtual Switch Interface .....	370
11.2.4.3	Deleting a Virtual Switch Interface .....	371
11.2.5	Filtering Virtual Switch Traffic .....	371
11.2.5.1	Enabling/Disabling Virtual Switch Filtering .....	371
11.2.5.2	Viewing a List of Virtual Switch Filters .....	371

11.2.5.3	Adding a Virtual Switch Filter .....	372
11.2.5.4	Deleting a Virtual Switch Filter .....	372
11.2.6	Managing Filtering Rules .....	372
11.2.6.1	Viewing a List of Rules .....	372
11.2.6.2	Viewing a List of Rules Assigned to a Virtual Switch Filter .....	372
11.2.6.3	Adding a Rule .....	373
11.2.6.4	Adding a Rule to a Virtual Switch Filter .....	374
11.2.6.5	Deleting a Rule .....	374
11.2.6.6	Deleting a Rule from a Virtual Switch Filter .....	374
11.2.7	Managing In/Out Interfaces .....	375
11.2.7.1	Viewing a List of In/Out Interfaces .....	375
11.2.7.2	Adding an In/Out Interface .....	375
11.2.7.3	Deleting an In/Out Interface .....	375
11.2.8	Managing VLANs for Virtual Switches .....	376
11.2.8.1	Viewing a List of Virtual Switch VLANs .....	376
11.2.8.2	Adding a Virtual Switch VLAN .....	376
11.2.8.3	Deleting a Virtual Switch VLAN .....	377
11.3	Managing the Layer2 Tunnel Daemon .....	377
11.3.1	Viewing Round Trip Time Statistics .....	377
11.3.2	Configuring the Layer 2 Tunnel Daemon .....	378
11.4	Managing L2TPv3 Tunnels .....	379
11.4.1	L2TPv3 Tunnel Scenarios .....	379
11.4.2	Creating an L2TPv3 Tunnel .....	381
11.4.3	Managing Static L2TPv3 Tunnels .....	381
11.4.3.1	Enabling/Disabling Static L2TPv3 Tunnels .....	381
11.4.3.2	Viewing a List of Static L2TPv3 Tunnels .....	382
11.4.3.3	Adding a Static L2TPv3 Tunnel .....	382
11.4.3.4	Deleting a Static L2TPv3 Tunnel .....	383
11.4.4	Managing Dynamic L2TPv3 Tunnels .....	383
11.4.4.1	Enabling and Configuring Dynamic L2TPv3 Tunnels .....	383
11.4.4.2	Viewing a List of Dynamic L2TPv3 Tunnels .....	384
11.4.4.3	Adding a Dynamic L2TPv3 Tunnel .....	384
11.4.4.4	Deleting a Dynamic L2TPv3 Tunnel .....	386
11.4.5	Managing Sessions for L2TPv3 Tunnels .....	387
11.4.5.1	Viewing a List of Sessions .....	387
11.4.5.2	Adding a Session for a Static L2TPv3 Tunnel .....	387
11.4.5.3	Adding a Session for a Dynamic L2TPv3 Tunnel .....	388
11.4.5.4	Configuring Local and Remote Cookies .....	389
11.4.5.5	Deleting a Session .....	390
11.4.6	Managing VLANs for L2TPv3 Tunnels .....	390
11.4.6.1	Viewing a List of VLANs .....	390
11.4.6.2	Adding a VLAN .....	391
11.4.6.3	Deleting a VLAN .....	391
11.4.7	Example: Establishing an L2TPv3 Tunnel Between Routers .....	391
11.5	Managing GOOSE Tunnels .....	393
11.5.1	Viewing the GOOSE Tunnel Statistics .....	395
11.5.2	Viewing a List of GOOSE Tunnels .....	395
11.5.3	Adding a GOOSE Tunnel .....	395

11.5.4	Deleting a GOOSE Tunnel .....	396
11.5.5	Managing Remote Daemons for GOOSE Tunnels .....	396
11.5.5.1	Viewing a List of Remote Daemons .....	396
11.5.5.2	Adding a Remote Daemon .....	397
11.5.5.3	Deleting a Remote Daemon .....	397
11.5.6	Example: Establishing a GOOSE Tunnel Between Routers .....	397
11.6	Managing Generic Tunnels .....	399
11.6.1	Viewing the Generic Tunnel Statistics .....	399
11.6.2	Viewing a List of Generic Tunnels .....	399
11.6.3	Adding a Generic Tunnel .....	400
11.6.4	Deleting a Generic Tunnel .....	400
11.6.5	Managing Remote Daemon IP Addresses for Generic Tunnels .....	400
11.6.5.1	Viewing a List of IP Addresses .....	401
11.6.5.2	Adding an IP Address .....	401
11.6.5.3	Deleting an IP Address .....	401
11.6.6	Managing Remote Daemon Egress Interfaces for Generic Tunnels .....	402
11.6.6.1	Viewing a List of Egress Interfaces .....	402
11.6.6.2	Adding an Egress Interface .....	402
11.6.6.3	Deleting an Egress Interface .....	402
11.6.7	Managing Ethernet Types for Generic Tunnels .....	403
11.6.7.1	Viewing a List of Ethernet Types .....	403
11.6.7.2	Adding an Ethernet Type .....	403
11.6.7.3	Deleting an Ethernet Type .....	403
11.7	Managing Generic Routing Encapsulation Tunnels .....	404
11.7.1	Viewing Statistics for GRE Tunnels .....	404
11.7.2	Viewing a List of GRE Tunnels .....	405
11.7.3	Adding a GRE Tunnel .....	405
11.7.4	Configuring a DSCP Marking for GRE Tunnel Traffic .....	407
11.7.5	Enabling/Disabling Keepalive Messages .....	408
11.7.6	Deleting a GRE Tunnel .....	409
11.7.7	Example: Configuring a GRE Tunnel with IPsec .....	409
11.8	Managing IPsec Tunnels .....	415
11.8.1	IPsec Tunneling Concepts .....	416
11.8.1.1	IPsec Modes .....	416
11.8.1.2	Supported Encryption Protocols .....	416
11.8.1.3	Public and Secret Key Cryptography .....	417
11.8.1.4	X509 Certificates .....	417
11.8.1.5	NAT Traversal .....	417
11.8.1.6	Remote IPsec Client Support .....	418
11.8.1.7	IPsec and Router Interfaces .....	418
11.8.2	Configuring IPsec Tunnels .....	418
11.8.3	Configuring Certificates and Keys .....	419
11.8.4	Viewing the IPsec Tunnel Status .....	420
11.8.5	Managing Pre-Shared Keys .....	420
11.8.5.1	Viewing a List of Pre-Shared Keys .....	420
11.8.5.2	Adding a Pre-Shared Key .....	420
11.8.5.3	Deleting a Pre-Shared Key .....	421
11.8.6	Managing Connections .....	421

11.8.6.1	Viewing a List of Connections .....	421
11.8.6.2	Adding a Connection .....	421
11.8.6.3	Configuring Dead Peer Detection .....	424
11.8.6.4	Deleting a Connection .....	425
11.8.6.5	Viewing the Status of a Connection .....	425
11.8.7	Managing the Internet Key Exchange (IKE) Protocol .....	426
11.8.7.1	Viewing a List of IKE Algorithms .....	426
11.8.7.2	Adding an IKE Algorithm .....	426
11.8.7.3	Deleting an IKE Algorithm .....	427
11.8.8	Managing the Encapsulated Security Payload (ESP) Protocol .....	427
11.8.8.1	Configuring ESP Encryption .....	427
11.8.8.2	Viewing a List of ESP Algorithms .....	428
11.8.8.3	Adding an ESP Algorithm .....	428
11.8.8.4	Deleting an ESP Algorithm .....	429
11.8.9	Managing Connection Ends .....	429
11.8.9.1	Configuring the Public IP Address for a Connection End .....	429
11.8.9.2	Configuring the System Public Key for a Connection End .....	430
11.8.9.3	Configuring the System Identifier for a Connection End .....	431
11.8.9.4	Configuring the Next Hop for a Connection End .....	431
11.8.9.5	Configuring the NAT Traversal Negotiation Method for a Connection End .....	432
11.8.10	Managing Private Subnets .....	433
11.8.10.1	Viewing a List of Addresses for Private Subnets .....	433
11.8.10.2	Adding an Address for a Private Subnet .....	433
11.8.10.3	Deleting an Address for a Private Subnet .....	433
11.8.11	Example: Configuring an Encrypted VPN Tunnel .....	433
11.9	Managing 6in4 and 4in6 Tunnels .....	437
11.9.1	Enabling/Disabling 6in4 or 4in6 Tunnels .....	438
11.9.2	Viewing a List of 6in4 or 4in6 Tunnels .....	438
11.9.3	Viewing the Status of 6in4/4in6 Tunnels .....	438
11.9.4	Adding a 6in4 or 4in6 Tunnel .....	438
11.9.5	Deleting a 6in4 or 4in6 Tunnel .....	439
11.10	Managing DMVPN .....	439
11.10.1	Understanding DMVPN .....	440
11.10.2	Configuring DMVPN .....	441
11.10.3	Managing DMVPN Interfaces .....	442
11.10.3.1	Viewing a List of DMVPN Interfaces .....	442
11.10.3.2	Adding a DMVPN Interface .....	442
11.10.3.3	Deleting a DMVPN Interface .....	443
11.10.4	Viewing the Status of DMVPN .....	443
<b>12</b>	<b>Unicast and Multicast Routing .....</b>	<b>445</b>
12.1	Viewing the Status of IPv4 Routes .....	445
12.2	Viewing the Status of IPv6 Routes .....	446
12.3	Viewing the Memory Statistics .....	446
12.4	Configuring ICMP .....	447
12.5	Managing Event Trackers .....	447

12.5.1	Viewing a List of Event Trackers .....	448
12.5.2	Viewing Event Tracker Statistics .....	448
12.5.3	Adding an Event Tracker .....	449
12.5.4	Deleting an Event Tracker .....	450
12.6	Managing IS-IS .....	450
12.6.1	IS-IS Concepts .....	450
12.6.1.1	IS-IS Routers .....	450
12.6.1.2	Network Entity Title (NET) Addresses .....	451
12.6.1.3	Advantages and Disadvantages of Using IS-IS .....	451
12.6.2	Configuring IS-IS .....	452
12.6.3	Viewing the Status of Neighbors .....	453
12.6.4	Viewing the Status of the Link-State Database .....	454
12.6.5	Managing Area Tags .....	454
12.6.5.1	Viewing a List of Area Tags .....	454
12.6.5.2	Adding an Area Tag .....	455
12.6.5.3	Deleting an Area Tag .....	456
12.6.6	Managing Interfaces .....	456
12.6.6.1	Viewing a List of Interfaces .....	457
12.6.6.2	Configuring an Interface .....	457
12.6.7	Managing LSP Generation .....	458
12.6.7.1	Viewing a List of LSP Generation Intervals .....	458
12.6.7.2	Adding an LSP Generation Interval .....	459
12.6.7.3	Deleting an LSP Generation Interval .....	459
12.6.8	Managing SPF Calculations .....	459
12.6.8.1	Viewing a List of SPF Calculation Intervals .....	460
12.6.8.2	Adding an SPF Calculation Interval .....	460
12.6.8.3	Deleting an SPF Calculation Interval .....	460
12.6.9	Managing the Lifetime of LSPs .....	461
12.6.9.1	Viewing a List of LSP Lifetime Intervals .....	461
12.6.9.2	Adding an LSP Lifetime Interval .....	461
12.6.9.3	Deleting an LSP Lifetime Interval .....	462
12.6.10	Managing LSP Refresh Intervals .....	462
12.6.10.1	Viewing a List of LSP Refresh Intervals .....	463
12.6.10.2	Adding an LSP Refresh Interval .....	463
12.6.10.3	Deleting an LSP Refresh Interval .....	464
12.6.11	Managing Network Entity Titles (NETs) .....	464
12.6.11.1	Viewing a List of NETs .....	464
12.6.11.2	Adding a NET .....	465
12.6.11.3	Deleting a NET .....	465
12.6.12	Managing Redistribution Metrics .....	465
12.6.12.1	Viewing a List of Redistribution Metrics .....	466
12.6.12.2	Adding a Redistribution Metric .....	466
12.6.12.3	Deleting a Redistribution Metric .....	467
12.7	Managing RIP .....	467
12.7.1	Configuring RIP .....	468
12.7.2	Viewing the Status of Dynamic RIP Routes .....	469
12.7.3	Managing Prefix Lists and Entries .....	471
12.7.3.1	Viewing a List of Prefix Lists .....	471



12.7.3.2	Viewing a List of Prefix Entries .....	471
12.7.3.3	Adding a Prefix List .....	472
12.7.3.4	Adding a Prefix Entry .....	472
12.7.3.5	Deleting a Prefix List .....	473
12.7.3.6	Deleting a Prefix Entry .....	473
12.7.4	Managing Networks .....	473
12.7.4.1	Configuring a Network .....	474
12.7.4.2	Tracking Commands .....	474
12.7.5	Managing Network IP Addresses .....	475
12.7.5.1	Viewing a List of Network IP Addresses .....	475
12.7.5.2	Adding a Network IP Address .....	475
12.7.5.3	Deleting a Network IP Address .....	476
12.7.6	Managing Network Interfaces .....	476
12.7.6.1	Viewing a List of Network Interfaces .....	476
12.7.6.2	Adding a Network Interface .....	476
12.7.6.3	Deleting a Network Interface .....	476
12.7.7	Managing Neighbors .....	477
12.7.7.1	Viewing a List of Neighbors .....	477
12.7.7.2	Adding a Neighbor .....	477
12.7.7.3	Deleting a Neighbor .....	477
12.7.8	Managing the Prefix List Distribution .....	477
12.7.8.1	Viewing a List of Prefix List Distribution Paths .....	478
12.7.8.2	Adding a Prefix List Distribution Path .....	478
12.7.8.3	Deleting a Prefix List Distribution Path .....	478
12.7.9	Managing Key Chains and Keys .....	479
12.7.9.1	Viewing a List of Key Chains .....	479
12.7.9.2	Viewing a List of Keys .....	479
12.7.9.3	Adding a Key Chain .....	479
12.7.9.4	Adding a Key .....	480
12.7.9.5	Deleting a Key Chain .....	481
12.7.9.6	Deleting a Key .....	481
12.7.10	Managing Redistribution Metrics .....	481
12.7.10.1	Viewing a List of Redistribution Metrics .....	481
12.7.10.2	Adding a Redistribution Metric .....	482
12.7.10.3	Deleting a Redistribution Metric .....	482
12.7.11	Managing Routing Interfaces .....	482
12.7.11.1	Viewing a List of Routing Interfaces .....	482
12.7.11.2	Configuring a Routing Interface .....	482
12.8	Managing BGP .....	483
12.8.1	Configuring BGP .....	484
12.8.2	Managing Route Maps .....	485
12.8.2.1	Viewing a List of Route Map Filters .....	485
12.8.2.2	Viewing a List of Route Map Filter Entries .....	485
12.8.2.3	Adding a Route Map Filter .....	486
12.8.2.4	Adding a Route Map Filter Entry .....	486
12.8.2.5	Deleting a Route Map Filter .....	487
12.8.2.6	Deleting a Route Map Filter Entry .....	487
12.8.2.7	Configuring Match Rules .....	487
12.8.2.8	Configuring a Set .....	488

12.8.3	Managing Prepended and Excluded Autonomous System Path Filters .....	489
12.8.3.1	Viewing a List of Prepended Autonomous System Path Filters .....	489
12.8.3.2	Viewing a List of Excluded Autonomous System Paths .....	490
12.8.3.3	Adding a Prepended Autonomous System Path Filter .....	490
12.8.3.4	Adding an Excluded Autonomous System Path filter .....	491
12.8.3.5	Deleting a Prepended Autonomous System Path Filter .....	491
12.8.3.6	Deleting an Excluded Autonomous System Path Filter .....	491
12.8.4	Managing Prefix Lists and Entries .....	492
12.8.4.1	Viewing a List of Prefix Lists .....	492
12.8.4.2	Viewing a List of Prefix Entries .....	492
12.8.4.3	Adding a Prefix List .....	492
12.8.4.4	Adding a Prefix Entry .....	493
12.8.4.5	Deleting a Prefix List .....	493
12.8.4.6	Deleting a Prefix Entry .....	494
12.8.5	Managing Autonomous System Paths and Entries .....	494
12.8.5.1	Viewing a List of Autonomous System Paths .....	494
12.8.5.2	Viewing a List of Autonomous System Path Entries .....	494
12.8.5.3	Adding an Autonomous System Path Filter .....	495
12.8.5.4	Adding an Autonomous System Path Filter Entry .....	495
12.8.5.5	Deleting an Autonomous System Path .....	496
12.8.5.6	Deleting an Autonomous System Path Filter Entry .....	496
12.8.6	Managing Neighbors .....	497
12.8.6.1	Viewing a List of Neighbors .....	497
12.8.6.2	Adding a Neighbor .....	497
12.8.6.3	Configuring the Distribution of Prefix Lists .....	498
12.8.6.4	Tracking Commands for BGP Neighbors .....	499
12.8.6.5	Deleting a Neighbor .....	499
12.8.7	Managing Networks .....	500
12.8.7.1	Viewing a List of Networks .....	500
12.8.7.2	Adding a Network .....	500
12.8.7.3	Tracking Commands for a BGP Network .....	501
12.8.7.4	Deleting a Network .....	502
12.8.8	Managing Aggregate Addresses .....	502
12.8.8.1	Viewing a List of Aggregate Addresses .....	502
12.8.8.2	Adding an Aggregate Address .....	502
12.8.8.3	Deleting an Aggregate Address .....	503
12.8.9	Managing Aggregate Address Options .....	503
12.8.9.1	Viewing a List of Aggregate Address Options .....	503
12.8.9.2	Adding an Aggregate Address Option .....	503
12.8.9.3	Deleting an Aggregate Address Option .....	504
12.8.10	Managing Redistribution Metrics .....	504
12.8.10.1	Viewing a List of Redistribution Metrics .....	504
12.8.10.2	Adding a Redistribution Metric .....	504
12.8.10.3	Deleting a Redistribution Metric .....	505
12.8.11	Managing Route Reflector Options .....	505
12.8.11.1	Understanding Route Reflectors .....	505
12.8.11.2	Configuring the Device as a Route Reflector .....	508
12.8.11.3	Configuring BGP Neighbors as Clients .....	508
12.8.11.4	Example: Basic Route Reflection .....	509

12.8.11.5	Example: Linking Clusters .....	511
12.8.11.6	Example: Clusters in Clusters .....	513
12.8.11.7	Example: Route Reflection in a VRF Instance .....	515
12.8.11.8	Example: Route Reflection with VPNv4 Clients .....	519
12.8.12	Viewing the Status of Dynamic BGP Routes .....	519
12.8.13	Resetting a BGP Session .....	520
12.9	Managing OSPF .....	522
12.9.1	OSPF Concepts .....	522
12.9.2	Configuring OSPF .....	523
12.9.3	Viewing the Status of Dynamic OSPF Routes .....	525
12.9.4	Managing Prefix Lists and Entries .....	525
12.9.4.1	Viewing a List of Prefix Lists .....	525
12.9.4.2	Viewing a List of Prefix Entries .....	526
12.9.4.3	Adding a Prefix List .....	527
12.9.4.4	Adding a Prefix Entry .....	527
12.9.4.5	Deleting a Prefix List .....	528
12.9.4.6	Deleting a Prefix Entry .....	529
12.9.5	Managing Areas .....	529
12.9.5.1	Viewing a List of Areas .....	529
12.9.5.2	Adding an Area .....	530
12.9.5.3	Deleting an Area .....	531
12.9.6	Managing Route Maps .....	531
12.9.6.1	Viewing a List of Route Map Filters .....	531
12.9.6.2	Viewing a List of Route Map Filter Entries .....	532
12.9.6.3	Adding a Route Map Filter .....	532
12.9.6.4	Adding a Route Map Filter Entry .....	533
12.9.6.5	Deleting a Route Map Filter .....	534
12.9.6.6	Deleting a Route Map Filter Entry .....	534
12.9.6.7	Configuring Match Rules .....	535
12.9.7	Managing Incoming Route Filters .....	535
12.9.7.1	Viewing List of Incoming Route Filters .....	536
12.9.7.2	Adding an Incoming Route Filter .....	536
12.9.7.3	Deleting an Incoming Route Filter .....	536
12.9.8	Managing Redistribution Metrics .....	537
12.9.8.1	Viewing a List of Redistribution Metrics .....	537
12.9.8.2	Adding a Redistribution Metric .....	537
12.9.8.3	Deleting a Redistribution Metric .....	538
12.9.9	Managing Routing Interfaces .....	538
12.9.9.1	Viewing a List of Routing Interfaces .....	538
12.9.9.2	Configuring a Routing Interface .....	539
12.9.10	Managing Message Digest Keys .....	541
12.9.10.1	Viewing a List of Message Digest Keys .....	541
12.9.10.2	Adding a Message Digest Key .....	542
12.9.10.3	Deleting a Message Digest Key .....	542
12.9.11	Managing ABR Route Summarization .....	543
12.9.11.1	Understanding ABR Route Summarization .....	543
12.9.11.2	Viewing a List of Summary Routes .....	543
12.9.11.3	Adding a Summary Route .....	544
12.9.11.4	Deleting a Summary Route .....	544

12.9.11.5	Example: Basic Route Summarization .....	544
12.10	Managing MPLS .....	546
12.10.1	Viewing the Status of IP Binding .....	547
12.10.2	Viewing the Status of the Forwarding Table .....	547
12.10.3	Enabling/Disabling MPLS .....	548
12.10.4	Managing the MPLS Interfaces .....	548
12.10.4.1	Viewing the Status of MPLS Interfaces .....	548
12.10.4.2	Viewing a List of MPLS Interfaces .....	548
12.10.4.3	Enabling/Disabling an MPLS Interface .....	549
12.10.5	Managing Static Label Binding .....	549
12.10.5.1	Viewing the Status of Static Label Binding .....	549
12.10.5.2	Viewing a List of Static Labels .....	550
12.10.5.3	Adding a Static Label .....	550
12.10.5.4	Deleting a Static Label .....	551
12.10.6	Managing Static Cross-Connects .....	551
12.10.6.1	Viewing the Status of Static Cross-Connects .....	551
12.10.6.2	Viewing a List of Static Cross-Connects .....	552
12.10.6.3	Adding a Static Cross-Connect .....	552
12.10.6.4	Deleting a Static Cross-Connect .....	553
12.10.7	Managing LDP .....	553
12.10.7.1	Viewing the Status of LDP Binding .....	553
12.10.7.2	Viewing the Status of the LDP Discovery Interfaces .....	554
12.10.7.3	Viewing the Status of the LDP Neighbor Local Node Information .....	554
12.10.7.4	Viewing the Status of the LDP Neighbor Connection Information .....	555
12.10.7.5	Viewing the Status of the LDP Neighbor Discovery Information .....	555
12.10.7.6	Configuring LDP .....	556
12.10.7.7	Configuring Neighbor Discovery .....	556
12.10.7.8	Viewing a List of LDP Interfaces .....	557
12.10.7.9	Enabling/Disabling an LDP Interface .....	557
12.11	Managing Virtual Routing and Forwarding (VRF) .....	558
12.11.1	VRF Concepts .....	558
12.11.1.1	VRF and VRF-Lite .....	558
12.11.1.2	Advantages and Disadvantages of Using VRF .....	558
12.11.2	Viewing VRF Interface Statistics .....	559
12.11.3	Configuring VRF .....	559
12.11.4	Configuring a VRF Interface .....	560
12.11.5	Managing VRF Definitions .....	561
12.11.5.1	Viewing a List of VRF Definitions .....	561
12.11.5.2	Adding a VRF Definition .....	562
12.11.5.3	Deleting a VRF Definition .....	563
12.11.6	Managing Route Targets .....	563
12.11.6.1	Viewing a List of Route Targets .....	563
12.11.6.2	Adding a Route Target .....	563
12.11.6.3	Deleting a Route Target .....	564
12.11.7	Managing VRF Instances and OSPF .....	564
12.11.7.1	Viewing a List of VRF Instances .....	564
12.11.7.2	Adding a VRF Instance and Configuring OSPF .....	564
12.11.7.3	Deleting a VRF Instance .....	566

12.11.8	Managing IP/VPN Tunnels .....	567
12.11.8.1	Viewing a List of IP/VPN Tunnels .....	567
12.11.8.2	Adding an IP/VPN Tunnel .....	567
12.11.8.3	Deleting an IP/VPN Tunnels .....	568
12.11.9	Managing VPNv4 Neighbors .....	568
12.11.9.1	Viewing a List of Neighbors .....	568
12.11.9.2	Adding a Neighbor .....	568
12.11.9.3	Deleting a Neighbor .....	569
12.11.10	Managing IPv4 Address Families .....	569
12.11.10.1	Viewing a List of IPv4 Address Families .....	569
12.11.10.2	Adding an IPv4 Address Family .....	569
12.11.10.3	Deleting an IPv4 Address Family .....	570
12.11.11	Managing Redistribution for IPv4 Address Families .....	570
12.11.11.1	Viewing a List of Redistributions .....	570
12.11.11.2	Adding a Redistribution .....	571
12.11.11.3	Deleting a Redistribution .....	571
12.11.12	Managing Neighbors for IPv4 Address Families .....	571
12.11.12.1	Viewing a List of Neighbors .....	572
12.11.12.2	Adding a Neighbor .....	572
12.11.12.3	Configuring the Distribution of Prefix Lists .....	573
12.11.12.4	Tracking Commands .....	574
12.11.12.5	Deleting a Neighbor .....	574
12.11.13	Managing Static VRF Routes .....	575
12.11.13.1	Viewing a List of Static VRF Routes .....	575
12.11.13.2	Adding a Static VRF Route .....	575
12.11.13.3	Configuring a Black Hole Connection for a Static VRF Route .....	576
12.11.13.4	Deleting a Static VRF Route .....	576
12.11.14	Managing Gateways for Static VRF Routes .....	577
12.11.14.1	Viewing a List of Gateways for Static VRF Routes .....	577
12.11.14.2	Adding a Gateway for a Static VRF Route .....	577
12.11.14.3	Deleting a Gateway for a Static VRF Route .....	578
12.11.15	Managing Interfaces for Static VRF Routes .....	578
12.11.15.1	Viewing a List of Interfaces for Static VRF Routes .....	578
12.11.15.2	Adding a Gateway for a Static VRF Route .....	578
12.11.15.3	Deleting a Gateway for a Static VRF Route .....	579
12.11.16	Example: Configuring OSPF on a VRF-Lite Instance .....	579
12.11.17	Example: Configuring BGP on a VRF-Lite Instance .....	582
12.12	Managing Static Routing .....	585
12.12.1	Viewing a List of Static Routes .....	585
12.12.2	Adding an IPv4 Static Route .....	585
12.12.3	Adding an IPv6 Static Route .....	586
12.12.4	Deleting a Static Route .....	587
12.12.5	Configuring a Black Hole Connection for an IPv4 Static Route .....	587
12.12.6	Managing Gateways for Static Routes .....	588
12.12.6.1	Configuring Gateways for IPv6 Static Routes .....	588
12.12.6.2	Viewing a List of Gateways for IPv4 Static Routes .....	588
12.12.6.3	Adding a Gateway for an IPv4 Static Route .....	588
12.12.6.4	Deleting a Gateway for an IPv4 Static Route .....	589
12.12.7	Managing Interfaces for Static Routes .....	589

12.12.7.1	Configuring Interfaces for IPv6 Static Routes .....	589
12.12.7.2	Viewing a List of Interfaces for IPv4 Static Routes .....	590
12.12.7.3	Adding an Interface for an IPv4 Static Route .....	590
12.12.7.4	Deleting an Interface for an IPv4 Static Route .....	590
12.13	Managing Static Multicast Routing .....	591
12.13.1	Enabling/Disabling Static Multicast Routing .....	591
12.13.2	Managing Static Multicast Groups .....	591
12.13.2.1	Viewing a List of Static Multicast Groups .....	591
12.13.2.2	Adding a Static Multicast Group .....	592
12.13.2.3	Deleting a Static Multicast Group .....	593
12.13.3	Managing Out-Interfaces .....	593
12.13.3.1	Viewing a List of Out-Interfaces .....	593
12.13.3.2	Adding an Out-Interface .....	593
12.13.3.3	Deleting an Out-Interface .....	594
12.14	Managing Dynamic Multicast Routing .....	594
12.14.1	Understanding Protocol Independent Multicast .....	594
12.14.1.1	PIM-SM Concepts .....	594
12.14.1.2	Internet Group Management Protocol .....	596
12.14.1.3	PIM-SSM .....	596
12.14.2	Viewing the Status of PIM-SM .....	597
12.14.3	Viewing the Status of Dynamic Multicast Routing .....	599
12.14.4	Configuring PIM-SM .....	599
12.14.5	Setting the Device as a BSR Candidate .....	600
12.14.6	Setting the Device as an RP Candidate .....	600
12.14.7	Managing PIM-SM Interfaces .....	601
12.14.7.1	Viewing a List of PIM-SM Interfaces .....	601
12.14.7.2	Enabling/Disabling a PIM-SM Interface .....	601
12.14.8	Managing Static RP Addresses .....	602
12.14.8.1	Viewing a List of Static RP Addresses .....	602
12.14.8.2	Adding a Static RP Address .....	603
12.14.8.3	Deleting a Static RP Address .....	603
12.14.9	Managing Multicast Group Prefixes .....	604
12.14.9.1	Viewing a List of Multicast Group Prefixes .....	604
12.14.9.2	Adding a Multicast Group Prefix .....	604
12.14.9.3	Deleting a Multicast Group Prefix .....	604
12.14.10	Example: Configuring Protocol Independent Multicast .....	605
<b>13</b>	<b>Network Redundancy .....</b>	<b>611</b>
13.1	Managing VRRP .....	611
13.1.1	VRRP Concepts .....	611
13.1.1.1	Static Routing vs. VRRP .....	611
13.1.1.2	VRRP Terminology .....	612
13.1.1.3	Connection Synchronization .....	615
13.1.2	Viewing the Status of VRRP .....	615
13.1.3	Enabling/Disabling VRRP .....	616
13.1.4	Managing VRRP Trackers .....	616
13.1.4.1	Viewing a List of VRRP Trackers .....	617
13.1.4.2	Adding a VRRP Tracker .....	617

13.1.4.3	Deleting a VRRP Tracker .....	618
13.1.5	Managing VRRP Groups .....	618
13.1.5.1	Viewing a List of VRRP Groups .....	618
13.1.5.2	Adding a VRRP Group .....	618
13.1.5.3	Deleting a VRRP Group .....	619
13.1.6	Managing VRRP Instances .....	619
13.1.6.1	Viewing a List of VRRP Instances .....	619
13.1.6.2	Adding a VRRP Instance .....	619
13.1.6.3	Deleting a VRRP Instance .....	622
13.1.7	Managing VRRP Monitors .....	622
13.1.7.1	Viewing a List of VRRP Monitors .....	622
13.1.7.2	Adding a VRRP Monitor .....	622
13.1.7.3	Deleting a VRRP Monitor .....	623
13.1.8	Managing Track Scripts .....	623
13.1.8.1	Viewing a List of Track Scripts .....	623
13.1.8.2	Adding a Track Script .....	623
13.1.8.3	Deleting a Track Script .....	624
13.1.9	Managing Virtual IP Addresses .....	624
13.1.9.1	Viewing a List of Virtual IP Addresses .....	624
13.1.9.2	Adding a Virtual IP Address .....	624
13.1.9.3	Deleting a Virtual IP Address .....	625
13.1.10	Managing Connection Synchronization .....	625
13.1.10.1	Configuring Connection Synchronization .....	625
13.1.10.2	Enabling/Disabling Connection Synchronization .....	626
13.1.10.3	Viewing a List of Dedicated Links .....	626
13.1.10.4	Adding a Dedicated Link .....	626
13.1.10.5	Deleting a Dedicated Link .....	627
13.1.10.6	Selecting a Default Dedicated Link .....	627
13.1.10.7	Viewing the Status of Each Dedicated Link .....	628
13.2	Managing VRRP within VRF .....	629
13.2.1	Configuring VRRP within VRF .....	629
13.2.2	Viewing the VRRP Status for a VRF .....	629
13.2.3	Configuring VRRP Service for a VRF .....	630
13.2.3.1	Viewing a List of VRFs Configured with VRRP Service .....	630
13.2.3.2	Adding VRRP Service to a VRF .....	630
13.2.3.3	Deleting VRRP Service from a VRF .....	631
13.2.4	Managing VRRP Trackers for a VRF .....	631
13.2.4.1	Viewing a List of VRRP Trackers for a VRF .....	631
13.2.4.2	Adding a VRRP Tracker for a VRF .....	631
13.2.4.3	Deleting a VRRP Tracker for a VRF .....	633
13.2.5	Managing VRRP Groups for a VRF .....	633
13.2.5.1	Viewing a List of VRRP Groups for a VRF .....	633
13.2.5.2	Adding a VRRP Group for a VRF .....	633
13.2.5.3	Deleting a VRRP Group .....	634
13.2.6	Managing VRRP Instances for a VRF .....	634
13.2.6.1	Viewing a List of VRRP Instances for a VRF .....	634
13.2.6.2	Adding a VRRP Instance for a VRF .....	634
13.2.6.3	Deleting a VRRP Instance for a VRF .....	636
13.2.7	Managing VRRP Monitors for a VRF .....	636

13.2.7.1	Viewing a List of VRRP Monitors for a VRF .....	636
13.2.7.2	Adding a VRRP Monitor to a VRF .....	637
13.2.7.3	Deleting a VRRP Monitor from a VRF .....	637
13.2.8	Managing VRRP Track Scripts for a VRF .....	637
13.2.8.1	Viewing a List of VRRP Track Scripts for a VRF .....	638
13.2.8.2	Adding a VRRP Track Script to a VRF .....	638
13.2.8.3	Deleting a VRRP Track Script from a VRF .....	638
13.2.9	Managing Virtual IP Addresses for a VRF .....	639
13.2.9.1	Viewing a List of Virtual IP Addresses .....	639
13.2.9.2	Adding a Virtual IP Address to a VRF .....	639
13.2.9.3	Deleting a Virtual IP Address from a VRF .....	640
13.2.10	Example: Configuring VRRP within a VRF .....	640
13.3	Managing Link Failover Protection .....	643
13.3.1	Viewing the Link Failover Log .....	643
13.3.2	Viewing the Link Failover Status .....	643
13.3.3	Managing Link Failover Parameters .....	644
13.3.3.1	Viewing a List of Link Failover Parameters .....	644
13.3.3.2	Adding a Link Failover Parameter .....	644
13.3.3.3	Deleting a Link Failover Parameter .....	645
13.3.4	Managing Link Failover Backup Interfaces .....	646
13.3.4.1	Viewing a List of Link Failover Backup Interfaces .....	646
13.3.4.2	Adding a Link Failover Backup Interface .....	646
13.3.4.3	Deleting a Link Failover Backup Interface .....	647
13.3.5	Managing Link Failover Ping Targets .....	647
13.3.5.1	Viewing a List of Link Failover Ping Targets .....	647
13.3.5.2	Adding a Link Failover Ping Target .....	648
13.3.5.3	Deleting a Link Failover Ping target .....	648
13.3.6	Testing Link Failover .....	648
13.3.7	Canceling a Link Failover Test .....	649
13.4	Managing Spanning Tree Protocol .....	649
13.4.1	RSTP Operation .....	650
13.4.1.1	RSTP States and Roles .....	650
13.4.1.2	Edge Ports .....	652
13.4.1.3	Point-to-Point and Multipoint Links .....	652
13.4.1.4	Path and Port Costs .....	652
13.4.1.5	Bridge Diameter .....	653
13.4.1.6	eRSTP .....	654
13.4.1.7	Fast Root Failover .....	654
13.4.2	RSTP Applications .....	655
13.4.2.1	RSTP in Structured Wiring Configurations .....	655
13.4.2.2	RSTP in Ring Backbone Configurations .....	657
13.4.2.3	RSTP Port Redundancy .....	658
13.4.3	MSTP Operation .....	659
13.4.3.1	MSTP Regions and Interoperability .....	659
13.4.3.2	MSTP Bridge and Port Roles .....	660
13.4.3.3	Benefits of MSTP .....	661
13.4.3.4	Implementing MSTP on a Bridged Network .....	663
13.4.4	Configuring STP Globally .....	663



13.4.5	Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces .....	667
13.4.6	Managing Multiple Spanning Tree Instances Globally .....	668
13.4.6.1	Viewing Statistics for Multiple Spanning Tree Instances .....	669
13.4.6.2	Viewing a List of Multiple Spanning Tree Instances .....	670
13.4.6.3	Adding a Multiple Spanning Tree Instance .....	670
13.4.6.4	Deleting a Multiple Spanning Tree Instance .....	671
13.4.7	Managing Multiple Spanning Tree Instances Per-Port .....	671
13.4.7.1	Viewing Per-Port Multiple Spanning Tree Instance Statistics .....	671
13.4.7.2	Viewing a List of Per-Port Multiple Spanning Tree Instances .....	672
13.4.7.3	Adding a Port-Specific Multiple Spanning Tree Instance .....	673
13.4.7.4	Deleting a Port-Specific Multiple Spanning Tree Instances .....	674
13.4.8	Viewing the Status of RSTP .....	675
13.4.9	Viewing RSTP Per-Port Statistics .....	676
13.4.10	Clearing Spanning Tree Protocol Statistics .....	677
13.5	Managing Redundant Network Access (RNA) .....	677
13.5.1	Understanding RNA .....	678
13.5.1.1	Parallel Redundancy Protocol (PRP) .....	678
13.5.1.2	Supervision Frames .....	679
13.5.1.3	PRP Requirements .....	679
13.5.2	Configuring RNA .....	680
13.5.3	Viewing the Proxy Nodes Table .....	680
13.5.4	Viewing the Nodes Table .....	681
13.5.5	Viewing Statistics Collected for RNA Ports .....	681
13.5.6	Clearing Statistics Collected for RNA Ports .....	682
13.6	Managing the Media Redundancy Protocol (MRP) .....	683
13.6.1	Understanding MRP .....	683
13.6.1.1	MRP Operation .....	683
13.6.1.2	MRA .....	684
13.6.1.3	MRP Instances .....	685
13.6.1.4	Requirements and Restrictions .....	685
13.6.2	Configuring MRP Globally .....	685
13.6.3	Enabling/Disabling SNMP Traps for MRP .....	686
13.6.4	Viewing the List of MRP Instances .....	686
13.6.5	Adding an MRP Instance .....	686
13.6.6	Deleting an MRP Instance .....	688
13.6.7	Viewing the Status of MRP Instances .....	689
13.6.8	Example: Configuring an MRP Ring .....	690
<b>14</b>	<b>Network Discovery and Management .....</b>	<b>693</b>
14.1	Managing LLDP .....	693
14.1.1	Configuring LLDP .....	694
14.1.2	Viewing Global Statistics .....	695
14.1.3	Viewing Global Statistics and Advertised System Information .....	696
14.1.4	Viewing Statistics for LLDP Neighbors .....	698
14.1.5	Viewing Statistics for LLDP Ports .....	702
14.2	Managing SNMP .....	703
14.2.1	Enabling and Configuring SNMP Sessions .....	704
14.2.2	Viewing Statistics for SNMP .....	706

14.2.3	Discovering SNMP Engine IDs .....	707
14.2.4	Managing SNMP Communities .....	707
14.2.4.1	Viewing a List of SNMP Communities .....	707
14.2.4.2	Adding an SNMP Community .....	708
14.2.4.3	Deleting an SNMP Community .....	708
14.2.5	Managing SNMP Target Addresses .....	708
14.2.5.1	Viewing a List of SNMP Target Addresses .....	708
14.2.5.2	Adding an SNMP Target Address .....	709
14.2.5.3	Deleting an SNMP Target Address .....	711
14.2.6	Managing SNMP Users .....	711
14.2.6.1	Viewing a List of SNMP Users .....	711
14.2.6.2	Adding an SNMP User .....	711
14.2.6.3	Deleting an SNMP User .....	713
14.2.7	Managing SNMP Security Model Mapping .....	713
14.2.7.1	Viewing a List of SNMP Security Models .....	714
14.2.7.2	Adding an SNMP Security Model .....	714
14.2.7.3	Deleting an SNMP Security Model .....	715
14.2.8	Managing SNMP Group Access .....	715
14.2.8.1	Viewing a List of SNMP Groups .....	715
14.2.8.2	Adding an SNMP Group .....	715
14.2.8.3	Deleting an SNMP Group .....	717
14.3	Managing NETCONF .....	717
14.3.1	Enabling and Configuring NETCONF Sessions .....	717
14.3.2	Viewing NETCONF Statistics .....	719
14.4	Managing IPv4 Neighbors .....	720
14.4.1	IPv4 Neighbor Concepts .....	720
14.4.2	Viewing IPv4 Neighbors .....	720
14.4.3	Clearing IPv4 Neighbors .....	721
<b>15</b>	<b>Traffic Control and Classification .....</b>	<b>723</b>
15.1	Managing Port Mirroring .....	723
15.1.1	Configuring Port Mirroring .....	723
15.1.2	Managing Egress Source Ports .....	724
15.1.2.1	Viewing a List of Egress Source Ports .....	724
15.1.2.2	Adding an Egress Source Port .....	725
15.1.2.3	Deleting an Egress Source Port .....	725
15.1.3	Managing Ingress Source Ports .....	725
15.1.3.1	Viewing a List of Ingress Source Ports .....	725
15.1.3.2	Adding an Ingress Source Port .....	725
15.1.3.3	Deleting an Ingress Source Port .....	726
15.2	Managing Traffic Control .....	726
15.2.1	Enabling and Configuring Traffic Control .....	726
15.2.2	Managing Traffic Control Interfaces .....	728
15.2.2.1	Viewing a List of Traffic Control Interfaces .....	728
15.2.2.2	Adding a Traffic Control Interface .....	728
15.2.2.3	Deleting a Traffic Control Interface .....	730
15.2.3	Managing Traffic Control Priorities .....	730
15.2.3.1	Viewing a List of Traffic Control Priorities .....	730

15.2.3.2	Adding a Traffic Control Priority .....	730
15.2.3.3	Deleting a Traffic Control Priority .....	731
15.2.4	Managing Traffic Control Classes .....	732
15.2.4.1	Viewing a List of Traffic Control Classes .....	732
15.2.4.2	Adding a Traffic Control Class .....	732
15.2.4.3	Deleting a Traffic Control Class .....	735
15.2.5	Managing Traffic Control Devices .....	735
15.2.5.1	Viewing a List of Traffic Control Devices .....	735
15.2.5.2	Adding a Traffic Control Device .....	735
15.2.5.3	Deleting a Traffic Control Device .....	736
15.2.6	Managing Traffic Control Rules .....	736
15.2.6.1	Viewing a List of Traffic Control Rules .....	737
15.2.6.2	Adding a Traffic Control Rule .....	737
15.2.6.3	Configuring QoS Marking .....	739
15.2.6.4	Deleting a Traffic Control Rule .....	742
15.2.7	Managing QoS Mapping for VLANs .....	742
15.2.7.1	Viewing a List of QoS Maps for VLANs .....	742
15.2.7.2	Adding a QoS Map .....	743
15.2.7.3	Deleting a QoS Map .....	744
15.2.8	Managing Egress Markers for QoS Maps .....	744
15.2.8.1	Viewing a List of Egress Marks .....	744
15.2.8.2	Adding an Egress Mark .....	745
15.2.8.3	Deleting an Egress Mark .....	746
15.2.9	Viewing QoS Statistics .....	746
15.3	Managing Classes of Service .....	747
15.3.1	Configuring Classes of Service .....	748
15.3.2	Managing Priority-to-CoS Mapping .....	749
15.3.2.1	Viewing a List of Priority-to-CoS Mapping Entries .....	749
15.3.2.2	Adding a Priority-to-CoS Mapping Entry .....	749
15.3.2.3	Deleting a Priority-to-CoS Mapping Entry .....	750
15.3.3	Managing DSCP-to-CoS Mapping .....	750
15.3.3.1	Viewing a List of DSCP-to-CoS Mapping Entries .....	750
15.3.3.2	Adding a DSCP-to-CoS Mapping Entry .....	750
15.3.3.3	Deleting a DSCP-to-CoS Mapping Entry .....	751
15.4	Managing NetFlow Data Export .....	751
15.4.1	Understanding NetFlow Data Export .....	752
15.4.1.1	Flow Records .....	753
15.4.2	Configuring NetFlow Data Export .....	753
15.4.3	Enabling/Disabling NetFlow .....	754
15.4.4	Setting the NetFlow Engine ID .....	754
15.4.5	Controlling the NetFlow Cache .....	754
15.4.6	Controlling Active/Inactive Flows .....	755
15.4.7	Managing NetFlow Interfaces .....	755
15.4.7.1	Viewing a List of NetFlow Interfaces .....	756
15.4.7.2	Adding a NetFlow Interface .....	756
15.4.7.3	Deleting a NetFlow Interface .....	756
15.4.8	Managing NetFlow Collectors .....	756
15.4.8.1	Viewing a List of NetFlow Collectors .....	757

15.4.8.2	Adding a NetFlow Collector .....	757
15.4.8.3	Enabling/Disabling a NetFlow Collector .....	757
15.4.8.4	Deleting a NetFlow Collector .....	758
15.4.9	Viewing the Status of NetFlow .....	758
15.4.10	Example: Exporting Flows to Multiple Collectors .....	758
15.5	Managing Port Rate Limiting .....	760
15.5.1	Understanding Port Rate Limiting .....	760
15.5.2	Configuring Port Rate Limiting .....	760
<b>16</b>	<b>Time Services .....</b>	<b>763</b>
16.1	Configuring the Time Synchronization Settings .....	763
16.2	Configuring the System Time and Date .....	764
16.3	Configuring the System Time Zone .....	764
16.4	Configuring the Local Time Settings .....	764
16.5	Enabling and Configuring the NTP Service .....	765
16.6	Viewing the NTP Service Status .....	766
16.7	Viewing the Status of Reference Clocks .....	767
16.8	Managing NTP Servers .....	768
16.8.1	Viewing a List of NTP Servers .....	768
16.8.2	Monitoring Subscribers .....	768
16.8.3	Adding an NTP Server .....	769
16.8.4	Deleting an NTP Server .....	770
16.8.5	Managing Server Keys .....	770
16.8.5.1	Viewing a List of Server Keys .....	771
16.8.5.2	Adding a Server Key .....	771
16.8.5.3	Deleting a Server Key .....	771
16.8.6	Managing Server Restrictions .....	771
16.8.6.1	Viewing a List of Server Restrictions .....	772
16.8.6.2	Adding a Server Restriction .....	772
16.8.6.3	Deleting a Server Restriction .....	773
16.9	Managing NTP Broadcast/Multicast Clients .....	773
16.9.1	Enabling and Configuring NTP Multicast Clients .....	773
16.9.2	Enabling and Configuring NTP Broadcast Clients .....	774
16.9.3	Managing NTP Broadcast/Multicast Addresses .....	774
16.9.3.1	Viewing a List of Broadcast/Multicast Addresses .....	775
16.9.3.2	Adding a Broadcast/Multicast Address .....	775
16.9.3.3	Deleting a Broadcast/Multicast Address .....	776
<b>17</b>	<b>Applications .....</b>	<b>777</b>
17.1	Viewing a List of Installed Applications .....	777
17.2	Installing an Application .....	777
17.3	Upgrading an Application .....	778
17.4	Uninstalling an Application .....	778

<b>18</b>	<b>Troubleshooting</b> .....	<b>781</b>
18.1	Management Access .....	781
18.2	Feature Keys .....	782
18.3	Ethernet Ports .....	782
18.4	Multicast Filtering .....	782
18.5	Spanning Tree .....	783
18.6	VLANs .....	785
<b>19</b>	<b>Reference</b> .....	<b>787</b>
19.1	Supported MIBs .....	787
19.2	Standard SNMP Traps .....	849
19.3	Proprietary SNMP Traps .....	851
19.4	Supported Cipher Suites .....	862

# Preface

This document describes the Web-based user interface for RUGGEDCOM ROX II v2.16 running on the RUGGEDCOM RX5000/MX5000/MX5000RE. It contains instructions and guidelines on how to use the software, as well as some general theory.

It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for use by network and system planners, system programmers, and line technicians.

---

## Note

This document is updated to match the version of RUGGEDCOM ROX II v2.16 available at the time of publication, including minor releases (e.g. 2.16.1, 2.16.2, etc.). To determine the current release of RUGGEDCOM ROX II v2.16, refer to Siemens Industrial Online Support:

- **Product Notes**

<https://support.industry.siemens.com/cs/search?search=ROX&type=ProductNote&o=0>

- **Downloads**

<https://support.industry.siemens.com/cs/search?search=ROX&type=Download&o=0>

Users can also set up a daily or weekly e-mail notification to inform of them of recent releases/updates. For more information, refer to the [Siemens Industrial Online Support \[https://support.industry.siemens.com\]](https://support.industry.siemens.com) website.

---

## Note

Some of the parameters and options described may not be available depending on variations in the device hardware. While every attempt is made to accurately describe the specific parameters and options available, this document should be used as a companion to the Help text included in the software.

---

## Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent

such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/cert>.

## Firmware/software support model

Siemens only monitors the latest firmware version for security vulnerabilities. Therefore, bug and security fixes are provided only for the latest released firmware version.

## SIMATIC NET glossary

The SIMATIC NET glossary describes special terms that may be used in this document.

The glossary is available online via Siemens Industry Online Support (SIOS) at:

<https://support.industry.siemens.com/cs/ww/en/view/50305045>

## System Requirements

Each workstation used to connect to the RUGGEDCOM ROX II Web user interface must meet the following system requirements:

- Must have one of the following Web browsers installed:
  - Microsoft Edge 86
  - Mozilla Firefox 78.0
  - Google Chrome 86
- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM RX5000/MX5000/MX5000RE.
- The ability to configure an IP address and netmask on the computer's Ethernet interface

## Accessing documentation

The latest user documentation for RUGGEDCOM ROX II v2.16 is available online at <https://support.industry.siemens.com>. To request or inquire about a user document, contact Siemens Customer Support.

## License conditions

RUGGEDCOM ROX II contains open source software. Read the license conditions for open source software carefully before using this product.

License conditions are detailed in a separate document accessible via RUGGEDCOM ROX II. To access the license conditions, log in to the RUGGEDCOM ROX II CLI and type the following command:

```
file show-license LicenseSummary.txt
```

## Registered trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens Canada Ltd.:

- RUGGEDCOM
- ROS
- RCDP
- Discovery Protocol

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

## Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit <https://www.siemens.com> or contact a Siemens customer service representative.



## Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit <https://www.siemens.com> or contact a Siemens Sales representative.

## Customer support

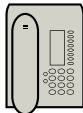
Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

### Online



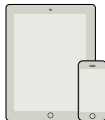
Visit <http://www.siemens.com/automation/support-request> to submit a Support Request (SR) or check on the status of an existing SR.

### Telephone



Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit [https://w3.siemens.com/aspa\\_app/?lang=en](https://w3.siemens.com/aspa_app/?lang=en).

### Mobile app



Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

## Contacting Siemens

<b>Address</b>	Siemens Canada Ltd. Digital Industries
----------------	---

	Process Automation 300 Applewood Crescent Concord, Ontario Canada, L4K 5C7
<b>Telephone</b>	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288 Fax: +1 905 856 1995
<b>E-Mail</b>	<a href="mailto:info.ruggedcom@siemens.com">info.ruggedcom@siemens.com</a>
<b>Web</b>	<a href="https://www.siemens.com">https://www.siemens.com</a>



# Introduction

Welcome to the **RUGGEDCOM ROX II (Rugged Operating System on Linux®) v2.16 Configuration Manual**. This document details how to configure the RX5000 via the RUGGEDCOM ROX II Web interface. RUGGEDCOM ROX II also features a Command Line Interface (CLI), which is described in a separate Configuration Manual.

## NOTICE

This Configuration Manual describes all features of RUGGEDCOM ROX II, but some features can only be configured through the Command Line Interface (CLI). This is indicated throughout the Configuration Manual where applicable.

This document is specific to the following device platforms:

- RUGGEDCOM RX5000
- RUGGEDCOM MX5000
- RUGGEDCOM MX5000RE

## 1.1 Features and Benefits

Feature support in RUGGEDCOM ROX II is driven by feature keys that unlock feature levels. For more information about feature keys, refer to "Feature Keys" (Page 6).

The following describes the many features available in RUGGEDCOM ROX II and their benefits:

- **Cyber Security**

Cyber security is an urgent issue in many industries where advanced automation and communications networks play a crucial role in mission critical applications and where high reliability is of paramount importance. Key RUGGEDCOM ROX II features that address security issues at the local area network level include:

<b>Passwords</b>	Multi-level user passwords secures against unauthorized configuration
<b>SSH/SSL</b>	Extends capability of password protection to add encryption of passwords and data as they cross the network
<b>Enable/Disable Ports</b>	Capability to disable ports so that traffic cannot pass
<b>IEEE 802.1Q VLAN</b>	Provides the ability to logically segregate traffic between predefined ports on switches
<b>SNMPv3</b>	Encrypted authentication and access security
<b>HTTPS</b>	For secure access to the Web interface
<b>Firewall</b>	Integrated stateful firewall provides protected network zones
<b>VPN/IPSEC</b>	Allows creation of secure encrypted and authenticated tunnels

<b>IEEE 802.1X</b>	Offers network access control through port-based authentication and authorization
<b>RADIUS/TACACS+</b>	Provides UDP- or TLS-based user authentication via remote authentication servers

- SSL/TLS Ciphers**  
RUGGEDCOM ROX II uses TLS v1.0, TLS v1.2, and SSL/TLS cipher suites to secure all data transfers. Grade 4 cipher suites and above are enabled by default.  
For a list of support ciphers and algorithms, refer to "Supported Cipher Suites" (Page 862).
- Enhanced Rapid Spanning Tree Protocol (eRSTP)<sup>™</sup>**  
Siemens's eRSTP allows the creation of fault-tolerant ring and mesh Ethernet networks that incorporate redundant links that are *pruned* to prevent loops. eRSTP implements both STP and RSTP to promote interoperability with commercial switches, unlike other proprietary *ring* solutions. The fast root failover feature of eRSTP provides quick network convergence in case of an RSTP root bridge failure in a mesh topology.
- Quality of Service (IEEE 802.1p)**  
Some networking applications such as real-time control or VoIP (Voice over IP) require predictable arrival times for Ethernet frames. Switches can introduce latency in times of heavy network traffic due to the internal queues that buffer frames and then transmit on a first come first serve basis. RUGGEDCOM ROX II supports *Class of Service*, which allows time critical traffic to jump to the front of the queue, thus minimizing latency and reducing *jitter* to allow such demanding applications to operate correctly. RUGGEDCOM ROX II allows priority classification by port, tags, MAC address, and IP Type of Service (ToS). A configurable *weighted fair queuing* algorithm controls how frames are emptied from the queues.
- VLAN (IEEE 802.1Q)**  
Virtual Local Area Networks (VLAN) allow the segregation of a physical network into separate logical networks with independent broadcast domains. A measure of security is provided since hosts can only access other hosts on the same VLAN and traffic storms are isolated. RUGGEDCOM ROX II supports 802.1Q tagged Ethernet frames and VLAN trunks. Port based classification allows legacy devices to be assigned to the correct VLAN. GVRP support is also provided to simplify the configuration of the switches on the VLAN.
- Remote Monitoring and Configuration with SINEC NMS**  
SINEC NMS is Siemens's Network Management System software for the discovery, monitoring and management of RUGGEDCOM products and other IP enabled devices on a network. This highly configurable, full-featured product records and reports on the availability and performance of network components and services. Device, network and service failures are quickly detected and reported to reduce downtime.  
  
SINEC NMS is especially suited for remotely monitoring and configuring Siemens routers, switches, serial servers and WiMAX wireless network equipment. For more information, contact a Siemens Sales representative.

- **Device Management with SINEC PNI**

RUGGEDCOM ROX II devices are compatible with SINEC PNI (Primary Network Initialization), a tool for commissioning Siemens RUGGEDCOM routers and switches. Use SINEC PNI to quickly add one or more devices to a network.

Some of the features offered by SINEC PNI include:

- Bulk device management
- Change, load, or download device configurations
- Upgrade or downgrade firmware
- IP address assignment

- **Simple Network Management Protocol (SNMP)**

SNMP provides a standardized method, for network management stations, to interrogate devices from different vendors. Supported SNMP versions include v1, v2c and v3. SNMPv3 in particular provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions. Numerous standard MIBs (Management Information Base) allow for easy integration with any Network Management System (NMS). A feature of SNMP supported by RUGGEDCOM ROX II is the ability to generate *traps* upon system events. SINEC NMS, the Siemens management solution, can record traps from multiple devices providing a powerful network troubleshooting tool. It also provides a graphical visualization of the network and is fully integrated with all Siemens products.

- **NETCONF Configuration Interface**

The NETCONF configuration interface allows administrators to set device parameters and receive device updates through the use of XML-based commands. This standard, supported by multiple vendors, makes it possible to greatly simplify the task of network management.

For more information about how to use NETCONF to configure RUGGEDCOM ROX II, refer to the "[RUGGEDCOM ROX II NETCONF Reference Guide \[https://support.industry.siemens.com/cs/us/en/view/109737085\]](https://support.industry.siemens.com/cs/us/en/view/109737085)".

- **NTP (Network Time Protocol)**

NTP automatically synchronizes the internal clock of all RUGGEDCOM ROX II devices on the network. This allows for correlation of time stamped events for troubleshooting.

- **Port Rate Limiting**

RUGGEDCOM ROX II supports configurable rate limiting per port to limit unicast and multicast traffic. This can be essential to managing precious network bandwidth for service providers. It also provides edge security for Denial of Service (DoS) attacks.

- **Broadcast Storm Filtering**

Broadcast storms wreak havoc on a network and can cause attached devices to malfunction. This could be disastrous on a network with mission critical equipment. RUGGEDCOM ROX II limits this by filtering broadcast frames with a user-defined threshold.

- **Port Mirroring**  
RUGGEDCOM ROX II can be configured to duplicate all traffic on one port to a designated mirror port. When combined with a network analyzer, this can be a powerful troubleshooting tool.
- **Port Configuration and Status**  
RUGGEDCOM ROX II allows individual ports to be *hard* configured for speed, duplex, auto-negotiation, flow control and more. This allows proper connection with devices that do not negotiate or have unusual settings. Detailed status of ports with alarm and SNMP trap on link problems aid greatly in system troubleshooting.
- **Port Statistics and RMON (Remote Monitoring)**  
RUGGEDCOM ROX II provides continuously updating statistics per port that provide both ingress and egress packet and byte counters, as well as detailed error figures.  
  
Also provided is full support for RMON statistics. RMON allows for very sophisticated data collection, analysis and detection of traffic patterns.
- **Event Logging and Alarms**  
RUGGEDCOM ROX II records all significant events to a non-volatile system log allowing forensic troubleshooting. Events include link failure and recovery, unauthorized access, broadcast storm detection, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay is de-energized during the presence of critical alarms, allowing an external controller to react if desired.
- **HTML Web Browser User Interface**  
RUGGEDCOM ROX II provides a simple, intuitive user interface for configuration and monitoring via a standard graphical Web browser or via a standard telecom user interface. All system parameters include detailed online Help to facilitate setup and configuration. RUGGEDCOM ROX II presents a common look and feel and standardized configuration process, allowing easy migration to other RUGGEDCOM managed products.
- **Command Line Interface (CLI)**  
A command line interface used in conjunction with remote shell to automate data retrieval, configuration updates, and firmware upgrades. A powerful Telecom Standard style Command Line Interface (CLI) allows expert users the ability to selectively retrieve or manipulate any parameters the device has to offer.
- **Link Backup**  
Link backup provides an easily configured means of raising a backup link upon the failure of a designated main link. The main and backup links can be Ethernet, Cellular, T1/E1, DDS or T3. The feature can back up to multiple remote locations, managing multiple main: backup link relationships. The feature can also back up a permanent high speed WAN link to a permanent low speed WAN link and can be used to migrate the default route from the main to the backup link.

- **OSPF (Open Shortest Path First)**

OSPF is a routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on link states between nodes and several quality parameters. OSPF is an Interior Gateway Protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol, meaning the best route is determined by the type and speed of the inter-router links, not by how many router hops they are away from each other (as in distance-vector routing protocols such as RIP).
- **BGP (Border Gateway Protocol)**

BGPv4 is a path-vector routing protocol where routing decisions are made based on the policies or rules laid out by the network administrator. It is typically used where networks are multi-homed between multiple Internet Service Providers, or in very large internal networks where internal gateway protocols do not scale sufficiently.
- **RIP (Routing Information Protocol)**

RIP version 1 and version 2 are distance-vector routing protocols that limit the number of router hops to 15 when determining the best routing path. This protocol is typically used on small, self-contained networks, as any router beyond 15 hops is considered unreachable.
- **IS-IS (Intermediate System - Intermediate System)**

IS-IS is one of a suite of routing protocols tasked with sharing routing information between routers. The job of the router is to enable the efficient movement of data over sometimes complex networks. Routing protocols are designed to share routing information across these networks and use sophisticated algorithms to decide the shortest route for the information to travel from point A to point B. One of the first link-state routing protocols was IS-IS developed in 1985 and adopted by the ISO in 1998 (ISO/IEC 10589:2002). It was later republished as an IETF standard ([RFC 1142 \[http://tools.ietf.org/html/rfc1142\]](http://tools.ietf.org/html/rfc1142)).
- **Brute Force Attack Prevention**

Protection against Brute Force Attacks (BFAs) is standard in RUGGEDCOM ROX II. If an external host fails to log in to the CLI, NETCONF or Web interfaces after a fixed number of attempts, the host's IP address will be blocked for a period of time. That period of time will increase if the host continues to fail on subsequent attempts.
- **USB Mass Storage**

Use a removable USB Mass Storage drive to manage important files and configure RUGGEDCOM ROX II.

  - Upgrade/Downgrade Firmware – Use the USB Mass Storage drive as a portable repository for new or legacy versions of the RUGGEDCOM ROX II firmware.
  - Backup Files – Configure RUGGEDCOM ROX II to backup important information to the USB Mass Storage drive, such as rollbacks, log files, feature keys and configuration files.
  - Share Files – Quickly configure or upgrade other RUGGEDCOM RX5000 devices by copying files using the same microSD/microSDHC Flash drive.



 **NOTICE**

Do not remove the USB Mass Storage drive during a file transfer.

---

**Note**

Only USB Mass Storage drives with one partition are supported.

---

- **Hot Swapping Modules and SFP Transceivers**

Power Modules (PM), Line Modules (LM) and individual SFP transceivers can be safely replaced with modules/transceivers of exactly the same type while the device is running, with minimal disruption to the network. The device only needs to be restarted after swapping a module/transceiver with a different type, such as an Ethernet module with a serial module, or a 1000Base-X transceiver with a 100Base-FX transceiver.

Following a hot swap, the new module/transceiver will be automatically configured to operate in the same operational state as the previous module/transceiver.

---

**Note**

A reboot is required if a module/transceiver is installed in a slot/socket that was empty when the device was started.

---

**Note**

Hot swapping is not available for Switch Modules (SM). When an SM is removed during operation, all other LMs are disabled. Therefore, the device must always be restarted following the installation of a new SM module.

---

- **Jumbo Frames**

In an Ethernet data network, the term **jumbo frames** designates non-standard and oversize messages. The standard size is defined as 1518 bytes by the IEEE 802.3 standard. Messages that are longer than 1518 bytes are called jumbo frames.

The RUGGEDCOM RX5000 series of devices support frames of up to 9216 bytes on Gigabit Ethernet ports only.

## 1.2 Feature Keys

Feature keys add features to an existing installation of RUGGEDCOM ROX II. They can be purchased and installed at any time.

By default, each device is ordered with a base feature key, which is permanently installed on the device. Additional feature keys can be installed via a remote host or directly using removable media (e.g. compact flash card or USB Mass Storage drive).

**Note**

Feature keys are serial number specific and cannot be transferred between devices.

Feature keys include the following features:

Feature	Feature Key				
	Layer 2 Standard Edition (L2SE)	L3SEL3HW	L3SEL2HW	L3SECL3HW	L3SECL2HW
VLANs (802.1Q)	•	•	•	•	•
QoS (802.1p)	•	•	•	•	•
MSTP (802.1Q-2005)	•	•	•	•	•
RSTP	•	•	•	•	•
eRSTP™	•	•	•	•	•
NTP	•	•	•	•	•
L2TPv2 and L2TPv3	•	•	•	•	•
Port Rate Limiting	•	•	•	•	•
Broadcast Storm Filtering	•	•	•	•	•
Port Mirroring	•	•	•	•	•
SNMP v1/v2/v3	•	•	•	•	•
RMON	•	•	•	•	•
CLI	•	•	•	•	•
HTML User Interface	•	•	•	•	•
MPLS		•	•	•	•
DHCP		•	•	•	•
VRRPv2 and VRRPv3		•	•	•	•
PIM-SM		•	•	•	•
Firewall		•	•	•	•
OSPF		•	•	•	•
BGP		•	•	•	•
RIP v1/v2		•	•	•	•
IS-IS		•	•	•	•
Traffic Prioritization		•	•	•	•
VPN				•	•
IPSec				•	•
Hardware Accelerated Layer 3 Switching		•		•	

For information about installing and viewing the contents of feature keys, refer to "Managing Feature Keys" (Page 60).

## 1.3 Security Recommendations

To prevent unauthorized access to the device, note the following security recommendations:

### Authentication

**⚠ NOTICE****Accessibility hazard – risk of data loss**

Do not misplace the passwords for the device. If both the maintenance and boot passwords are misplaced, the device must be returned to Siemens Canada Ltd. for repair. This service is not covered under warranty. Depending on the action that must be taken to regain access to the device, data may be lost.

- Replace the default passwords for the admin and maintenance mode accounts before the device is deployed.
- Use strong passwords. Avoid weak passwords (e.g. *password1*, *123456789*, *abcdefgh*) or repeated characters (e.g. *abcabc*). For more information about creating strong passwords, refer to the password requirements in "Managing Passwords and Passphrases" (Page 118).  
This recommendation also applies to symmetric passwords/keys configured on the device.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Do not re-use passwords across different user names and systems, or after they expire.
- Record passwords in a safe, secure, off-line location for future retrieval should they be misplaced.
- When RADIUS or TACACS+ are utilized for user authentication, make sure all communications are within the security perimeter or protected by a secure channel.
- TACACS+ uses the MD5 algorithm for key encryption. Make sure to follow the security recommendations outlined in this document and configure the environment according to *defense in depth* best practices.
- PAP (Password Authentication Protocol) is not considered a secure protocol and, where possible, should be used in a protected network environment.
- Use the L2TP protocol in conjunction with IPsec to secure the L2TP tunnel.
- It is recommended to use shared keys for authentication between routing neighbors to help prevent unauthenticated routing updates.
- Be aware of any link layer protocols that do not provide any inherent authentication between endpoints, such as ARP in IPv4, neighbor discovery/DAD in IPv6, and Wi-Fi in wireless networks. A malicious entity could exploit weaknesses in these protocols to attack hosts, switches, and routers connected to the Layer 2 network, for example, by poisoning the ARP caches of systems

within the subnet and subsequently intercepting traffic. Appropriate safeguards against non-secure Layer 2 protocols, such as securing physical access to the local network and using secure higher layer protocols, should be taken to prevent unauthorized access to the network.

- Change passwords regularly and often.

### Physical/Remote Access

- It is highly recommended to enable Brute Force Attack (BFA) protection to prevent a third-party from obtaining unauthorized access to the device. For more information, refer to "Enabling/Disabling Brute Force Attack Protection" (Page 128).
- SSH and SSL keys are accessible to the root user. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with *throwaway* keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Replace all default and auto-generated SSL certificates with certificates and keys signed by a trusted Certificate Authority (CA). Default and auto-generated certificates are self-signed by RUGGEDCOM ROX II.
- Restrict physical access to the device to only trusted personnel. A malicious user in possession of the device's removable media could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the media.
- Passwords/passphrases for service mode and maintenance mode should only be known to a single trusted user. These modes should have restricted access to protect the confidentiality and integrity of the device.

When commissioning a unit, make sure the maintenance mode password is changed from its default setting.

- Control access to the serial console to the same degree as any physical access to the device. Access to the serial console allows for potential access to BIST and service mode, which includes tools that may be used to gain complete access to the device.
- Mirror ports allow bidirectional traffic (i.e. the device will not block incoming traffic to the mirror port or ports). This can lead to traffic being forwarded to unintended ports. For increased security, configure ingress filtering to control traffic flow when port mirroring is enabled. For more information about enabling port mirroring, refer to "Configuring Port Mirroring" (Page 723). For more information about enabling ingress filtering, refer to "Enabling/Disabling Ingress Filtering" (Page 319).
- For increased security, enable ingress filtering on all ports by default. For more information about enabling ingress filtering, refer to "Enabling/Disabling Ingress Filtering" (Page 319).

- When using SNMP (Simple Network Management Protocol):
  - Limit the number of IP addresses that can connect to the device.
  - Configure SNMP to raise any available traps on the occurrence of a security event.
  - Make sure the default community strings are changed to unique values.
  - Ensure that when enabling SNMP, SNMPv1 and SNMPv2c are disabled if not required.
  - Consider using SNMPv3 for additional security.

For more information about SNMP, refer to "Managing SNMP" (Page 703).

- When using RUGGEDCOM ROX II as a client to securely connect to a server (such as, in the case of a secure upgrade or a secure syslog transfer), make sure the server side is configured with strong ciphers and protocols.
- Limit the number of simultaneous Web Server, CLI, SFTP and NETCONF sessions allowed.
- If a firewall is required, configure and start the firewall before connecting the device to a public network. Make sure the firewall is configured to accept connections from a specific domain and deny all other traffic. For more information, refer to "Managing Firewalls" (Page 195).
- Serial protocols are deactivated by default in RUGGEDCOM ROX II. Some serial protocols lack the necessary protections to integrity and confidentiality inherently available to TCP/IP based protocols. Given the critical infrastructure of the systems that are often controlled by serial protocols it is imperative that these protocols be protected by any means available. Examples of protection measures include using MicroLok encapsulated with TCP/IP and encrypting with IPsec wherever possible. If IPsec is not available for a given network segment, make sure to configure the environment according to defense-in-depth best practices.
- To ensure the permanence of a device's audit trail, configure the device to forward all logs using TLS to a hardened remote syslog server. For more information, refer to "Managing Logs" (Page 64).
- Configuration files are provided in either NETCONF or CLI format for ease of use. Make sure configuration files are properly protected when they exist outside of the device. For instance, digitally sign and encrypt the files, store them in a secure place, and transfer configuration files via secure communication channels only.
- It is highly recommended that critical applications and access to management services be limited to private networks. Connecting a RUGGEDCOM ROX II device to the Internet is possible. However, the utmost care should be taken to protect the device and the network behind it using secure means such as firewall and IPsec. For more information about configuring firewalls and IPsec, refer to "Managing Firewalls" (Page 195) and "Managing IPsec Tunnels" (Page 415).
- The safekeeping and management of the certificates and keys is the responsibility of the device owner. Use RSA key sizes of 2048 bits in length to

employ standard cryptographic strength. Before returning the device to Siemens Canada Ltd. for repair, replace the current certificates and keys with temporary *throwaway* certificates and keys that can be destroyed upon the device's return.

- Be aware of any non-secure protocols enabled on the device. While some protocols, such as HTTPS, SSH and 802.1x, are secure, others, such as SNMPv1/v2c and RSTP were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Prevent access to external, untrusted Web pages while accessing the device via a Web browser. This can assist in preventing potential security threats, such as session hijacking.
- Make sure the device is fully decommissioned before taking the device out of service. For more information, refer to "Decommissioning the Device" (Page 59).
- Configure port security features on access ports to prevent an unauthorized third-party from physically connecting to the device. For more information, refer to "Configuring Port Security" (Page 139).

## Hardware/Software

### NOTICE

#### Configuration hazard – risk of data corruption

Maintenance mode is provided for troubleshooting purposes and should only be used by Siemens Canada Ltd. technicians. As such, this mode is not fully documented. Misuse of this maintenance mode commands can corrupt the operational state of the device and render it inaccessible.

- Make sure the latest firmware version is installed, including the latest security-related patches. For the latest information on security patches for Siemens products, visit the [Industrial Security website \[https://new.siemens.com/global/en/products/services/cert.html\]](https://new.siemens.com/global/en/products/services/cert.html). Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the [ProductCERT Security Advisories website \[https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications\]](https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications), or by following @ProductCert on Twitter.
- Select services are enabled by default in RUGGEDCOM ROX II. It is recommended to only enable the minimum services that are required. For more information about available services, "Available Services by Port" (Page 12).
- Physical interfaces that are not being used should be disabled. Unused physical ports could potentially be used to gain access to the network behind the device.
- Use the latest Web browser version compatible with RUGGEDCOM ROX II to make sure the most secure ciphers available are employed. Additionally, 1/n-1 record splitting is enabled in the latest Web browser versions of Mozilla Firefox, Google Chrome and Microsoft Edge, and mitigates against attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (e.g. BEAST).

- For optimal security, use SNMPv3 whenever possible and apply strong passwords.
- Validate the integrity of the running firmware as often as required. This task can be automated by scheduling a job to repeat every day or week. Firmware integrity can also be checked automatically at start-up.

If an unauthorized/unexpected modification is detected, inspect the syslog for messages related to firmware integrity to identify which programs and/or files may have been compromised. If remote system logging is configured, this task can also be automated using scripts to identify key log messages.

For more information about checking the firmware integrity, refer to "Monitoring Firmware Integrity" (Page 92).

## Policy

- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with the device for further security recommendations.

## 1.4 Available Services by Port

The following table lists the services available by the device, including the following information:

- **Services**  
The service supported by the device
- **Port Number**  
The port number associated with the service
- **Port Default**  
The default state of the port (i.e. open or closed)
- **Authenticated Access**  
Denotes whether the ports/services require authentication for access

### Note

All listed ports can be configured as open or closed in RUGGEDCOM ROX II.

Services	Port Number	Port Default	Authenticated Access
SSH	TCP/22	Open	Yes
SSH (Service Mode)	TCP/222	Closed	Yes
NETCONF	TCP/830	Open	Yes
SFTP	TCP/2222	Closed	Yes
HTTP	TCP/80	Open	N/A
NTP	UDP/123	Closed	No
SNMP	UDP/161	Closed	Yes

Services	Port Number	Port Default	Authenticated Access
HTTPS	TCP/443	Open	Yes
TCP Modbus	TCP/502	Closed	No
IPSec IKE	UDP/500	Closed	Yes
IPSec NAT-T	UDP/4500	Closed	Yes
DNPv3	TCP/20000 and UDP/20000	Closed	No
RawSocket	UDP/TCP 1024-65535	Closed	No
DHCP Agent	UDP/67	Closed	No
DHCP Server	UDP/67 listening, 68 responding	Closed	No
RADIUS	UDP/1812 to send, opens random port to listen	Closed	Yes
TACACS+	TCP/49 to send, opens random port to listen	Closed	Yes
L2TP	Random Port	Closed	Yes
BGP	TCP/179	Closed	No
RIP	UDP/520	Closed	No
MPLS-Ping	UDP/3503	Closed	No
LDP	TCP/646 and UDP/646	Closed	No
L2TPv3	UDP/1701	Closed	No

## 1.5 User Permissions

The following table lists the operation, configuration, and action commands permitted to the administrator, operator, and guest users.

Types of user access:

- **Create (C)** – can create and remove optional parameters
- **Execute (E)** – can run an action or command
- **No** – no access
- **Read (R)** – read access
- **Update (U)** – can modify existing parameter

Commands/Paths Permitted	Access		
	Administrator	Operator	Guest
config private   exclusive   no-confirm	Allowed	Allowed	No
/admin/software-upgrade	R/U	R	No
/admin/rox-imaging	R/U	R	No
/admin/authentication	R/U	No	No
/admin/authentication/password-complexity	R/U	No	No
/admin/logging	C/R/U	No	No
/admin/alarms (status)	R	R	No <sup>a</sup>
/admin/alarms-config/	R/U	R/U	No <sup>b</sup>
/admin/users	C/R/U	No	No



Commands/Paths Permitted	Access		
	Administrator	Operator	Guest
/admin/users/userid	R/U	R/U <sup>c</sup>	No
/admin/cli	R/U	R/U	No
/admin/snmp	C/R/U	No	No
/admin/netconf	R/U	No	No
/admin/dns	C/R/U	No	No
/admin/webui	R/U	R/U	No
/admin/scheduler	C/R/U	No	No
/admin/contact	R/U	No	No
/admin/hostname	R/U	No	No
/admin/location	R/U	No	No
/admin/session-limits	R/U	No	No
/admin/session-security	R/U	No	No
/admin/sftp	R/U	No	No
/admin/time (status)	R	R	No
/admin/switch-config (status)	R/U	R	No
/admin/system	R/U	No	No
/admin/system-name	R/U	No	No
/admin/timezone	R/U	No	No
/admin/clear-all-alarms (action)	E	C/R/U	No
/admin/backup-files (action)	E/R/U	No	No
/admin/delete-all-ssh-known-hosts (action)	E	No	No
/admin/delete-autoload-configuration-from-removable (action)	E	No	No
/admin/delete-logs (action)	E	No	No
/admin/delete-ssh-known-host (action)	E	No	No
/admin/full-configuration-load (action)	E/U	No	No
/admin/full-configuration-save (action)	E/U	No	No
/admin/install-files (action)	E/U	No	No
/admin/reboot (action)	E	E	No
/admin/restore-factory-defaults (action)	E/U	No	No
/admin/save-configuration-to-removable (action)	E/U	No	No
/admin/set-system-clock (action)	E/U	No	No
/admin/shutdown (action)	E	E	No
/apps	C/R/U	C/R/U	R
/chassis/part-list	R/U	R	R
/chassis/fixed-modules	C/R/U	No	R
/chassis/line-module-list	R/U	R	R
/chassis/line-modules/line-module	R/U	No	R
/interfaces	R	R	R
/interface	C/R/U	R/U	R

Commands/Paths Permitted	Access		
	Administrator	Operator	Guest
/routing	C/R/U	C/R/U	R
/routing/dynamic/ospf/interface	C/R/U	C/R/U	R
/routing/dynamic/rip/interface	C/R/U	C/R/U	R
/routing/multicast/dynamic/pim-sm/interface	C/R/U	C/R/U	R
/routing/dynamic/isis/interface	C/R/U	C/R/U	R
/security/firewall	C/R/U	C/R/U	R
/security/crypto	C/R/U	R	R
/security/crypto/private-key	C/R/U	No	No
/services	C/R/U	C/R/U	R
/services/time/ntp/key/	C/R/U	No	No
/tunnel/ipsec	C/R/U	No	No
/tunnel/l2tunneld	C/R/U	C/R/U	R
/ip	C/R/U	C/R/U	R
/mpls	C/R/U	C/R/U	R
/mpls/interface-mpls	C/R/U	C/R/U	R
/mpls/ldp/interface-ldp	C/R/U	C/R/U	R
/switch	C/R/U	C/R/U	R
/switch/vlans/all-vlans	C/R/U	C/R/U	R
/switch/port-security	R/U	No	No
/qos	C/R/U	C/R/U	R
/global	C/R/U	No	No
hints	E	E	E
monitor	E	E	No
mpls-ping	E	E	No
mpls-traceroute	E	E	No
ping	E	E	No
ping6	E	E	No
reportstats	E	E	No
ssh	E	E	No
tcpdump	E	E	No
telnet	E	E	No
traceroute	E	E	No
traceroute6	E	E	No
traceserial	E	E	No
wizard	E	No	No

<sup>a</sup> Only administrator and operator profiles can clear and acknowledge alarms or see the status of active alarms.

<sup>b</sup> Only administrator and operator profiles can create and delete alarm lists.

<sup>c</sup> Operator profiles can only change their own password and cannot create users.

## 1.6 Removable Memory

The RUGGEDCOM RX5000 features a user-accessible memory slot that supports a USB Mass Storage device. The drive can be used to manage configuration, firmware and other files on the device or a fleet of devices.

- Upgrade/Downgrade Firmware – Use the USB Mass Storage device as a portable repository for new or legacy versions of the RUGGEDCOM ROX II firmware.
- Backup Files – Configure RUGGEDCOM ROX II to backup important information to the USB Mass Storage device, such as rollbacks, log files, feature keys and configuration files.
- Share Files – Quickly configure or upgrade other RUGGEDCOM RX5000/MX5000/MX5000RE devices by copying files using the same USB Mass Storage device.

### NOTICE

Do not remove the USB Mass Storage device during a file transfer.

### Note

Only one partition is supported on the USB Mass Storage device.

For information about how to insert or remove the USB Mass Storage device, refer to the "Installation Manual" for the RUGGEDCOM RX5000/MX5000/MX5000RE.

For CLI commands used to manage the USB Mass Storage device, refer to the "RUGGEDCOM ROX II v2.16 CLI User Manual".

## 1.7 Logged Events

RUGGEDCOM ROX II logs all events locally and forwards them automatically to a syslog server if remote logging is enabled. This section defines events and lists the built-in syslog messages generated when specific events occur.

### Note

For information about enabling remote system logging, refer to "Configuring Secure Remote Syslog" (Page 66).

### 1.7.1 Structure of a Syslog Event

A syslog event is defined by the following elements:

Element	Description
Date	The date when the event was received/logged in the syslog server.
Time	The time when the event was received/logged in the System server.
Hostname	The name of the device that sent the event.
Facility <sup>a</sup>	The source of the event. Options include: <ul style="list-style-type: none"> <li>• AUTH</li> </ul>

Element	Description
	<ul style="list-style-type: none"> <li>AUTHPRIV</li> <li>DAEMON</li> <li>USER</li> </ul>
Severity <sup>a</sup>	The severity level associated with the event. Options include: <ul style="list-style-type: none"> <li>INFO</li> <li>NOTICE</li> <li>AUTH</li> <li>AUTHPRIV</li> <li>ERR</li> <li>CRITICAL</li> <li>EMERGENCY</li> </ul>
Message Text	Information about the event.

<sup>a</sup> Text defined in the SNMP Manager.

## 1.7.2 Syslog Event Types

Two types of syslog events are defined.

Event Type	Description
Event	Events are <i>authorized</i> activities that can be expected to occur during routine use.
Alarm	Alarms are activities that may indicate <i>unauthorized</i> activity.

Events of either type are stored locally on the device and transmitted automatically to the syslog server when they occur.

## 1.7.3 Logged Security Events

The following are security-related event messages that may be generated by RUGGEDCOM ROX II.

- SE\_LOCAL\_SUCCESSFUL\_LOGON**

Event Message	Facility	Severity	Event Type	Log
ruggedcom confd[ <i>{pid}</i> ]: audit user: <i>{user}</i> / <i>{user id}</i> assigned to groups: <i>{role}</i>	LOG_AUTHPRIV	Info	Event	Auth.log
ruggedcom rmfmgr[ <i>{pid}</i> ]: username: <i>{user name}</i> usid: <i>{user id}</i> started <i>{context}</i> session from ip:127.0.0.1 source-port: <i>{src port}</i> through <i>{local interface}</i> protocol	LOG_AUTH	Notice	Event	Auth.log

- **SE\_LOCAL\_UNSUCCESSFUL\_LOGON (Invalid Username)**

Event Message	Facility	Severity	Event Type	Log
audit user: {user name}/0 no such local user	LOG_AUTHPRIV	Info	Event	Auth.log
login failed, reason='No such local user', user='{username}', context='{context}', proto='{local interface}', user ipaddr='127.0.0.1'	LOG_AUTHPRIV	Error	Event	Auth.log

- **SE\_LOCAL\_UNSUCCESSFUL\_LOGON (Invalid Password)**

Event Message	Facility	Severity	Event Type	Log
audit user: {username}/0 Provided bad password	LOG_AUTHPRIV	Info	Event	Auth.log
login failed, reason='Bad password', user='{username}', context='{context}', proto='{protocol}', user ipaddr='127.0.0.1'	LOG_AUTHPRIV	Error	Event	Auth.log

- **SE\_NETWORK\_SUCCESSFUL\_LOGON**

Event Message	Facility	Severity	Event Type	Log
audit user: {username}/0 logged in over {protocol} from {source ip-address} with authmeth: {authentication-method}	LOG_AUTHPRIV	Info	Event	Auth.log
audit user: admin/{user id} assigned to groups: {role}	LOG_AUTHPRIV	Info	Event	Auth.log
username:{username} usid: {user id} started {session-type} session from ip: {source ip-address} source-port:{source port} through {protocol} protocol	LOG_AUTH	Notice	Event	Auth.log

- **SE\_NETWORK\_UNSUCCESSFUL\_LOGON (Invalid Username)**

Event Message	Facility	Severity	Event Type	Log
audit user: {user name}/0 no such local user	LOG_AUTHPRIV	Info	Event	Auth.log
login failed, reason='No such local user', user='{username}', context='{session-type}', proto='{protocol}', user ipaddr='{source ip-address}'	LOG_AUTHPRIV	Error	Event	Auth.log
audit user: {username}/0 Failed to login over {protocol}: No such local user	LOG_AUTHPRIV	Info	Event	Auth.log

- **SE\_NETWORK\_UNSUCCESSFUL\_LOGON (Invalid Password)**

Event Message	Facility	Severity	Event Type	Log
audit user: {username}/0 Provided bad password	LOG_AUTHPRIV	Info	Event	Auth.log
login failed, reason='Bad password', user='{username}', context='{session-type}', proto='{protocol}', user ipaddr='{source ip-address}'	LOG_AUTHPRIV	Error	Event	Auth.log
audit user: {username}/0 Failed to login over {protocol}: Bad password	LOG_AUTHPRIV	Info	Event	Auth.log

- **SE\_LOGOFF (Local)**

Event Message	Facility	Severity	Event Type	Log
username:{user name} userid:{user id} stopped {session-type} session from ip:127.0.0.1	LOG_AUTH	Notice	Event	Auth.log

- **SE\_LOGOFF(Network)**

Event Message	Facility	Severity	Event Type	Log
username:{user name} userid: {user id} stopped {context} session from ip:{source ip- address}	LOG_AUTH	Notice	Event	Auth.log
audit user: {user name}/0 Logged out {protocol} <local> user	LOG_AUTHPRIV	Info	Event	Auth.log

- **SE\_ACCESS\_PWD\_ENABLED**

Event Message	Facility	Severity	Event Type	Log
Enabling Brute Force Attack Protection	LOG_USER	Error	Event	Syslog

- **SE\_ACCESS\_PWD\_DISABLED**

Event Message	Facility	Severity	Event Type	Log
Brute Force Attack protection not enabled	LOG_USER	Error	Alarm	Syslog

- **SE\_ACCESS\_PWD\_CHANGED**

Event Message	Facility	Severity	Event Type	Log
audit user: {User Group}/ {User ID} WebUI action '/ rmf_admin:admin/users/ userid["{Target User}"/set- password'	LOG_DAEMON	Info	Event	Auth.log

- **SE\_ACCESS\_GRANTED**

Event Message	Facility	Severity	Event Type	Log
audit user: {Username}/0 logged in through Web UI from {IP Address}	LOG_DAEMON	Info	Event	Auth.log
audit user: {Username}/{User ID} assigned to groups: {User Group}	LOG_DAEMON	Info	Event	Auth.log
username:{Username} usid: {User ID} started {Context} session from ip:{IP Address} source-port:{Port} through {Protocol} protocol	LOG_AUTH	Notice	Event	Auth.log

- **SE\_ACCESS\_DENIED**

Event Message	Facility	Severity	Event Type	Log
audit user: {Username}/0 Provided Invalid Password	LOG_DAEMON	Info	Alarm	Auth.log
login failed, user:'{username}', reason='{reason}', user ipaddr='{IP Address}', context='{context}', proto='{protocol}'	LOG_AUTHPRIV	Error	Alarm	Auth.log

- **SE\_ACCOUNT\_LOCKED\_TEMP**

Event Message	Facility	Severity	Event Type	Log
ALARM: BFA from IP {IP Address} is blocked -> {Event Time}	LOG_DAEMON	Emergency	Alarm	Syslog
{Function}: detect BFA from {IP Address}, raise alarm	LOG_DAEMON	Verbose	Alarm	Syslog
{Function}: alarm asserted id={Event ID}	LOG_DAEMON	Verbose	Alarm	Syslog

- **SE\_ACCOUNT\_LOCKED\_TEMP (Freed)**

Event Message	Facility	Severity	Event Type	Log
{Function}: deassert BFA alarm ip={IP address}	LOG_DAEMON	Verbose	Event	Syslog

- **SE\_AUDIT\_LOG\_CLEARED**

Event Message	Facility	Severity	Event Type	Log
Deleted logs by restore-factory-defaults issued by user {Username}	LOG_DAEMON	Emergency	Alarm	Syslog

- **SE\_COMMUNICATION\_DATA\_INTEGRITY\_ERROR**

Event Message	Facility	Severity	Event Type	Log
FAILURE. The firmware integrity check has failed. This may indicate that some	LOG_DAEMON	Critical	Alarm	Syslog

Event Message	Facility	Severity	Event Type	Log
operating system files have been modified or tampered with. For assistance, contact Siemens Customer Support.				

- **SE\_SESSION\_CLOSED**

Event Message	Facility	Severity	Event Type	Log
username:{Username} usid: {User ID} stopped {Context} session from ip:{IP Address}	LOG_AUTH	Notice	Event	Auth.log

- **SE\_SESSION\_CLOSED (console)**

Event Message	Facility	Severity	Event Type	Log
username:{Username} usid: {User ID} started {Context} session from ip: 127.0.0.1 source-port:0 through console protocol	LOG_AUTH	Notice	Event	Auth.log

- **SE\_PATCH\_DEPLOYMENT\_SUCCEEDED**

Event Message	Facility	Severity	Event Type	Log
The other partition was imaged successfully. A reboot is required to boot the other partition.	LOG_DAEMON	Notice	Event	Upgrade

- **SE\_PATCH\_DEPLOYMENT\_FAILED (Failure during ROXFLASH)**

Event Message	Facility	Severity	Event Type	Log
A failure was encountered in the upgrade process.	LOG_DAEMON	Notice	Event	Upgrade

- **SE\_PATCH\_DEPLOYMENT\_FAILED (During uninstall - ROXFLASH)**

Event Message	Facility	Severity	Event Type	Log
A failure was encountered in the uninstallation process.	LOG_DAEMON	Notice	Event	Upgrade

- **SE\_PATCH\_DEPLOYMENT\_FAILED (Can not connect to upgrade server - ROXFLASH)**

Event Message	Facility	Severity	Event Type	Log
Failed to get upgrade details from server, please verify connection.	LOG_DAEMON	Notice	Event	Upgrade

- **SE\_PATCH\_DEPLOYMENT\_FAILED (No differences - ROXFLASH)**

Event Message	Facility	Severity	Event Type	Log
No differences detected in target version. Nothing to upgrade	LOG_DAEMON	Notice	Event	Upgrade



- **SE\_PATCH\_DEPLOYMENT\_FAILED (Failed to configure boot partition - ROXFLASH)**

Event Message	Facility	Severity	Event Type	Log
Failed to configure system to boot partition %s on next boot	LOG_DAEMON	Notice	Event	Upgrade

- **SE\_PATCH\_DEPLOYMENT\_FAILED (Failed to upgrade target partition - upgrade)**

Event Message	Facility	Severity	Event Type	Log
Failed upgrading target partition	LOG_DAEMON	Notice	Event	Upgrade

- **SE\_PATCH\_DEPLOYMENT\_FAILED (General) - upgrade**


Event Message	Facility	Severity	Event Type	Log
Failed running {Command} on target partition	LOG_DAEMON	Notice	Event	Upgrade

## Using RUGGEDCOM ROX II

This chapter describes how to use the RUGGEDCOM ROX II Web user interface.

### 2.1 Default User Names and Passwords

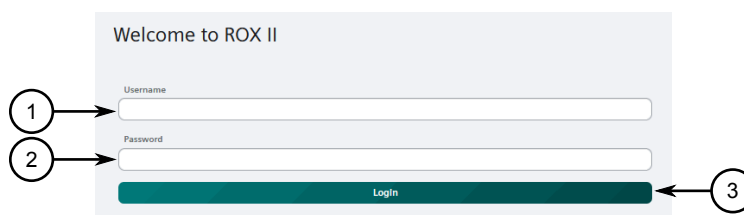
The following default passwords are pre-configured on the device for each access mode:

 <b>NOTICE</b>		
<b>Security hazard – risk of unauthorized access and/or exploitation</b> To prevent unauthorized access to the device, change the default passwords before commissioning the device. For more information, refer to "Managing Passwords and Passphrases" (Page 118).		
Mode	Username	Password
Administrator	admin	admin

### 2.2 Logging In

To log in to RUGGEDCOM ROX II, do the following:

1. Launch a Web browser and request a connection to the router. The **Log In** form appears.



- ① Username Box
- ② Password Box
- ③ Login Button

Figure 2.1 RUGGEDCOM ROX II Log In Form

---

**Note**

RUGGEDCOM ROX II features three default user accounts: admin, operator and guest. Additional user accounts can be added. For information about adding user accounts, refer to "Adding a User" (Page 117).

---

2. In the **Username** field, type the user name.

---

**Note**

If a unique password/passphrase has not been configured, use the factory default password. For more information, refer to "Default User Names and Passwords" (Page 23).

---

 **NOTICE**

**BFA Protection**

RUGGEDCOM ROX II features a Brute Force Attack (BFA) protection system to detect potentially malicious attempts to access the device. When enabled, the protection system will block an IP address after 15 failed login attempts over a 10 minute period. The IP address will be blocked for 720 seconds or 12 minutes the first time. If the same IP address fails again 15 times in a 10 minute period, it will be blocked again, but the waiting period will be 1.5 times longer than the previous wait period.

Siemens strongly recommends that BFA protection be enabled. For more information about enabling BFA protection, refer to "Enabling/Disabling Brute Force Attack Protection" (Page 128).

BFA protection is enabled by default for new installations of RUGGEDCOM ROX II.

3. In the **Password** field, type the password associated with the username.
4. Click **Login**. The main RUGGEDCOM ROX II menu appears.

## 2.3 Logging Out

To log out of the device, click the **Active User** icon (  ) in the toolbar, and then click **Logout**.



① Active User Icon

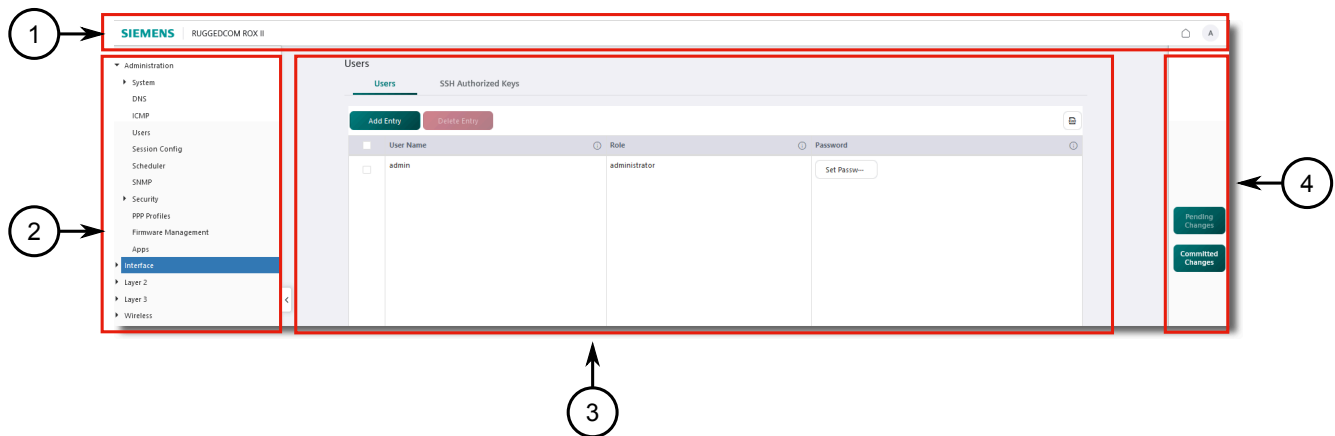
Figure 2.2 Active User Icon

## 2.4 Navigating the Interface

The following describes the general screen layout and features available for navigating the user interface.

### 2.4.1 Screen Layout

The user interface is made up of four sections: the **Toolbar**, the **Tree Menu**, the **Change Management Pane**, and the **Center Pane**.



- ① Toolbar
- ② Tree Menu
- ③ Center Pane
- ④ Change Management Pane

Figure 2.3 Screen Layout

#### Toolbar

The **Toolbar** contains the **Home** button (🏠), which returns the user to the home page, and the **Active User** icon (A), which represents the first initial of the logged-in user.

#### Tree Menu

The **Tree Menu** on the left side of the user interface lists top-level categories of features that can be configured. Click the right-pointing triangle (▶) next to a category to expand or collapse the links underneath.

Links in the tree menu display pages in the **Center Pane**.

#### Center Pane

The **Center Pane** is the main area for configuration.

This pane contains a table of configurable items or status entries. When a table contains many columns or entries, horizontal and vertical scrolling is available via a scroll bar either below the center pane list or on the right side.

### Change Management Pane

The **Change Management Pane** on the right side of the interface contains the **Pending Changes** and **Committed Changes** buttons.

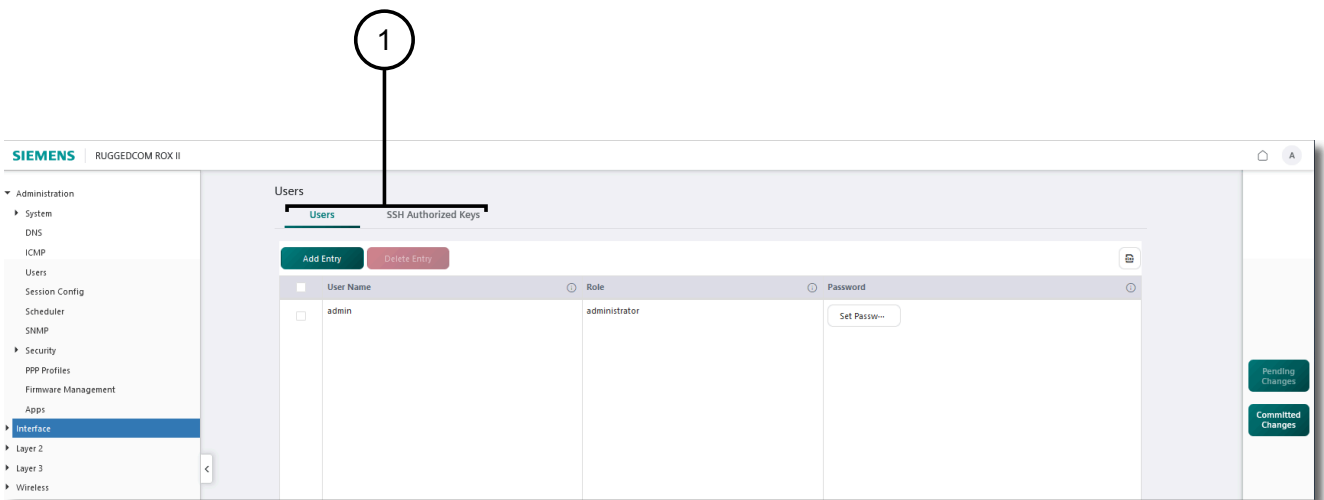
For more information about managing changes, refer to "Managing Changes" (Page 34).

### 2.4.2 Tabs

Configuration settings and information for each feature are broken into sub-categories, each represented by a tab. Clicking a tab displays the associated parameters and/or tables.

#### Note

Some tabs are only available when specific configuration settings are enabled or selected.



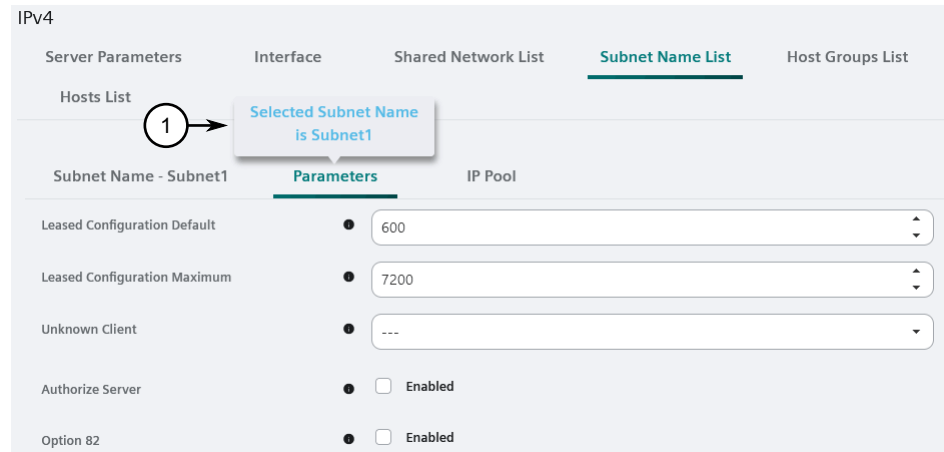
① Tabs

Figure 2.4 Tabs

### 2.4.3 Locator Tooltips

Multiple new entries can be added to a table. In some cases, additional child tabs are created for the new entries in the structure. To provide context, locator tooltips are used to inform the user of which parent parameter they are viewing or configuring.

When applicable, hovering over a parameter name indicates the selected parent. For example, in the graphic below, the **Parameters** tab is active for the **Subnet Name Subnet 1**.










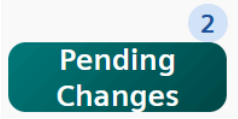




① Tooltip Notification







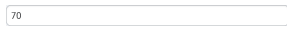

Figure 2.5 Locator Tooltip

## 2.4.4 UI Controls

The following controls appear in RUGGEDCOM ROX II:

Control	Description
	<b>Move</b> Click the icon to move rows up or down in a table.
	<b>Start</b> Click the button to start a process (e.g. diagnostic cable testing).
	<b>Up/Down</b> Click the up/down arrows to increase or decrease the value in a list.
	<b>Expand</b> Click and drag the icon to expand a box.
	<b>Perform</b> Click the button to perform an action (e.g. rebooting the device).

Control	Description
	<b>Select</b> Click the button to make a selection.
	<b>Abort</b> Click the button to abort a configuration change before committing.
	<b>Validate</b> Click the button to validate pending configuration changes.
	<b>Commit</b> Click the button to commit configuration changes.
	<b>Load Rollback</b> Click the button to revert to a prior configuration.
	<b>Delete Entry</b> Click the button to delete an entry from a table.
	<b>Add Entry</b> Click the button to add an entry to a table.
	<b>Pending Changes</b> Click the icon to access the <b>Change List</b> . The number in the top right corner indicates the number of pending changes.
	<b>Committed Changes</b> Click the icon to access the <b>Change List</b> .
	<b>Checkmark</b> Indicates the selection.
	<b>Checkbox Cleared</b> Click a check box to select or enable an option. Clear the check box to de-select or disable the option.
	<b>Checkbox Checked</b> Click a check box to select or enable an option. Clear the check box to de-select or disable the option.

Control	Description
	<b>Refresh</b> Click the button to refresh the data within a table.
	<b>Export All Data</b> Click the button to export table data to the Downloads folder in .xlsx format.
	<b>Info</b> Click the icon to display a description of the parameter and its usage.
	<b>Home</b> Click the icon to return to the <b>Home</b> page.
	<b>Active User</b> Displays the logged-in user. The letter used in the <b>Active User</b> icon represents the first initial of the logged-in user. For example, the <b>Administrator</b> login is represented as <b>A</b> .
	<b>Dropdown</b> Click the arrow to expand the items in a list.
	<b>Box</b> Type parameter values in text boxes.
	<b>Angle Brackets</b> Click to advance to the next page or return to the previous page in a multiple-page table.

## 2.5 Configuring the Device

The following sections describe the features available for making configuration changes to the device.

### 2.5.1 Using Tables

Tables are accessed via the selection made in the **Tree Menu**.

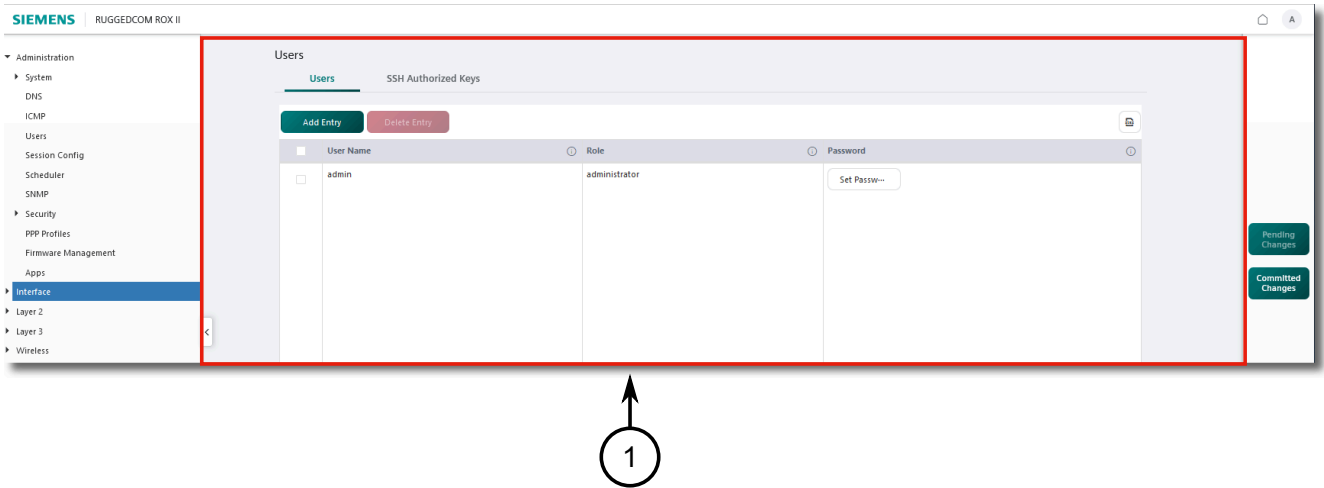
Tables are used to view status information, configure existing entries, and add or delete entries.

Configuration settings and information for each feature are broken into sub-categories, each represented by a tab. Clicking a tab displays the associated parameters and/or tables.



**Note**

Some tabs are only available when specific configuration settings are enabled or selected.



① Table

Figure 2.31 Table

**2.5.1.1 Selecting Entries in a Table**

Each configurable item in a table contains a selectable check box. One or more entries can be selected individually by selecting the individual check box beside each item, or all items can be selected by clicking the **Select All** check box.

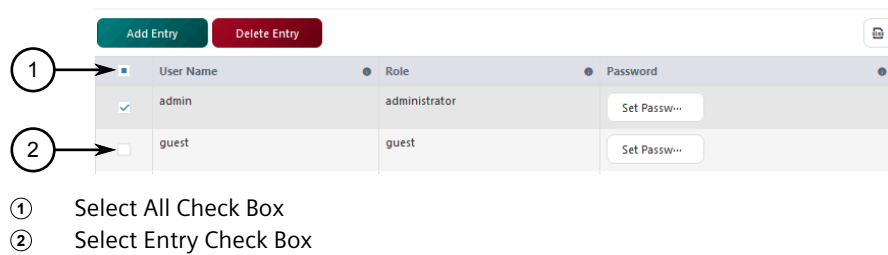
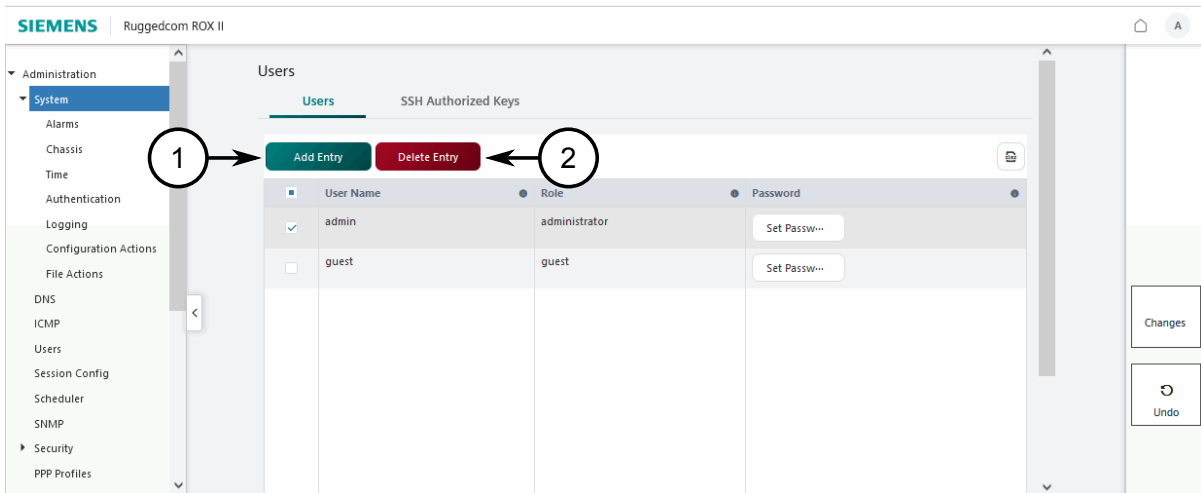


Figure 2.32 Selection Check Box

Select the check box beside the entry or entries to be configured, or click **Select All** to select all items in the list.

### 2.5.1.2 Adding and Deleting Table Entries

Items can be added to or deleted from a table by using the **Add Entry** or **Delete Entry** buttons.

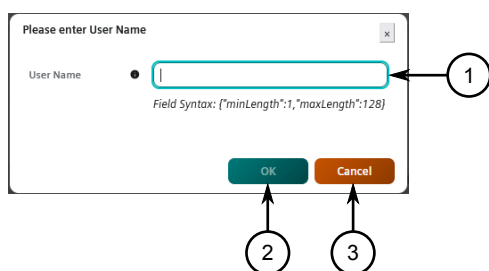


- ① Add Entry Button
- ② Delete Entry Button

Figure 2.33 Adding and Deleting Entries

### Adding an Entry

Entries are added to a table by clicking the **Add Entry** button. Once clicked, a dialog box appears allowing the user to configure the required parameter(s).



- ① Text Box
- ② OK Button
- ③ Cancel Button

Figure 2.34 Dialog Box

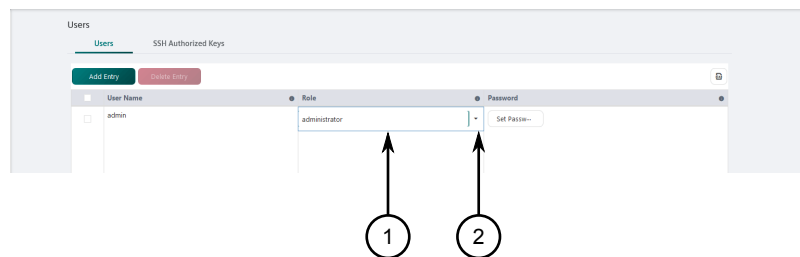
Click **OK** to add the entry, and then configure any additional parameters for the entry in the table as needed.

### Deleting an Entry

Entries are deleted from a table by selecting the entry and then clicking **Delete Entry**.

### 2.5.1.3 Editing Table Cells

Once the initial configuration takes place, additional configuration may be available by double clicking and configuring the applicable fields in the list columns. Each configurable field contains a text box, integer box, or drop down list, as applicable.

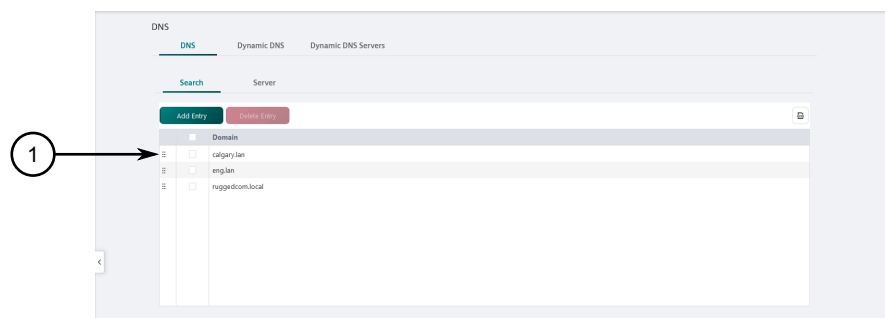


- ① List
- ② Drop Down Icon

Figure 2.35 Editing a Table Cell

### 2.5.1.4 Changing the Priority of Table Entries

Entries in a table can be moved up or down in the list using the **Move** icon (⋮).



- ① Move Icon

Figure 2.36 Move Icon

Click and drag the icon up or down to change the position of an item in the list.

### 2.5.1.5 Scrolling Between Table Pages

When a table contains multiple pages, users can scroll between pages by either selecting the desired page number or by clicking the angle brackets (< >) to advance to the next page or return to the previous page.

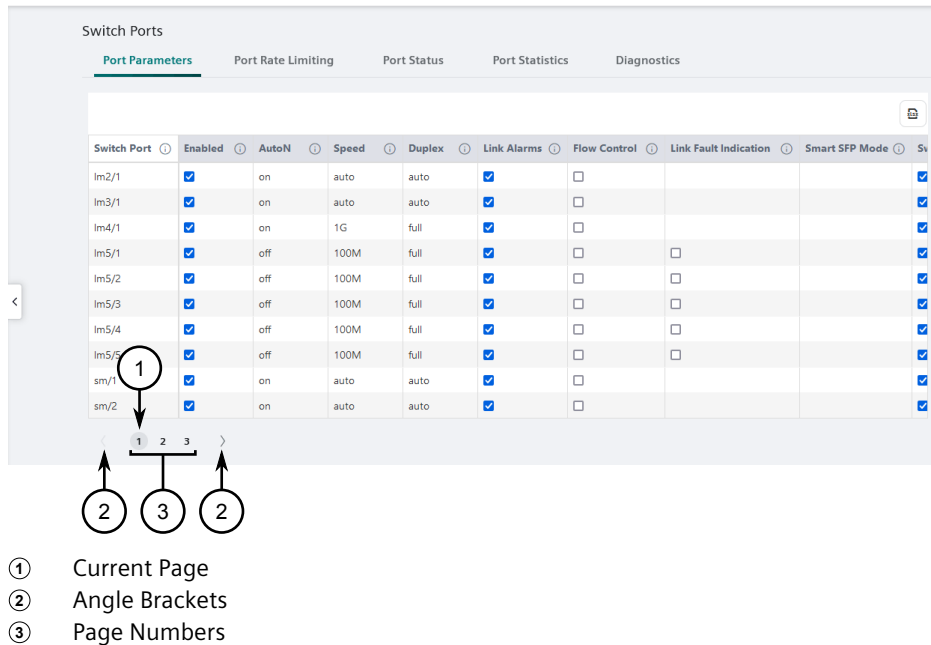
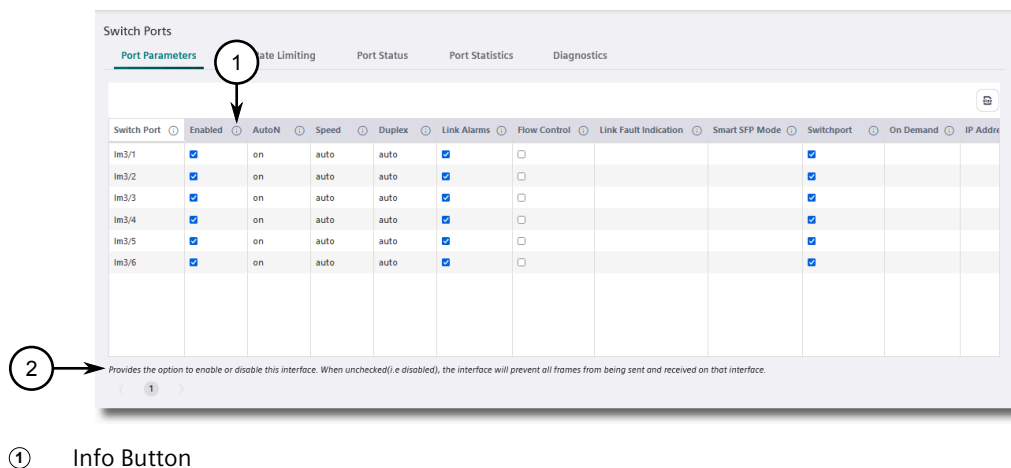


Figure 2.37 Multiple Page Table

### 2.5.2 Using the Info Button

The info button (ⓘ) displays a brief description of the associated parameter or table column. This information describes the general purpose of the parameter or table column and may include details on configuration requirements, syntax, available options, etc.




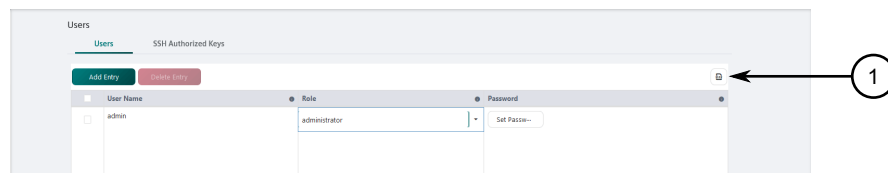
② Displayed Information

Figure 2.38 Info Button

Click the button to display the description below the parameter or table.

## 2.5.3 Exporting Data to Excel

The **Export All Data** button (  ) allows users to export form data to Microsoft Excel (\*.xlsx).



① Export All Data Button

Figure 2.39 Export All Data Button

Click the button to start the process. A window appears showing the status of the download.

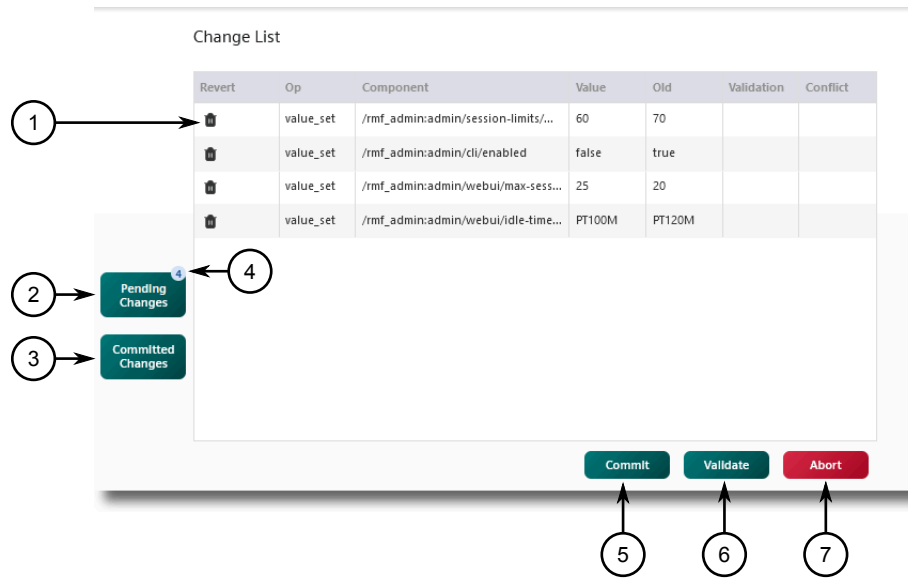
## 2.6 Managing Changes

The following sections describe how to view, validate, discard, and commit changes to the running configuration.

### 2.6.1 Viewing Configuration Changes

The **Change List** slide out allows users to view a list of all changes made since the last commit. These changes are pending and need to be committed before they are applied to the running configuration. Changes can also be validated (to identify potential errors) or aborted.

A counter on the **Pending Changes** button indicates the number of pending changes.



- ① Revert Button
- ② Pending Changes Button
- ③ Committed Changes Button
- ④ Pending Changes Count
- ⑤ Commit Button
- ⑥ Validate Button
- ⑦ Abort Button

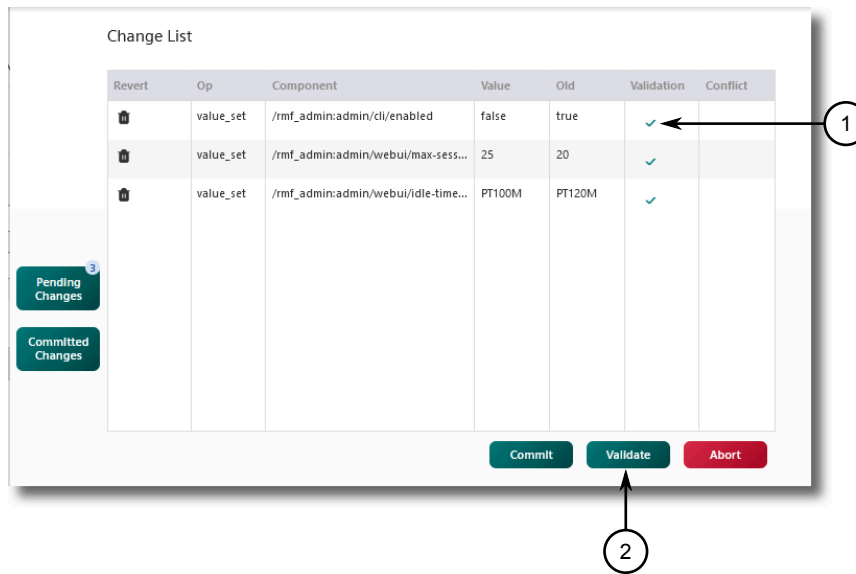
Figure 2.40 Change List

## 2.6.2 Validating Configuration Changes

Before committing changes, each change should be validated to identify configurations errors. This is done from the **Change List** slide out by clicking **Validate**.

If validation is successful, a check mark appears in the **Validation** column next to each candidate.

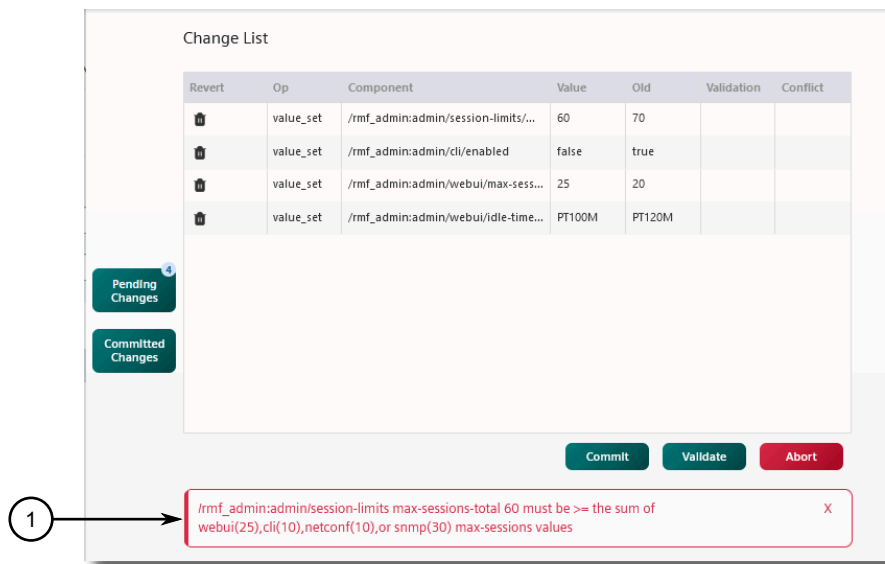
2.6.2 Validating Configuration Changes



- ① Validation Success Check Mark
- ② Validate Button

Figure 2.41 Change List

If validation was not successful, a notification appears describing the first error identified.

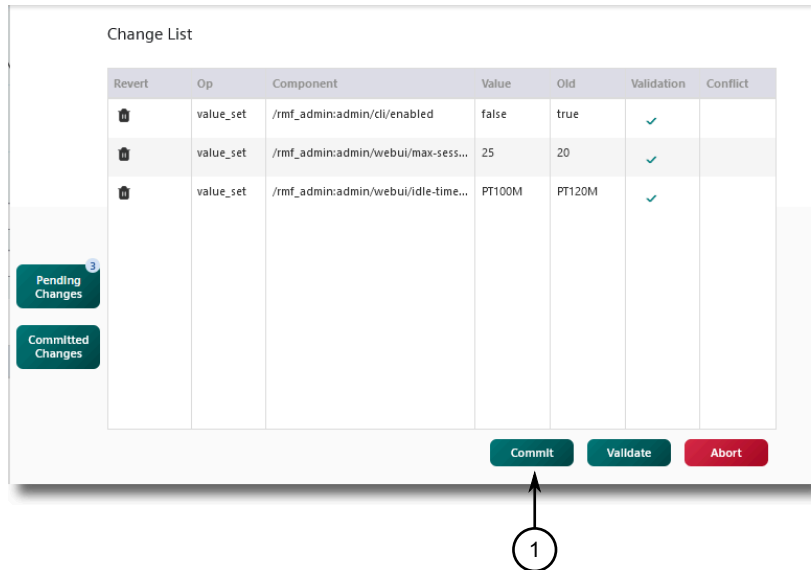


- ① Error Message

Figure 2.42 Validation Error

### 2.6.3 Committing a Change

All changes made during a configuration session are considered *candidates* until they are committed and applied to the running configuration. This is done by clicking **Commit** in the **Change List**.



① Commit Button

Figure 2.43 Change List

Changes can be committed as they are made, or collected until it is time to commit all changes.

#### Note

When collecting changes to be committed later, it is recommended to validate the occasional change to lessen the chance of running into errors at the end of the configuration session.

#### Note

Candidates are not visible to other users until they are committed.

#### Note

If a user opens a configuration session during another user's configuration session, the user cannot commit their changes until the other user ends their session.

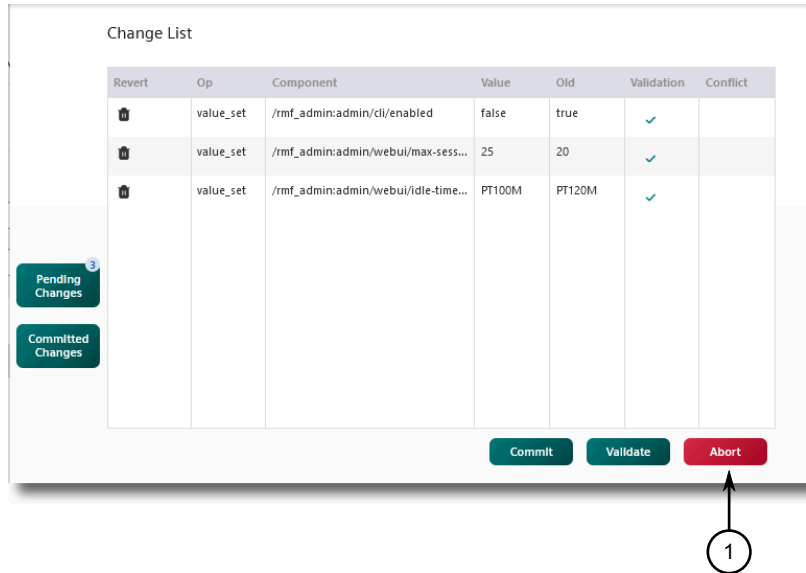
### 2.6.4 Discarding a Change

There are two methods to discard changes: abort and rollback. Each method is available by accessing the **Change List** slide out.



## Aborting a Change

The **Abort** button discards all pending changes made since the last commit.



① Abort Button

Figure 2.44 Change List

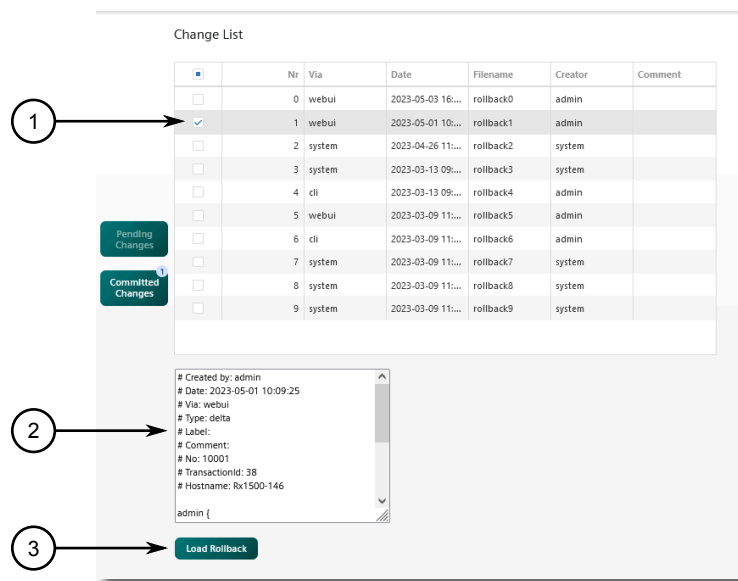
To abort all changes, click **Abort**.

## Rolling Back a Configuration

The **Load Rollback** button allows users to revert to an earlier committed configuration.

Configurations are sorted by date, with the most recent changes at the top of the list.

When an entry is selected, details about the configuration are displayed in the **Load Rollback Details** window.



- ① Selected Rollback
- ② Load Rollback Details Window
- ③ Load Rollback Button

Figure 2.45 Change List

To use this feature, select a configuration to which to revert, click the **Load Rollback** button, and then commit the change.

## 2.7 Using Network Utilities

RUGGEDCOM ROX II features built-in troubleshooting tools for pinging hosts, tracing routes, and analyzing packets. All utilities are available under **Tools » Network Utilities** in the tree menu.

### 2.7.1 Pinging an IPv4 Address or Host

To ping an IPv4 address or host, do the following:

1. Navigate to the **Ping** tab under **Tools » Network Utilities**.
2. Under **Type**, select **Ping**.
3. Configure the following parameters as required:

Parameter	Description
Destination	The IPv4 address or name of the host.
Ping Counts	The number of ping attempts.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.

5. Under **Ping Control**, click **Start**. The results of the ping action are displayed in the box below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.2 Pinging an IPv6 Address or Host

To ping an IPv6 address or host, do the following:

1. Navigate to the **Ping** tab under **Tools » Network Utilities**.
2. Under **Type**, select **Ping6**.
3. Configure the following parameters as required:

Parameter	Description
Destination	The IPv6 address or name of the host.
Ping Counts	The number of ping attempts.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Ping Control**, click **Start**. The results of the ping action are displayed in the box below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.3 Pinging MPLS Endpoints

To ping an MPLS endpoint, do the following:

1. Navigate to the **Ping** tab under **Tools » Network Utilities**.
2. Under **Type**, select **mpls-ping**.
3. Configure the following parameters as required:

Parameter	Description
Destination	The IPv4 address and prefix of the MPLS endpoint.
Ping Counts	The number of ping attempts.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Ping Control**, click **Start**. The results of the ping action are displayed in the box below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.4 Pinging VRF Endpoints

To ping an VRF endpoint, do the following:

1. Navigate to the **Ping** tab under **Tools » Network Utilities**.
2. Under **Type**, select **vrf-ping**.
3. Configure the following parameters as required:

Parameter	Description
VRF	The target VRF.
Destination	The IPv4 address and prefix of the VRF endpoint.
Ping Counts	The number of ping attempts.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Ping Control**, click **Start**. The results of the ping action are displayed in the box below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.5 Tracing a Route to an IPv4 Host

To trace a route to an IPv4 host, do the following:

1. Navigate to the **Traceroute** tab under **Tools » Network Utilities**.
2. Under **Type**, select **traceroute**.
3. Configure the following parameters as required:

Parameter	Description
Hostname	The name or IP address of the host.
Verbose Output	When selected, trace results provide more detail.
Lookup Address	When selected, the source IP address is displayed in the trace results.
Use ICMP Instead of UDP	When selected, ICMP is used in place of UDP.
Max Number of Hops	The maximum number of hops to the remote host.
Packet Length	The maximum length of each packet.
Interface	The interface connected to the remote host.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Traceroute Control**, click **Start**. The results of the trace action are displayed in the box below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.6 Tracing a Route to an IPv6 Host

To trace a route to an IPv6 host, do the following:

1. Navigate to the **Traceroute** tab under **Tools » Network Utilities**.
2. Under **Type**, select **traceroute6**.
3. Configure the following parameters as required:

Parameter	Description
Hostname	The name or IP address of the host.
Verbose Output	When selected, trace results provide more detail.
Lookup Address	When selected, the source IP address is displayed in the trace results.
Use ICMP Instead of UDP	When selected, ICMP is used in place of UDP.
Max Number of Hops	The maximum number of hops to the remote host.
Packet Length	The maximum length of each packet.
Interface	The interface connected to the remote host.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Traceroute Control**, click **Start**. The results of the trace action are displayed in the box below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.7 Tracing a Route to an MPLS Endpoint

To trace a route to an MPLS endpoint, do the following:

1. Navigate to the **Traceroute** tab under **Tools » Network Utilities**.
2. Under **Type**, select **mpls-traceroute**.
3. Type the IPv4 address in the **Remote IP Address/Prefix** box.
4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Traceroute Control**, click **Start** to start the trace. The results of the trace action are displayed below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.8 Tracing a Route to a VRF Endpoint

To trace a route to a VRF endpoint, do the following:

1. Navigate to the **Traceroute** tab under **Tools » Network Utilities**.

2. Under **Type**, select **vrf-traceroute**.
3. Configure the following parameters as required:

Parameter	Description
Hostname	The name or IP address of the host.
Verbose Output	When selected, trace results provide more detail.
Lookup Address	When selected, the source IP address is displayed in the trace results.
Use ICMP Instead of UDP	When selected, ICMP is used in place of UDP.
Max Number of Hops	The maximum number of hops to the remote host.
Packet Length	The maximum length of each packet.
VRF	The target VRF.
Interface	The interface connected to the remote host.

4. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
5. Under **Traceroute Control**, click **Start** to start the trace. The results of the trace action are displayed below.
6. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.7.9 Capturing Packets from a Network Interface

Tcpdump is a packet analyzer for TCP/IP and other packets. It can be used to capture packets at a specified network interface and dump them to a terminal or file.

To capture packets, do the following:

1. Navigate to the **TCP Dump** tab under **Tools » Network Utilities**.
2. Under **Type**, select **tcpdump**.
3. Under **Interface To Capture On**, select the interface to capture data from.
4. Under **Maximum Packets Captured**, set the maximum number of packets to capture.
5. Under **Maximum Capture Time (seconds)**, set the maximum time to capture packets.
6. If necessary, select **Lookup Address** to display the source IP for each packet.
7. If necessary, select **Display Link Level Header** to display the link level header information for each packet.
8. If necessary, select **Perform HEX/ASCII Dump** to convert the data to hexadecimal or ASCII characters.

9. Under **Verbosity**, set the verbosity level to control how much information is dumped.
10. If a specific host name should be ignored, define the name of the host.
11. If a specific protocol(s) should be ignored, define the protocol type(s).
12. If packets are to be captured on a particular port, define the port.
13. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
14. Under **TCP Dump Control**, click **Start** to start the dump. The results are displayed in the box below.
15. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

### Sample Output

```

tcpdump -i fe-2-1 -c 10 --
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on fe-2-1, link-type EN10MB (Ethernet), capture size 262144 bytes
14:16:37.692382 IP 192.168.12.1 > 224.0.0.5: OSPFv2, Hello, length 48
14:16:37.696158 IP 192.168.12.2 > 224.0.0.5: OSPFv2, Hello, length 48
14:16:37.761546 IP 192.168.12.2 > 224.0.0.13: igmp v2 report 224.0.0.13
14:16:38.172063 IP 192.168.12.1 > 224.0.0.2: igmp v2 report 224.0.0.2
14:16:40.289550 IP 192.168.12.2 > 224.0.0.22: igmp v2 report 224.0.0.22
14:16:41.662618 IP 192.168.12.1 > 224.0.0.13: PIMv2, Hello, length 26
14:16:44.593544 IP 192.168.12.2 > 224.0.0.6: igmp v2 report 224.0.0.6
14:16:45.297569 IP 192.168.12.2 > 224.0.0.5: igmp v2 report 224.0.0.5
14:16:45.298858 IP 192.168.12.2 > 224.0.0.13: PIMv2, Hello, length 26
14:16:47.692585 IP 192.168.12.1 > 224.0.0.5: OSPFv2, Hello, length 48
10 packets captured
10 packets received by filter
0 packets dropped by kernel
stopped

```

## 2.7.10 Capturing Packets from a VRF Network Interface

VRF Tcpcdump is a packet analyzer for TCP/IP and other packets. It can be used to capture packets at a specified VRF network interface and dump them to a terminal or file.

To capture packets, do the following:

1. Navigate to the **TCP Dump** tab under **Tools » Network Utilities**.
2. Under **Type**, select **vrf-tcpdump**.
3. Under **Interface To Capture On**, select the interface to capture data from.
4. Under **Maximum Packets Captured**, set the maximum number of packets to capture.
5. Under **Maximum Capture Time (seconds)**, set the maximum time to capture packets.
6. [Optional] Select **Lookup Addresses** to display the source IP for each packet.

7. [Optional] Select **Display Link Level Header** to display the link level header information for each packet.
8. [Optional] Select **Perform HEX/ASCII Dump** to convert the data to hexadecimal or ASCII characters.
9. Under **Verbosity**, set the verbosity level to control how much information is dumped.
10. If a specific host name should be ignored, define the name of the host.
11. If a specific protocol(s) should be ignored, define the protocol type(s).
12. If packets are to be captured on a particular source and/or destination port, define the port.
13. [Optional] Under **Auto Scroll on Output**, select **Enabled** to allow auto scrolling.
14. Under **TCP Dump Control**, click **Start** to start the dump. The results are displayed in the box below.
15. [Optional] Under **Pop Out Output Window**, click **Pop Out** to display the log in a separate dialog box.

## 2.8 Using the Command Line Interface

The Web user interface includes a built-in Command Line Interface (CLI). To access the Command Line Interface (CLI) from within the Web interface, navigate to **Tools » CLI** in the tree menu.

For more information about how to use the Command Line Interface, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual" for the device.

## 2.9 Accessing Different Modes

Aside from normal mode, there are three additional modes within RUGGEDCOM ROX II that offer various controls over the operating system. These include BIST mode, service mode, and maintenance mode. For information about switching to one of these modes, refer to the "RUGGEDCOM ROX II CLI Configuration Manual" for the device.

### 2.9.1 Enabling/Disabling SSH Access in Maintenance Mode

SSH access to the device is disabled by default when the device is in maintenance mode. However, temporary access may be required.



**⚠ NOTICE****Security hazard – risk of unauthorized access and/or exploitation**

Before enabling SSH access, make sure a strong password is configured and the device is connected to a trusted network. Failure to protect the device could allow a user with remote access to the device and the root password to access the Linux shell

To temporarily enable SSH access on port 222 while the device is in maintenance mode, enter the following commands at the command prompt:

```
rm /etc/ssh/sshd_not_to_be_run
systemctl start sshd.service
```

To again disable SSH access, enter the following commands:

```
systemctl stop sshd.service
touch /etc/ssh/sshd_not_to_be_run
```

## 2.9.2 Managing Maintenance Mode Authorization

Maintenance mode grants access to the Linux shell. It is used primarily by Siemens Customer Support to access diagnostic information when needed as part of the troubleshooting process.

Misuse of the commands available in this mode can corrupt the operational state of the device and render it inaccessible. As such, a reusable access key specific to the device is required to authorize access to the maintenance mode command. To obtain an access key, contact Siemens Customer Support. Note that once the access key has been obtained, a maintenance mode password is still required to access maintenance mode.

Maintenance mode authorization is configurable to allow access either temporarily or permanently. When maintenance mode access is configured temporarily, access will remain active until either the device is rebooted or maintenance mode access is disabled manually. Upgrading the device requires a reboot that will disable maintenance mode access.

When maintenance mode access is configured permanently, access will remain active until either the device software is flashed, restored to factory default settings or disabled manually. Upgrading the device with permanent maintenance mode configured will retain the enabled maintenance mode setting.

**⚠ NOTICE****Configuration hazard – risk of data corruption**

To avoid accidental data corruption, Siemens recommends disabling maintenance mode access immediately when no longer required.

### 2.9.2.1 Temporarily Enabling Maintenance Mode Authorization

To enable maintenance mode authorization until the next device reboot, do the following:

---

**Note**

The access key contains several characters in multiple formats, and can be difficult to convey via telephone. As such, Siemens recommends providing the key via email. If email is unavailable, a hexadecimal format access key can be provided via telephone support.

For more information about obtaining a hexadecimal format access key via telephone, contact Siemens Customer Support.

---

1. Contact Siemens Customer Support to obtain an access key.  
The MLFB (if provided) and serial number of the device will be required. To obtain this information, refer to "Displaying Device and Software Information" (Page 53).
2. Navigate to the **Maintenance Mode** tab under **Administration » System**.
3. Under **Maintenance Mode Key**, insert the key provided by Siemens Customer Support.
4. Under **Enable Maintenance Mode**, click **Perform**.  
A confirmation dialog box appears. Click **OK** to proceed.  
Maintenance mode authorization will be enabled until the next device reboot.
5. [Optional] To verify maintenance mode authorization status has been successfully enabled, refer to "Displaying Device and Software Information" (Page 53).
6. [Optional] Access maintenance mode. For more information, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual" for the device.

### 2.9.2.2 Permanently Enabling Maintenance Mode Authorization

Maintenance mode authorization can be enabled permanently, until either the device software is flashed/downgraded or the device is restored to factory default settings.

For more information about upgrading or downgrading software, refer to "Upgrading/Downgrading Software" (Page 83).

For more information about restoring the factory default settings for the device, refer to "Restoring Factory Defaults" (Page 58).

 **NOTICE**

**Configuration hazard – risk of data corruption**

Siemens recommends enabling permanent maintenance mode access only when absolutely necessary, and disabling maintenance mode access when no longer required.

To permanently enable maintenance mode authorization, do the following:

1. Enable maintenance mode. For more information, refer to "Temporarily Enabling Maintenance Mode Authorization" (Page 47).
2. Navigate to the **Maintenance Mode** tab under **Administration » System**.
3. Under **Enable Maintenance Mode Permanently**, click **Perform**.

A confirmation dialog box appears. Click **OK** to proceed.

Maintenance mode authorization is enabled permanently until the device software is upgraded/downgraded or the device is restored to factory default settings.

### 2.9.2.3 Disabling Maintenance Mode Authorization

To disable maintenance mode authorization, do the following:

1. Navigate to the **Maintenance Mode** tab under **Administration » System**.
2. Under **Disable Maintenance Mode**, click **Perform**.

Maintenance mode access is disabled.

## Getting Started

This section describes startup tasks to be performed during the initial commissioning of the device. Tasks include connecting to the device and accessing the RUGGEDCOM ROX II Web User Interface, as well as configuring a basic network.

### 3.1 Connecting to RUGGEDCOM ROX II

The Web user interface and Command Line Interface (CLI) can be accessed via a direct connection between a workstation and a device or a remote connection over the network.

#### 3.1.1 Default IP Address

The default IP address for the device is as follows:

Port	IP Address/Mask
MGMT	192.168.1.2/24
All other Ethernet ports	192.168.0.2/24

#### 3.1.2 Connecting Directly via a Port

The Web user interface can be accessed directly using an appropriate cable connection between the device and a workstation.

---

**Note**

For information about connecting directly via the serial console, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".

---

To access the Web user interface using a direct connection to the device, do the following:

1. Connect a workstation running a Web browser to either the MGMT (Management) port or any other RJ45 Ethernet port on the device.

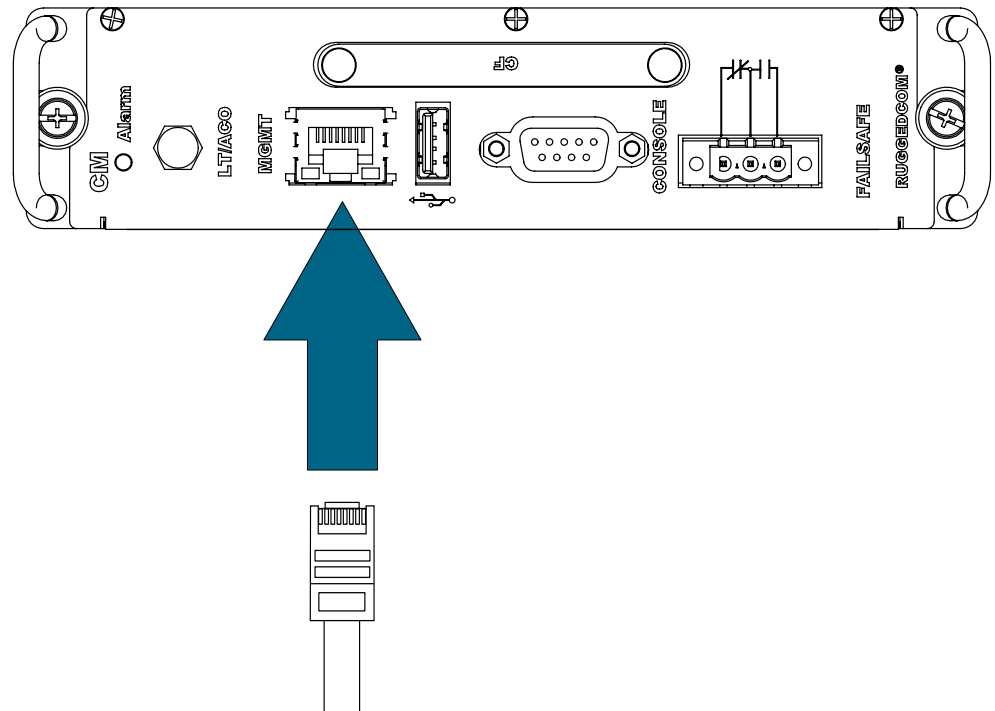


Figure 3.1 MGMT Port

2. Configure the IP address range and subnet for the workstation's Ethernet port. The range is typically the IP address for the device's IP interface plus one, ending at \*.\*\*.254.

For example, if the device's IP address is 192.168.0.2, configure the workstation's Ethernet port with an IPv4 address in the range of 192.168.0.3 to 192.168.0.254.

3. Launch a Web browser.
4. If using a proxy server, make sure the IP address and subnet for the device are included in the list of exceptions.
5. In the address bar, enter the host name or IP address for the device, and then press **Enter**.
6. If the device's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Click **Yes** to continue. The login prompt appears.
7. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 23).

### 3.1.3 Connecting Remotely via a Web Browser

The Web user interface can be accessed securely and remotely using a Web browser.

**Note**

For information about connecting remotely via SSH using the CLI, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".

To access the Web user interface over the network, do the following:

1. Launch a Web browser.
2. If using a proxy server, make sure the IP address and subnet for the device are included in the list of exceptions.
3. In the address bar, enter the host name or IP address for the device, and then press **Enter**.
4. If the device's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Click **Yes** to continue. The login prompt appears.
5. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 23).

## 3.2 Configuring a Basic Network

RUGGEDCOM ROX II has the following Internet interfaces configured by default: *dummy0*, *fe-cm-1* and *switch.0001*. The default IP addresses for *fe-cm-1* and *switch.0001* are configured under the **ip » { interface } » ipv4**, where { interface } is the name of the interface. The default *switch.0001* interface is the VLAN interface and is only seen if there is one or more Ethernet line modules installed. It is created implicitly, as all switched ports have a default PVID of 1.

The following table lists the default IP addresses.

Interface	IP Address
switch.0001	192.168.0.2/24
fe-cm-1	192.168.1.2/24
fe-em-1 <sup>a</sup>	192.168.2.1/24

<sup>a</sup> Optional expansion module.

### 3.2.1 Configuring a Basic IPv4 Network

To configure a basic IPv4 network, do the following:

1. Connect a computer to the Fast Ethernet (fe-cm-1) of the device and configure the computer to be on the same subnet as the port.
2. Configure the computer to use the IPv4 address of the Fast Ethernet port as the default gateway.
3. Connect one of the switched ports from any available line module to a switch that is connected to a LAN.

4. Make sure the computer connected to the switch is on the same subnet as the switch.
5. Enable the Brute Force Attack (BFA) protection system on the device. For more information, refer to "Enabling/Disabling Brute Force Attack Protection" (Page 128).
6. Configure the switch and all the computers behind it to use switch.0001's IP address as the default gateway. The default IP address is 192.168.0.2.
7. Make sure all computers connected to the device can ping one another.

### 3.2.2 Configuring a Basic IPv6 Network

To configure a basic IPv6 network, do the following:

1. Connect a computer to the Fast Ethernet port (fe-cm-1) of the device and configure the computer to be on the same subnet as the port.
2. Configure an IPv6 address and default gateway for the computer (e.g. FDD1:9AEF:3DE4:1/24 and FDD1:9AEF:3DE4:2).
3. Configure the fe-cm-1 and switch.0001 interfaces on the device with IPv6 addresses.
4. Connect one of the switched ports from any available line module to an IPv6 capable network.
5. Configure the computers on the IPv6 network to be on the same IP subnet as switch.0001 and configure the default gateway address.
6. Enable the Brute Force Attack (BFA) protection system on the device. For more information, refer to "Enabling/Disabling Brute Force Attack Protection" (Page 128).
7. Enable IPv6 Neighbor Discovery. For more information, refer to "Configuring IPv6 Neighbor Discovery" (Page 227).
8. Make sure all computers connected to the device can ping one another.

## Device Management

This chapter describes how to manage device hardware, including ports, files, logs, firmware, etc.

### 4.1 Displaying Device and Software Information

During troubleshooting or when ordering new devices/features, Siemens may request specific information about the device, such as the model, order code (MLFB), or system serial number.

To display general information about the device and its software, navigate to the **Chassis Status** tab under **Administration » System » Chassis » System**.

The following information is provided:

Parameter	Description
Chassis Model	<b>Synopsis:</b> A string The RuggedCom device model name.
Software License	<b>Synopsis:</b> A string The current software capability.
MLFB	<b>Synopsis:</b> A string up to 256 characters long MLFB(Machine-Readable Product Designation) or order code
rox-release	<b>Synopsis:</b> A string The release of ROX running on the chassis.
system-serial-number	<b>Synopsis:</b> A string up to 32 characters long The system serial number on the chassis label.
Last Integrity Check	<b>Synopsis:</b> A string up to 32 characters long The last time the firmware integrity was checked.
Last Integrity Check Result	<b>Synopsis:</b> A string The result of the last integrity check.
Maintenance Mode Status	<b>Synopsis:</b> A string The maintenance mode status (enabled or disabled).



## 4.2 Viewing Chassis Information and Status

This section describes how to view information about the device chassis, such as its configuration and operating status.

### 4.2.1 Viewing the Slot Hardware

To view a list of the hardware installed in each slot, navigate to the **Hardware** tab under **Administration » System » Chassis**.

The table provides the following information:

Parameter	Description
Slot	<p><b>Synopsis:</b> [ ---   pm1   pm2   main   sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   cm   em   trnk ]</p> <p>The slot name, as marked on the silkscreen across the top of the chassis.</p>
Order Code	<p><b>Synopsis:</b> A string up to 25 characters long</p> <p>The order code of the chassis as derived from the current hardware configuration.</p>
Detected Module	<p><b>Synopsis:</b> A string up to 60 characters long</p> <p>The installed module's type specifier.</p>

### 4.2.2 Viewing Module Information

To view information about the modules installed in the device, navigate to the **System** tab under **Administration » System » Chassis**, and then click **Info**.

The table provides the following information:

Parameter	Description
Detected Module	<p><b>Synopsis:</b> A string up to 60 characters long</p> <p>The installed module's type specifier.</p>
Boot Loader	<p><b>Synopsis:</b> A string</p> <p>The version of the ROX bootloader software on the installed module.</p>
FPGA	<p><b>Synopsis:</b> A string</p> <p>The version of the ROX FPGA firmware (if any) running on the installed module.</p>

### 4.2.3 Viewing Flash Card Storage Utilization

To view the Flash card storage utilization statistics for the Flash card installed in the device, navigate to the **System** tab under **Administration » System » Chassis**, and then click **Storage**.

The table provides the following information:

Parameter	Description
Storage Name	<b>Synopsis:</b> A string between 0 and 32 characters long The type of storage.
Total Capacity (KiB)	<b>Synopsis:</b> An integer between 0 and 4294967295 The total capacity of the flash storage in KB.
Current Partition	<b>Synopsis:</b> A string between 0 and 32 characters long The partition ROX is currently running on and booted from.
Current Partition Capacity (KiB)	<b>Synopsis:</b> An integer between 0 and 4294967295 The capacity of the current partition in KB.
Secondary Partition Capacity (KiB)	<b>Synopsis:</b> An integer between 0 and 4294967295 The capacity of the secondary partition in KB.
Current Partition Usage (%)	<b>Synopsis:</b> An integer between 0 and 100 The %usage of the current partition.
Model Number	<b>Synopsis:</b> A string between 0 and 255 characters long The model number of the storage device.
Serial Number	<b>Synopsis:</b> A string between 0 and 255 characters long The serial number of the storage device.

### 4.2.4 Viewing CPU/RAM Utilization

To view the CPU/RAM utilization statistics for each module installed in the device, navigate to the **System** tab under **Administration » System » Chassis**, and then click **CPU**.

The table provides the following information:

Parameter	Description
Detected Module	<b>Synopsis:</b> A string up to 60 characters long The installed module's type specifier.
CPU Load (%)	<b>Synopsis:</b> An integer between 0 and 100 The CPU load, in percent, on the installed module.

4.2.5 Viewing the Slot Status

Parameter	Description
RAM Avail (%)	<b>Synopsis:</b> An integer between 0 and 100 The proportion of memory (RAM) currently unused, in percent, on the installed module.
RAM Low (%)	<b>Synopsis:</b> An integer between 0 and 100 The lowest proportion of unused memory (RAM), in percent, recorded for the installed module since start-up.

4.2.5 Viewing the Slot Status

To view the overall status of each slot, navigate to the **Slots** tab under **Administration » System » Chassis**, and then click **Slot Status**.

The table provides the following information:

Parameter	Description
Slot	<b>Synopsis:</b> [ ---   pm1   pm2   main   sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   cm   em   trnk ] The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	<b>Synopsis:</b> A string up to 60 characters long The installed module's type specifier.
State	<b>Synopsis:</b> [ unknown   empty   disabled   resetting   operating   failed   disconnected ] The current state of the installed module.
Status	<b>Synopsis:</b> A string The runtime status of the installed module.
Uptime	<b>Synopsis:</b> A string The total time elapsed since the start-up of the installed module.
Start Date	<b>Synopsis:</b> A string The date on which the installed module was started up.
Start Time	<b>Synopsis:</b> A string The time at which the installed module was started up.

4.2.6 Viewing the Slot Sensor Status

To view information about the slot sensors, navigate to the **Slots** tab under **Administration » System » Chassis**, and then click **Slot Sensors**.

The table provides the following information:

Parameter	Description
Slot	<b>Synopsis:</b> [ ---   pm1   pm2   main   sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   cm   em   trnk ]  The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	<b>Synopsis:</b> A string up to 60 characters long  The installed module's type specifier.
Temperature (C)	<b>Synopsis:</b> An integer between -55 and 125  The temperature, in degrees C, of the installed module. If multiple temperature sensors are present on the board, the maximum reading is reported.
Power Supply (mA)	<b>Synopsis:</b> An integer between 0 and 15000  The power supply current, in mA, being drawn by the installed module.
Power Supply (mV)	<b>Synopsis:</b> An integer between 0 and 15000  The power supply voltage, in mV, seen by the installed module.

## 4.2.7 Viewing the Power Controller Status

To view the status of the power controller, navigate to the **System** tab under **Administration » System » Chassis**, and then click **Controller**.


The table provides the following information:

Parameter	Description
PM Slot	<b>Synopsis:</b> [ pm1   pm2 ]  The name of the power module slot as labeled on the chassis.
MOV Protection	<b>Synopsis:</b> [ na   working   damaged ]  The state of the MOV protection circuit. Possible values include: <ul style="list-style-type: none"> <li><b>na</b> – MOV protection is not applicable to the device.</li> <li><b>working</b> – MOV protection is working.</li> <li><b>damaged</b> – The MOV protection fuse is damaged. Contact Siemens Customer Support.</li> </ul>
PM Temperature (C)	<b>Synopsis:</b> An integer between -55 and 125  The temperature (Celsius) inside the power module.
PM Current (mA)	<b>Synopsis:</b> An integer between 0 and 15000  The current (mA) sourced by the power module.

Parameter	Description
PM Voltage (mV)	<b>Synopsis:</b> An integer between 0 and 15000 The voltage (mV) sourced by the power module.

## 4.3 Shutting Down the Device

To shut down the device, do the following:

 <b>NOTICE</b>
<b>Security hazard – risk of unauthorized access and/or exploitation</b>
Always shutdown the device before disconnecting power. Failure to shutdown the device first could result in data corruption.

### Note

The device never enters a permanent shutdown state. When instructed to shutdown, the device shuts down and provides a time-out period during which power can be disconnected from the device. The default time-out period is 300 seconds (five minutes). At the end of the time-out period, the device reboots and restarts.

### Note

If wiring hinders the process of disconnecting power from the device, the power module(s) can be removed instead.

1. Navigate to the **Bootup/Shutdown** tab under **Administration » System**.
2. Under **This command shuts down services...**, click **Perform**.

## 4.4 Rebooting the Device

To reboot the device, do the following:

1. Navigate to the **Bootup/Shutdown** tab under **Administration » System**.
2. Under **Reboot the Device**, click **Perform**.

## 4.5 Restoring Factory Defaults

To restore the factory defaults for the device, do the following:

1. Navigate to the **Restore Factory Defaults** tab under **Administration » System » Configuration Actions**.
2. Click **Perform**. A confirmation dialog box appears. Click **OK** to proceed.
3. Configure the following parameter(s) as required:

Parameter	Description
Delete Logs	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Delete system logs as well as restoring default settings.
Default Both Partitions	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Perform the operation on both partitions.
Delete Saved Configurations	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Delete saved configuration files (works with default-both-partitions option).
Shutdown	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Shutdown rather than reboot after restoring factory defaults.

4. Click **OK**.

## 4.6 Decommissioning the Device

Before taking the device out of service, either permanently or for maintenance by a third-party, make sure the device has been fully decommissioned. This includes removing any sensitive, proprietary information.

### Note

For additional assistance in decommissioning the device , contact Siemens Customer Support.

To decommission the device, do the following:

1. Obtain a copy of the RUGGEDCOM ROX II firmware currently installed on the device. For more information, contact Siemens Customer Support.
2. Log in to maintenance mode. For more information, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".
3. Delete the current boot password/passphrase by typing:

```
rox-delete-bootpwd --force
```
4. Type `exit` and then press **Enter**.
5. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 23).

6. Flash the RUGGEDCOM ROX II firmware obtained in step 1 (Page 59) to the inactive partition and reboot the device. For more information, refer to "Downgrading Software" (Page 90).
7. Repeat step 5 (Page 59) and step 6 (Page 60) to flash the RUGGEDCOM ROX II firmware obtained in step 1 (Page 59) to the other partition and reboot the device.
8. Shut down the device. For more information, refer to "Shutting Down the Device" (Page 58).

**⚠ NOTICE****Security hazard – risk of data exploitation**

Regardless of the erasure tool or method employed, even following multiple rounds of flashing, erasure, or overwriting, residual data may still be present on Flash-based storage media. To guarantee the destruction of all sensitive data persisting on the unit, physical destruction of the storage media/platform may be required.

## 4.7 Managing Feature Keys

Feature keys expand the capabilities of RUGGEDCOM ROX II on a device by adding a feature level. This may include VLANs (802.1Q), QoS (802.1p), broadcast storm filtering, port mirroring, etc.

For a full list of available feature keys, refer to "Feature Keys" (Page 6). Further information is also available through <https://www.siemens.com> or a Siemens Sales representative.

---

**Note****Ordering Feature Keys**

When ordering feature keys, make sure to provide the *main* serial number and *cm* serial number for the device. An upgraded feature key file will be provided that is licensed to the device.

For information about how to determine the *main* serial number and *cm* serial number, refer to "Displaying Device and Software Information" (Page 53).

---

### 4.7.1 Installing Feature Keys

When a feature key is installed, RUGGEDCOM ROX II evaluates the key and enables the most capable feature level described by the key.

Feature keys can be installed via a remote host or removable media (i.e. compact flash card or USB Mass Storage drive).

## Installing From a Remote Host

1. Obtain the following information:
  - The file name of the feature key
  - The user name and password required to log into the remote host where the feature key is stored
  - The name or IP address of the host where the feature key is stored
2. Navigate to **Tools » CLI** and then click **Start**.
3. [Optional] Click **Pop Out** to open the console in a separate dialog box.
4. Install the feature key by typing:

```
file scp-featurekey-from-url { username }@{ host }:/
{ path }/{ current-filename }{ new-filename }
```

Where:

- { username } is the name of a user who can log into the computer where the feature key file is stored.
- { host } is the hostname or IP address of the computer where the feature key file is stored.
- { path } is the directory path to the feature key file in the host computer.
- { current-filename } is the current name of the feature key file.
- { new-filename } is the new name of the feature key file on the device. This parameter is optional. The current filename will be used if a new filename is not provided.

For example:

```
file scp-featurekey-from-url wsmith@10.200.10.39:/files/keys/L3SE_cm
RUMHD06096338.key L3SE_cmRUMHD06096338.key
```

5. When prompted, type the user's password and then press **Enter**. The system uploads the feature key file:

```
ruggedcom# file scp-featurekey-from-url wsmith@10.200.20.39:/files/keys/
L3SE_cmRUMHD06096338.key L3SE_cmRUMHD06096338.key
wsmith@10.200.20.39's password:
L3SE_cmRUMHD06096338.key          100% 192      0.2KB/s   00:00
```

## Installing From Removable Media

For instructions about installing a feature key from removable media (i.e. compact flash card or USB flash drive), refer to "Installing Files" (Page 62).

## 4.8 Managing Files


RUGGEDCOM ROX II allows the transfer of select files to and from the device using the following methods:



- **Install**  
Allows users to upload files from a PC, a USB flash drive or from a remote server using a file transfer protocol, such as FTP.
- **Backup**  
Allows users to download files to a PC, a USB flash drive or to a remote server using a file transfer protocol, such as FTP.

### 4.8.1 Installing Files

To install a file on the device, such as a configuration file or feature key, do the following:

 <b>NOTICE</b> RUGGEDCOM ROX II only accepts configuration files from devices with the same hardware profile running the same software version. It is recommended to only load configuration files from the same device.
--

1. If the source of the file is a USB Mass Storage drive, insert the drive in the USB port on the device. For more information, refer to the "RUGGEDCOM RX5000/MX5000/MX5000RE Installation Manual".
2. Navigate to the **Install Files** tab under **Administration » System » File Actions**.
3. Under **File Location Type**, select **URL** or **File** depending on the source.
4. If **URL** is selected as the file location type, configure the following parameters:

**Note**

RUGGEDCOM ROX II supports implicit FTP over TLS (FTPS) URLs. Explicit FTP over TLS is not supported.

**Note**

For SFTP transfers, the SFTP server's public key must be added as a Known Host. For more information, refer to "Managing Known Hosts" (Page 185).

Parameter	Description
file-type	<p><b>Synopsis:</b> [ config   featurekey   vmfile ]</p> <p>The file types to be copied.</p>
url	<p><b>Synopsis:</b> A string between 1 and 1024 characters long</p> <p>The URL of the ROX II file to copy. Supported URIs are HTTP, SCP, SFTP, FTPS and FTP.</p> <p>To install from a USB flash drive or microSD card (if applicable), the URL format is "usb://{ usb-device-name }/path-to-file-on-system" or "sd://{sd-1}/path-to-file-on-system". Run "show chassis" to determine the name of the USB device. Note that only one single partition is supported for either data medium.</p>

Parameter	Description
	For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If "port" is not specified, the default port for the protocol is used.

5. If **File** is selected as the file location type, do the following:
  - a. Click the **Select** button. The **File Upload** dialog box appears.
  - b. Select the desired file and click **Open**.
6. Click **Perform** to install the file.
7. If the VPE feature key (VIRTUALM) was installed, reboot the device to reveal the virtualization features. For more information, refer to "Rebooting the Device" (Page 58).

## 4.8.2 Backing Up Files

To backup files stored on the device, do the following:

1. If the file's destination is a USB Mass Storage drive, insert the drive in the USB port on the device. For more information, refer to the "RUGGEDCOM RX5000/MX5000/MX5000RE Installation Manual".
2. Navigate to the **Backup Files** tab under **Administration » System » File Actions**.
3. Under **File Location Type**, select **URL** or **File** depending on the destination.
4. If **URL** is selected as the file location type, configure the following parameters:

---

### Note

RUGGEDCOM ROX II supports implicit FTP over TLS (FTPS) URLs. Explicit FTP over TLS is not supported.

---

### Note

For SFTP transfers, the SFTP server's public key must be added as a Known Host. For more information, refer to "Managing Known Hosts" (Page 185).

---

Parameter	Description
file-type	<b>Synopsis:</b> [ config   featurekey   logfiles   rollbacks   licenses   logarchive ]  The file types to copy.
file	<b>Synopsis:</b> A string between 1 and 255 characters long  The name of the logarchive or a list of file names to copy. For logarchive, only 1 file name is accepted to name the tar-archive that will be used to backup of the entire /var/log directory. The archive is created in /tmp directory and will be automatically deleted.

Parameter	Description
timestamp	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>If enabled, a time stamp will be appended to the file name. This option is not applicable to file names that contain '*'.</p>
url	<p><b>Synopsis:</b> A string between 1 and 1024 characters long</p> <p>The URL of the ROX II file to copy. Supported URIs are HTTP, SCP, SFTP, FTPS and FTP.</p> <p>To save to a USB flash drive or microSD card (if applicable), the URL format is "usb://{ usb-device-name }/path-to-file" or "sd://sd-1//path-to-file". Run "show chassis" to determine the name of the USB device. Note that only one single partition is supported for either data medium.</p> <p>For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If using a path only, close it with '/'. If "port" is not specified, the default port for the protocol is used.</p>

5. If **File** is selected as the file location type, under **File**, select the type of file to download from the device. Files of that type, if available, are automatically listed.
6. Click **Perform**.

## 4.9 Managing Logs

RUGGEDCOM ROX II maintains various logs to record information about important events. Each log falls into one of the following log types:

<b>Security Event Logs</b>	<p>Information related to the following security events are logged by RUGGEDCOM ROX II:</p> <hr/> <p><b>Note</b></p> <p>Passwords can be retried up to 3 times before the login attempt is considered a security event.</p> <hr/> <ul style="list-style-type: none"> <li>• Successful and unsuccessful login attempts</li> <li>• Local and remote (RADIUS) authentication</li> <li>• Security-sensitive commands (whether successful or unsuccessful)</li> <li>• An optionally configurable SNMP Authentication Failure Trap (disabled by default) in accordance with SNMPv2-MIB</li> </ul> <p>All security event logs are recorded in <b>var/log/auth.log</b> and can be viewed in the Authlog Viewer. For more information about viewing logs, refer to "Viewing Logs" (Page 65).</p>
<b>Syslogs</b>	<p>Syslog allows users to configure local and remote syslog connections to record important, non-security event information. The remote Syslog protocol, defined in <a href="http://tools.ietf.org/html/rfc3164">RFC 3164</a> [<a href="http://tools.ietf.org/html/rfc3164">http://tools.ietf.org/html/rfc3164</a>], is a UDP/IP-based transport that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog</p>

	<p>servers. The protocol is designed to simply transport these event messages from the generating device to the collector.</p> <p>All log files are organized in the log directory (<b>/var/log</b>) according to the facility and priority at which they have been logged. Remote Syslog sends the requested logs to the remote server(s) at whichever facility and priority they were initially logged, after filtering the logs based on the selectors configured for the server.</p> <p>The following log files are setup with the following default selectors:</p> <ul style="list-style-type: none"> <li>• <b>syslog</b> catches all logs except <code>daemon.debug</code>, <code>auth</code> or <code>authpriv</code> logs</li> <li>• <b>daemon.log</b> catches all <i>err</i> level (and above) logs written to the <code>daemon</code> facility</li> <li>• <b>messages</b> catches all <i>info</i>, <i>notice</i> and <i>warn</i> level logs for all facilities except <code>auth</code>, <code>authpriv</code>, <code>cron</code>, <code>daemon</code>, <code>mail</code> and <code>news</code></li> </ul> <p>A selector setup using the following facilities at level <i>info</i> and up is recommended:</p> <ul style="list-style-type: none"> <li>• <code>daemon</code></li> <li>• <code>user</code></li> <li>• <code>kern</code></li> <li>• <code>syslog</code></li> </ul>
<b>Diagnostic Logs</b>	Diagnostic logs record system information for the purposes of troubleshooting.

## 4.9.1 Viewing Logs

Select logs can be viewed directly within the Web interface. Otherwise, these and other logs can be downloaded from the device and viewed in a text editor/viewer.

### Note

For information about downloading log files from the device, refer to "Backing Up Files" (Page 63).

To view a log in the Web interface, do the following:

1. Navigate to **Tools » Log Viewers**. The **Log Viewers** form appears.
2. Under **Log information**, select the log information to display:

<b>Message</b>	Displays all events from <b>/var/log/messages</b>
<b>Syslog</b>	Displays syslog events from <b>/var/log/syslog</b>
<b>Authlog</b>	Displays authentication events from <b>/var/log/auth.log</b>
<b>Layer 2 log</b>	Displays Layer 2 events from <b>/var/log/layer2</b>
<b>Kernlog</b>	Displays kernel events from <b>/var/log/kern.log</b>

3. [Optional] Under **Click to start/stop log viewer**, click **Start**. The selected log appears.

To control the content and appearance of the log, do the following:

- Enter a number in the **Last number of lines** box to control the number of lines displayed

- Enter a number, word or phrase in the **Filter text** box then click **Apply** to show only lines that contain the specified text
- Click **Pop Out** to display the log in a separate dialog box.
- Under **Click to enable autoscroll**, select **Enabled** to allow auto scrolling.


### 4.9.2 Deleting Logs

To delete all logs stored on the device, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **Delete Log Files**, click **Perform**.

### 4.9.3 Configuring Secure Remote Syslog

Secure remote syslog encrypts all system logs sent to syslog servers using an Secure Sockets Layer (SSL) certificate signed by a Certified Authority (CA).

 <b>NOTICE</b>
The client (RUGGEDCOM ROX II) and server certificates must be signed by the same CA.

#### 4.9.3.1 Enabling/Disabling Secure Remote Syslog

To configure a specific source IP address for all remote syslog messages, do the following:

1. Navigate to the **System Remote Log** tab under **Administration » System » logging**.


---

#### Note

Once secure remote system logging is enabled and a remote syslog server is configured, TCP port 6514 is automatically opened.

---

2. Under **Secure Remote Syslog**, click **Enabled** to enable secure remote syslog, or clear the check box to disable secure remote syslog.

 <b>NOTICE</b>
All certificates must meet the following requirements: <ul style="list-style-type: none"><li>• X.509 v3 digital certificate format</li><li>• PEM format</li><li>• RSA key pair, 512 to 2048 bits in length</li></ul>

3. If secure remote syslog is enabled, specify a certificate to use for authentication with remote syslog server. If the desired certificate is not listed, add it. For more information, refer to "Adding a Certificate" (Page 184).
4. [Optional] Define one or more match patterns or *permitted peers*. Permitted peers compare the server's host name to the common name defined in the SSL certificate. For more information, refer to "Adding a Permitted Peer" (Page 67).
5. Commit the changes.

#### 4.9.3.2 Viewing a List of Permitted Peers

To view a list of permitted peers, navigate to the **System Remote Log** tab under **Administration » System » logging**. If permitted peers have been configured, the **Permitted Peer Pattern** table appears.

If no permitted peers have been configured, add peers as needed. For more information, refer to "Adding a Permitted Peer" (Page 67).

#### 4.9.3.3 Adding a Permitted Peer

To add a permitted peer for secure remote syslog, do the following:

1. Navigate to the **System Remote Log** tab under **Administration » System » Logging**, and then click **Add Entry**.
2. Configure the following parameter(s) as required:

Parameter	Description
Permitted Peer Pattern	<b>Synopsis:</b> A string between 1 and 255 characters long Patterns used to match peer common name.

3. Commit the change.

#### 4.9.3.4 Deleting a Permitted Peer

To delete a permitted peer for secure remote syslog, do the following:

1. Navigate to the **System Remote Log** tab under **Administration » System » Logging**. The **Permitted Peers** table appears.
2. Select the peer to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 4.9.3.5 Configuring a Source IP Address for Remote Syslog Messages

IP packets for remote syslog messages include a destination IP address and a source IP address. The source IP address is the interface from which the message is sent (e.g. switch.0001). However, that address may not be meaningful within the system log, or the address may conflict with a firewall rule or policy. In such cases, an alternative source IP address can be configured for all remote syslog messages.

To configure a specific source IP address for all remote syslog messages, do the following:

1. Make sure an IP address is first defined for the desired interface. For more information, refer to either "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).
2. Navigate to the **Remote Logging** tab under **Administration » System » Logging**.
3. Under **Source IP**, type the alternative source IP address.
4. Commit the change.

## 4.9.4 Managing Diagnostic Logs

Diagnostic logs are available for troubleshooting the device. Various device behavior is recorded in the following logs:

Log	Filename
Developer's Log	<code>/var/log/confd-dev.log</code>
SNMP Log	<code>/var/log/snmp-trace.log</code>
NETCONF Summary Log	<code>/var/log/netconf.log</code>
NETCONF Trace Log	<code>/var/log/netconf-trace.log</code>
XPATH Trace Log	<code>/var/log/xpath-trace.log</code>
WebUI Trace Log	<code>/var/log/webui-trace.log</code>

### NOTICE

#### Configuration hazard – risk of reduced performance

Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

### 4.9.4.1 Enabling/Disabling the Developer's Log

The Developer's log records internal system transactions from the operational view.

**⚠ NOTICE****Configuration hazard – risk of reduced performance**

Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

To enable or disable the Developer's log, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **Developer Log** and **Developer Log Level**, configure the following parameter(s) as required:

Parameter	Description
Developer Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/Disables developer logging to the confd-dev.log.</p>
Developer Log Level	<p><b>Synopsis:</b> [ error   info   trace ]</p> <p><b>Default:</b> info</p> <p>Sets the verbosity level for developer logging.</p>

3. Commit the changes.

#### 4.9.4.2 Enabling/Disabling the SNMP Log

The SNMP log records all SNMP related events.

**⚠ NOTICE****Configuration hazard – risk of reduced performance**

Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

To enable or disable the SNMP log, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **SNMP Log**, configure the following parameter(s) as required:

Parameter	Description
SNMP Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/Disables SNMP logging to the snmp-trace.log.</p>

3. Commit the change.



### 4.9.4.3 Enabling/Disabling the NETCONF Summary Log

The NETCONF summary log briefly records NETCONF protocol transactions and, in particular, those which completed successfully. For example:

```
.
.
.
<INFO> 5-Apr-2012::04:26:33.877 ruggedcom confd[2098]: netconf id=9450 new ssh
session for user "admin" from 192.168.0.10
<INFO> 5-Apr-2012::04:27:03.574 ruggedcom confd[2098]: netconf id=9450 got rpc:
{urn:ietf:params:xml:ns:netconf:base:1.0}validate attrs: message-id="103"
<INFO> 5-Apr-2012::04:27:04.167 ruggedcom confd[2098]: netconf id=9450 validate
source=candidate attrs: message-id="103"
<INFO> 5-Apr-2012::04:27:06.691 ruggedcom confd[2098]: netconf id=9450 sending
rpc-reply, attrs: message-id="103"
.
.
.
```

#### NOTICE

##### Configuration hazard – risk of reduced performance

Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

To enable or disable the NETCONF Summary log, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **NETCONF Summary Log**, configure the following parameter(s) as required:

Parameter	Description
NETCONF Summary Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/Disables NETCONF logging to the netconf.log.</p>

3. Commit the change.

### 4.9.4.4 Enabling/Disabling the NETCONF Trace Log

The NETCONF trace log records the text of each NETCONF XML message received by and sent from the device. Each entry includes the NETCONF session identifier and the full text of the XML message. If the session identifier is followed by the word *read*, the XML message was received by the device. The word *write* indicates the XML message was sent by the device. For example:

```
.
.
.
**> sess:9450 read:
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="103">
  <validate>
  <source>
```

```

    <running/>
  </source>
</validate>
</rpc>

**< sess:9450 write:
<rpc-reply message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
.
.
.

```

### NOTICE

#### Configuration hazard – risk of reduced performance

Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

To enable or disable the NETCONF Trace log, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **NETCONF Trace Log**, configure the following parameter(s) as required:

Parameter	Description
NETCONF Trace Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables NETCONF Trace logging to netconf-trace.log.</p>

3. Commit the change.

#### 4.9.4.5 Enabling/Disabling the XPATH Trace Log

The XPATH trace log records internal events related to XPATH routines that require interaction with an XPATH component.

### NOTICE

#### Configuration hazard – risk of reduced performance

Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

To enable or disable the XPATH Trace log, do the following:


1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **XPATH Trace Log**, configure the following parameter(s) as required:

Parameter	Description
XPATH Summary Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables XPATH Trace logging to the xpath-trace.log.</p>

3. Commit the change.

#### 4.9.4.6 Enabling/Disabling the WebUI Trace Log

The WebUI trace log records all transactions related to the Web interface, such as configuration changes, error messages, etc.

<p> <b>NOTICE</b></p> <p><b>Configuration hazard – risk of reduced performance</b></p> <p>Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.</p>
--

To enable or disable the WebUI Trace log, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **WebUI Trace Log**, configure the following parameter(s) as required:

Parameter	Description
WebUI Trace Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables WebUI Trace logging to the webui-trace.log.</p>

3. Commit the change.

#### 4.9.4.7 Enabling/Disabling the JSON-PRC Log

The JSON-PRC log records all JSON-PRC traffic information.

To enable or disable the JSON-PRC log, do the following:

1. Navigate to the **Diagnostics** tab under **Administration » System » Logging**.
2. Under **JSONRPC Log**, configure the following parameter(s) as required:

Parameter	Description
JSONRPC Log	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/Disables JSON-RPC traffic logging to jsonrpc.log.</p>

3. Commit the change.

## 4.9.5 Managing Remote Syslog Servers

RUGGEDCOM ROX II can support up to 6 event message collectors, or remote Syslog servers. Remote Syslog provides the ability to configure:

- IP address(es) of collector(s)
- Event filtering for each collector based on the event severity level

### 4.9.5.1 Viewing a List of Remote Servers

To view a list of remote servers, navigate to the **Server** tab under **Administration » System » Logging**. If remote servers have been configured, the **Remote Server** table appears.

If no remote servers have been configured, add servers as needed. For more information, refer to "Adding a Remote Server" (Page 73).

### 4.9.5.2 Adding a Remote Server

To add a remote server, do the following:

1. Navigate to the **Server** tab under **Administration » System » Logging**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Server IP Address	<b>Synopsis:</b> A string between 1 and 253 characters long  The IPv4 address of a logging server. Up to 8 logging servers can be added.

4. Click **OK**. The **Remote Server - { server name }** form appears.
5. Configure the following parameter(s) as required:

Parameter	Description
Enable	Enables/disables the feed to the remote logging server.
Transport Protocol	<b>Synopsis:</b> [ udp   tcp ] <b>Default:</b> udp  TCP or UDP.
Monitor Interface	<b>Synopsis:</b> A string  The interface to monitor. If the IP address is changed on the interface, the logging daemon will restart.

Parameter	Description
Port	<p><b>Synopsis:</b> An integer between 1 and 65535</p> <p><b>Default:</b> 514</p> <p>Port number.</p>

6. Configure one or more selectors for the server. For more information, refer to "Adding a Remote Server Selector" (Page 74).
7. Commit the changes.

#### 4.9.5.3 Deleting a Remote Server

To delete a remote server, do the following:

1. Navigate to the **Server** tab under **Administration » System » Logging**. The **Remote Server** table appears.
2. Click **Delete Entry** next to the chosen remote server.
3. Commit the change.

### 4.9.6 Managing Remote Server Selectors

Remote server selectors filter the information sent to specific servers.

#### 4.9.6.1 Viewing a List of Remote Server Selectors

To view a list of remote server selectors, do the following:

1. Navigate to the **Server** tab under **Administration » System » Logging**.
2. Select a remote server, and then click **Selector**. If remote server selectors have been configured, the **Selector** table appears.

If no remote server selectors have been configured, add selectors as needed. For more information, refer to "Adding a Remote Server Selector" (Page 74).

#### 4.9.6.2 Adding a Remote Server Selector

To add a remote server selector, do the following:

1. Navigate to the **Server** tab under **Administration » System » Logging**.
2. Select a remote server, and then click **Selector**. The **Selector** form appears.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> An integer</p> <p>The log selector identifier. Enter an integer greater than 0; up to 8 selectors can be added. The log selector determines which subsystem messages are included in the log.</p>

- Click **OK**. The **Selector for Remote Server - { server name }** form appears.
- Configure the following parameter(s) as required:

Parameter	Description
Negate	<p>Excludes messages defined in the <b>Remote Server Selector</b> fields from the log. Selecting this option acts as a logical NOT for the selector definition.</p> <p>For example: Selecting <b>same</b>, <b>debug</b>, and <b>mail</b> in the <b>Comparison</b>, <b>Level</b>, and <b>Facility-list</b> fields includes debug messages from the mail subsystem in the log. Selecting <b>Negate</b> <b>excludes</b> debug messages from the mail subsystem from the log.</p>
Comparison	<p><b>Synopsis:</b> [ same_or_higher   same ]</p> <p><b>Default:</b> same_or_higher</p> <p>The message severity levels to include in the log:</p> <ul style="list-style-type: none"> <li><b>same:</b> includes only messages of the severity level selected in the <b>Level</b> field.</li> <li><b>same_or_higher:</b> includes messages of the severity level selected in the <b>Level</b> field, and all messages of higher severity.</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>Selecting <b>debug</b> in the <b>Level</b> field and <b>same</b> in the <b>Comparison</b> field includes only debug messages in the log.</li> <li>Selecting <b>debug</b> in the <b>Level</b> field and <b>same_or_higher</b> in the <b>Comparison</b> field includes debug and all higher severity messages in the log.</li> </ul>
Level	<p><b>Synopsis:</b> [ emerg   alert   crit   err   warning   notice   info   debug   none   all ]</p> <p><b>Default:</b> all</p> <p>The base message severity level to include in the log. <b>all</b> includes all messages. <b>none</b> excludes all messages. Other levels are listed in order of increasing severity.</p>
Facility List	<p><b>Synopsis:</b> [ auth   authpriv   cron   daemon   ftp   kern   lpr   mail   news   security   syslog   user   uucp   local0   local1   local2   local3   local4   local5   local6   local7   all ]</p> <p>The subsystems generating log messages. Messages from the selected subsystems are included in the log. At least one subsystem must be selected; up to 8 subsystems can be selected.</p>

- Commit the changes.

### 4.9.6.3 Deleting a Remote Server Selector

To delete a remote server selector, do the following:

1. Navigate to the **Server** tab under **Administration » System » Logging**.
2. Select a remote server, and then click **Selector**.
3. Click **Delete** next to the chosen remote server selector.
4. Commit the change.

## 4.10 Managing the Software Configuration

Configuration parameters for RUGGEDCOM ROX II can be saved on the device and loaded in the future.

### 4.10.1 Backing Up the Software Configuration

To recover from unexpected device failures quickly, it is important to backup the software configuration on a regular basis. This can be done manually by saving the configuration to a microSD/SDHC card or a remote server. It can also be done using the job scheduler, RUGGEDCOM NMS or SINEC NMS, or a separate utility, such as Ansible.

The following is an example of a job created through the CLI with RUGGEDCOM ROX II's job scheduler. This job backs up the software configuration locally and to a remote SFTP server every 24 hours.

```
admin
scheduler
  scheduled-jobs backup-config
    job-minute 13
    job-hour 14
    job-command "admin backup-files file-type config file test.cfg url sftp://
user:password@192.168.0.100/home/user/Documents/configs/"
  !
  scheduled-jobs save-config
    job-minute 12
    job-hour 14
    job-command "admin full-configuration-save format cli file-name test.cfg"
```

For information about using the job scheduler, refer to "Scheduling Jobs" (Page 123).

For information about backing up the software configuration manually, refer to "Saving the Configuration" (Page 77).

For all other methods, refer to the product's user documentation.

## 4.10.2 Saving the Configuration

The device configuration can be saved locally on the device (to be transferred later), to a USB Mass Storage device, or to a remote server.

To save the configuration settings, do the following:

### Saving the Configuration On the Device

1. Navigate to the **Load/Save** tab under **Administration » System » Configuration Actions**.
2. Click **Perform**. A confirmation dialog box appears. Click **OK** to proceed.
3. Under **Full Configuration Save**, configure the following parameters:

Parameter	Description
Format	<b>Synopsis:</b> [ cli ] Save full configuration to a file.
File Name	<b>Synopsis:</b> A string between 1 and 255 characters long

4. Click **Perform**.
5. [Optional] Backup the configuration file to a USB mass storage drive. For more information, refer to "Backing Up Files" (Page 63).
6. Click **OK**.
7. [Optional] Backup the configuration file to a USB mass storage drive. For more information, refer to "Backing Up Files" (Page 63).

### Saving the Configuration to a USB Mass Storage Device

To save the configuration to a USB Mass Storage device, do the following:


1. Navigate to the **Load/Save** tab under **Administration » System » Configuration Actions**.
2. Under **Save Configuration to Removable Drive**, do the following:
  - a. [Optional] Under **File Name**, enter a file name for the saved configuration with the extension **\*.cli**.  
  
The default file name is **autoload-config.cli**. This file name is recognized by RUGGEDCOM ROX II as a configuration that can be automatically loaded following a reboot, if the feature is enabled.  
  
For more information about automatically loading a saved configuration, refer to "Managing Automatic Configuration Loading" (Page 78).
  - b. [Optional] Under **Allow Overwrite**, select **Enabled** to overwrite any files on the storage device that have the same name as the new file.  
  
By default, this option is disabled. An error will occur if a file with the same file name exists on the storage device.



- c. Under **Save the Configuration to the Removable Drive**, click **Perform**. The current configuration will be saved to the storage device with the selected file name.

### 4.10.3 Loading a Configuration

To load a configuration file for RUGGEDCOM ROX II, do the following:

 <b>NOTICE</b>
RUGGEDCOM ROX II only accepts configuration files from devices with the same hardware profile running the same software version. It is recommended to only load configuration files from the same device.

1. [Optional] Install the configuration file on the device. For more information, refer to "Installing Files" (Page 62).
2. Navigate to the **Load/Save** tab under **Administration » System » Configuration Actions**.
3. Under **Full Configuration Load**, configure the following parameters:

Parameter	Description
Format	<b>Synopsis:</b> [ cli ] Load a full configuration from a file
File Name	<b>Synopsis:</b> A string between 1 and 255 characters long

4. Click **Perform**.

### 4.10.4 Managing Automatic Configuration Loading

RUGGEDCOM ROX II supports automatic loading of a configuration file via a USB Mass Storage device, following a reboot of the device.

Configurations can be created and modified on a PC, or saved from one device onto a USB Mass Storage device, then loaded onto another device or devices as needed. Saved configurations can also be loaded onto new devices to replace factory default settings.

#### 4.10.4.1 Enabling/Disabling Automatic Configuration Loading

To enable or disable the automatic configuration loading feature, do the following:

1. Navigate to the **Bootup/Shutdown** tab under **Administration » System**.
2. Under **Automatic Configuration Load from Removable Drive**, configure the following parameter(s) as required:

Parameter	Description
Automatic configuration load from removable drive	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables automatic loading of a configuration file from a connected removable drive, during startup</p>

3. Commit the change.

#### 4.10.4.2 Automatically Loading a Configuration File from a Removable Drive

A configuration file can be saved to a USB Mass Storage device and automatically loaded to an existing device. The loaded configuration will replace the existing configuration following a reboot.

##### Note

For more information about supported file systems in RUGGEDCOM ROX II, refer to "Removable Memory" (Page 16).

To automatically load a configuration file from a USB Mass Storage device following a reboot, do the following:

1. Enable automatic configuration loading on the target device. For more information, refer to "Enabling/Disabling Automatic Configuration Loading" (Page 78).
2. Create a configuration file from a PC or the desired source device. Name the file *autoload-config.cli*. For more information, refer to "Saving the Configuration" (Page 77).
3. Copy the configuration file to the removable drive. For more information, refer to "Backing Up Files" (Page 63).

##### NOTICE

If the Automatic Configuration Load feature is not enabled, the loading of any Auto-Load Configuration File found on the removable drive will not occur, and the RUGGEDCOM ROX II device will continue with its normal startup.

4. Insert the USB Mass Storage drive into the USB port on the target device. For more information, refer to the "RUGGEDCOM RX5000/MX5000/MX5000RE Installation Manual".
5. Reboot the target device. For more information about rebooting, refer to "Rebooting the Device" (Page 58).

The auto-loaded configuration file is loaded to the device.

#### 4.10.4.3 Overriding Factory Settings Using a Removable Drive

A configuration file can be saved to a USB Mass Storage device and automatically loaded to a new device. The loaded configuration will replace the factory default configuration following the initial boot.

---

##### Note

This procedure applies to the initial boot only. For information about loading the configuration from a USB Mass Storage device after the initial boot, refer to "Automatically Loading a Configuration File from a Removable Drive" (Page 79).

---

##### Note

For more information about supported file systems in RUGGEDCOM ROX II, refer to "Removable Memory" (Page 16).

---

To automatically override factory settings using a removable drive, do the following:

1. Create a configuration file from a PC or the desired source device (i.e. another RUGGEDCOM ROX II device). Name the file *autoload-config.cli*. For more information, refer to "Saving the Configuration" (Page 77).
2. Copy the configuration file to the removable drive. For more information, refer to "Backing Up Files" (Page 63).
3. Insert the USB Mass Storage drive into the USB port on the device. For more information, refer to the "RUGGEDCOM RX5000/MX5000/MX5000RE Installation Manual".
4. Start up and connect to the target device. For more information about connecting to the device, refer to "Connecting to RUGGEDCOM ROX II" (Page 49).

The auto-loaded configuration file is loaded to the device.

#### 4.10.4.4 Deleting an Automatic Configuration File

To remove an **autoconfig.cli** from a USB Mass Storage device, do the following:

1. Insert the USB Mass Storage device into the device. For more information, refer to the "RUGGEDCOM RX5000/MX5000/MX5000RE Installation Manual".
2. Navigate to the **Load/Save** tab under **Administration » System » Configuration Actions**.
3. Under **Delete Autoload Configuration from Removable Drive**, click **Perform**. The file **autoload-config.cli** is removed from the storage device.

### 4.11 Managing Upgrade Servers

RUGGEDCOM ROX II can be configured to retrieve software packages from a centralized upgrade server.

### 4.11.1 Understanding Upgrade Servers

Upgrade servers must meet the following requirements:

- The server must act as a Web server or FTP server, and be accessible to the device.
- The server must have sufficient disk space for at least two full software releases. Each full software release is approximately 102 MB, although most upgrades are typically much smaller.
- The server must have sufficient bandwidth. The bandwidth requirements will be based on the number of devices, the size of the upgrade, and when the devices launch an upgrade. The bandwidth is also limited by default for each device to 500 kbps. A modest (e.g. 486 class machine) Web server should be able to serve files up to the limit of the network interface bandwidth.
- The server must be able to accept at least as many HTTP, HTTPS, FTP, FTPS, or SFTP connections as there are devices on the network.
- The server must contain and publish a directory specifically for RUGGEDCOM ROX II software releases. The name of this directory will be specified in the upgrade settings for each device.
- Communication between the server and the device must be on a secure channel, such as IPsec.
- For upgrades via HTTPS, the server's public key must be signed by a trusted Certificate Authority (CA). A list of recognized CA's is available under **`/etc/ssl/certs/`**, which can be accessed via the CLI. For more information about viewing the contents of a file via the CLI, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".

---

#### Note

It is recommended to configure each device to upgrade at different times to minimize impact on the network. A large upgrade (or a low bandwidth limiting value on each device) may cause all devices to upgrade at the same time.

---

### 4.11.2 Configuring the Upgrade Server

For RUGGEDCOM ROX II to properly retrieve files from an upgrade server, the following must be configured on the server:

- **MIME Types**  
The following MIME types must be defined for the chosen upgrade server (e.g. Microsoft IIS Manager, Apache HTTP Server, Lighttpd, etc.) for RUGGEDCOM ROX II to properly retrieve files from the server:
  - `application/x-bzip2`
  - `text/plain`

RUGGEDCOM ROX II software and application upgrades/installations may fail if these MIME types or not configured.

- **Enable Double-Escaping**  
**Only required for firmware versions lower than RUGGEDCOM ROX II v2.14.0.** Double-escaping allows special double-encoded characters, such as +, % and &, in a URI. As some files in RUGGEDCOM ROX II upgrade/downgrade packages may contain a + sign in their file names, double-escaping must be enabled for the upgrade server. If double-escaping is not enabled, some files will be un-retrievable and the upgrade will fail.  
  
In the case of Microsoft's Internet Information Services (IIS) Manager, double-escaping is enabled by setting the **allowDoubleEscaping** attribute in **web.config** to **true**.

```
<system.webServer>  
  <security>  
    <requestFiltering allowDoubleEscaping="true" />  
  </security>  
</system.webServer>
```

For more information about configuring MIME types and double-escaping for the upgrade server, consult the product's user documentation.

## 4.12 Managing Software Versions

RUGGEDCOM ROX II uses a dual partition system to upgrade or downgrade (rollback) the system software while allowing the device to continue operating on the network.

Software can be installed directly on the device using removable media or remotely over the network via an upgrade server.

---

### Note

If upgrading from a previous release of RUGGEDCOM ROX II to v2.16, refer to the documentation for the release that is currently installed on the device. **The following instructions only describe how to upgrade from RUGGEDCOM ROX II v2.16 to a newer version.**

---

### NOTICE

#### Restrictions/Requirements

Restrictions/requirements may apply when upgrading/downgrading to a newer or older software version. Before installing a different version of RUGGEDCOM ROX II, check the **Firmware Download** announcement for the target software release.

For a list of **Firmware Download** announcements for RUGGEDCOM ROX II, visit <https://support.industry.siemens.com/cs/search?search=rox&type=Download>.

If an announcement is not available for the target software version, contact Siemens Customer Support.

### 4.12.1 Understanding Upgrades/Downgrades

Software upgrades are managed between two partitions. The active (or primary) partition contains the software version currently used by the device. The inactive (or secondary) partition contains an inactive version of RUGGEDCOM ROX II.

When upgrading or downgrading to a different version of RUGGEDCOM ROX II, the target software is uploaded to the inactive partition. Any software image already installed on the inactive partition is automatically replaced by the target software image.

Following a successful reboot, which is part of the upgrade/downgrade process, the inactive partition is made the active partition. The previous version of RUGGEDCOM ROX II is on the inactive partition. This mechanism allows the device to remain operational on the network while the upgrade/downgrade process takes place. It also allows users to revert to the previous version if needed.

---

#### Note

In the case of a software upgrade, the configuration and feature keys from the active partition are also copied to the inactive partition.

---

### 4.12.2 Upgrading/Downgrading Software

 <b>NOTICE</b>
<b>Restriction</b>
Downgrading to a version lower than v2.16.0 is not permitted.

When upgrading the software, alternative methods are available that either retain the current device configuration or reset the configuration to factory defaults.

 <b>NOTICE</b>
<b>Upgrade/downgrade paths</b>
Directly upgrading or downgrading the current software to a specific release may not be possible due to potential changes to the RUGGEDCOM ROX II system architecture at key release points. Depending on the software release to be installed, one or more intermediary releases may need to be installed.
For details about upgrade and downgrade paths, refer to the FAQ " <a href="https://support.industry.siemens.com/cs/us/en/view/109806037">How to determine the software upgrade/downgrade path for a RUGGEDCOM ROX II device?</a> ".

---

#### Note

The software upgrade/downgrade process is backwards compatible with select upgrade commands from previous RUGGEDCOM ROX II releases. This allows users to continue using any custom scripts or third-party software they have used previously. If compatibility issues occur, contact Siemens Customer Support.

---

#### 4.12.2.1 Determining the Current Software Partition and Version

To determine which software partition is active and which version of RUGGEDCOM ROX II is running, navigate to the **Monitor** tab under **Administration » Firmware Management**.

The following information is displayed:

Parameter	Description
Software Partition	<b>Synopsis:</b> A string up to 31 characters long The active partition. ROXflash is always performed on the other partition.
Current Version	<b>Synopsis:</b> A string up to 31 characters long The operating software version on the current software partition.

#### 4.12.2.2 Obtaining a Software Release

Valid software releases are available online via [Siemens Industry Online Support \(SIOS\)](https://support.industry.siemens.com) [https://support.industry.siemens.com] or through Siemens Customer Support.

#### Obtaining a Newer or Older Software Package

For details on how to obtain a newer or older version of RUGGEDCOM ROX II, refer to [Guide to Download RUGGEDCOM Software and Firmware](https://support.industry.siemens.com/cs/us/en/view/109739630) [https://support.industry.siemens.com/cs/us/en/view/109739630].

#### Digital Signature

Software images for RUGGEDCOM ROX II provided by Siemens are cryptographically signed by GNU Privacy Guard (GPG). As such, software images require a companion GPG signature file.

Each software image is packaged together with its associated GPG signature file in a compressed ZIP file. The ZIP file is then available for download from [Siemens Industry Online Support \(SIOS\) website](https://support.industry.siemens.com/cs/us/en/ps/21322/pm) [https://support.industry.siemens.com/cs/us/en/ps/21322/pm] or through Siemens Customer Support.

After obtaining the software image and associated GPG signature, make sure both files remain together. RUGGEDCOM ROX II uses the GPG signature file to verify the integrity and authenticity of the software image at the time of installation.

#### Installing a Software Package

After obtaining a software package, do the following:

1. Download the software package as instructed.

The software package is a compressed ZIP file that contains the software image and associated GPG signature. The name of the ZIP file will be in the form of **rrX.Y.Z.zip**, where *X* represents the major release number, *Y* represents the minor release number, and *Z* represents the patch release number.

---

**Note**

If the software package is provided by Siemens Customer Support, specific instructions will be provided.

---

2. Save the file to either:
  - A local upgrade server
  - A USB flash drive
3. Extract the contents of the compressed file, making sure not to modify the resulting file/directory structure. Make sure the image and GPG signature remain together.
4. During the software upgrade process, target the USB flash drive or upgrade server.

### 4.12.2.3 Stopping/Declining a Software Upgrade

To stop/decline an active software upgrade and revert back to the previously installed version, do the following:

 <b>NOTICE</b>
---

A software upgrade can only be declined before the device is rebooted. If a system reboot has occurred, the previous software version can only be restored with a rollback.
---

For more information about rolling back RUGGEDCOM ROX II to the previous software version, refer to "Rolling Back a Software Upgrade" (Page 92).
--

1. Navigate to the **Upgrade** tab under **Administration » Firmware Management**.
2. Under **Decline software upgrade**, click **Perform**.

### 4.12.2.4 Upgrading the Software and Retaining the Configuration

To install a newer version of RUGGEDCOM ROX II and retain the current device configuration, do the following:

---

**Note**

The target version must be greater than the active version currently in use.

---



---

**Note**

If upgrading from a previous release of RUGGEDCOM ROX II to v2.16, refer to the documentation for the release that is currently installed on the device. **The following instructions only describe how to upgrade from RUGGEDCOM ROX II v2.16 to a newer version.**

---

**Note**

Before upgrading to a newer version of RUGGEDCOM ROX II, note the following:

- The **Firmware Download** announcement for the target version may detail special upgrade requirements/restrictions. Make sure to review these details before proceeding.

For a list of **Firmware Download** announcements for RUGGEDCOM ROX II, visit <https://support.industry.siemens.com/cs/search?search=rox&type=Download>.

If an announcement is not available for the target software version, contact Siemens Customer Support.

- Due to potential differences in the system architecture between releases, an intermediary version of RUGGEDCOM ROX II may need to be installed before the target version is installed.

Some versions of RUGGEDCOM ROX II may require a GPG signature file.

For more information about upgrade paths and GPG signature file requirements, refer to the FAQ "How to determine the firmware upgrade path for a RUGGEDCOM ROX II device? [<https://support.industry.siemens.com/cs/us/en/view/109806037>]".

- Make sure the system time and date are current. For more information, refer to "Configuring the System Time and Date" (Page 764).
- 

1. Obtain the software package for the target release. For more information, refer to "Obtaining a Software Release" (Page 84).
2. If the software will be installed from a removable USB flash drive, insert the drive into the USB port.

For more information, refer to the "Installation Manual" for the device.

3. Make sure all applications installed on the device are compatible with the target version of RUGGEDCOM ROX II.

If an application is not compatible, the upgrade process will stop automatically and details will be recorded in the upgrade log.

4. Navigate to the **Upgrade** tab under **Administration » Firmware Management**.
- 

**Note**

For upgrades via HTTPS (SSL), the server's root CA certificate and CRL must be added. For more information, refer to "Adding a CA Certificate and CRL" (Page 179).

---

**Note**

For upgrades via FTPS, if the URL includes the port value **990** or no port is specified, the connection to the remote FTPS server will use **Implicit FTPS** mode. If a port value other than **990** is used, the connection will use **Explicit FTPS** mode.

5. Under **Launch Software Upgrade**, click **Perform**. A confirmation dialog box appears. Click **OK** to proceed.
6. Configure the following parameter:

Parameter	Description
Upgrade Server URL	<p><b>Synopsis:</b> A string up to 256 characters long</p> <p>The URL of the ROX II image to download. Supported URIs are HTTP, HTTPS, FTP, FTPS, SFTP, USB and SD.</p> <p>To flash from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". To determine the device name, insert your device and in the web ui, go to "chassis", "storage", "removable", OR, in the cli, type "show chassis". Note that only one single partition is supported for either data medium.</p> <p>For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".</p>

**Note**

If a removable drive is used, do not remove the drive from the device until the upgrade process is complete.

7. Click **OK**. The target software is downloaded to the inactive partition and installed.

The progress of the software upgrade can be monitored in real-time.

For more information, refer to "Monitoring Software Upgrades/Downgrades" (Page 92).

**Note**

Rebooting the device is the final stage of the upgrade process. After a successful reboot, the inactive (secondary) partition where the software package was installed is switched to the active (primary) partition.

For information on how to stop/decline the current upgrade, refer to "Stopping/Declining a Software Upgrade" (Page 85)

8. When the software upgrade is complete, reboot the device.
- For more information about rebooting the device, refer to "Rebooting the Device" (Page 58).

#### 4.12.2.5 Upgrading the Software and Resetting the Configuration

To install a newer version of RUGGEDCOM ROX II and reset the device configuration to factory defaults, do the following:

---

##### Note

The target version must be greater than the active version currently in use.

---

##### Note

If upgrading from a previous release of RUGGEDCOM ROX II to v2.16, refer to the documentation for the release that is currently installed on the device. **The following instructions only describe how to upgrade from RUGGEDCOM ROX II v2.16 to a newer version.**

---

##### Note

Before upgrading to a newer version of RUGGEDCOM ROX II, note the following:

- The **Firmware Download** announcement for the target version may detail special upgrade requirements/restrictions. Make sure to review these details before proceeding.

For a list of **Firmware Download** announcements for RUGGEDCOM ROX II, visit <https://support.industry.siemens.com/cs/search?search=rox&type=Download>.

If an announcement is not available for the target software version, contact Siemens Customer Support.

- Due to potential differences in the system architecture between releases, an intermediary version of RUGGEDCOM ROX II may need to be installed before the target version is installed.

Some versions of RUGGEDCOM ROX II may require a GPG signature file.

For more information about upgrade paths and GPG signature file requirements, refer to the FAQ "[How to determine the software upgrade/downgrade path for a RUGGEDCOM ROX II device? \[https://support.industry.siemens.com/cs/us/en/view/109806037\]](https://support.industry.siemens.com/cs/us/en/view/109806037)".

- Make sure the system time and date are current. For more information, refer to "Configuring the System Time and Date" (Page 764).
- 

1. Obtain the software package for the target release. For more information, refer to "Obtaining a Software Release" (Page 84).
2. If the software will be installed from a removable USB flash drive, insert the drive into the USB port.

For more information, refer to the "Installation Manual" for the device.

3. Make sure all applications installed on the device are compatible with the target version of RUGGEDCOM ROX II.

If an application is not compatible, the upgrade process will stop automatically and details will be recorded in the upgrade log.

4. Navigate to the **ROX Flash** tab under **Administration » Firmware Management**.

---

**Note**

For upgrades via HTTPS (SSL), the server's root CA certificate and CRL must be added. For more information, refer to "Adding a CA Certificate and CRL" (Page 179).

---

**Note**

For upgrades via FTPS, if the URL includes the port value **990** or no port is specified, the connection to the remote FTPS server will use **Implicit FTPS** mode. If a port value other than **990** is used, the connection will use **Explicit FTPS** mode.

---

**Note**

URL strings may only contain numbers, lowercase and uppercase characters, spaces, and the following special characters: `.-:/%@`

---

5. Under **ROX II Image URL**, configure the following parameter:

Parameter	Description
ROX II Image URL	<p><b>Synopsis:</b> A string up to 256 characters long</p> <p>The URL of the ROX II image to download. Supported URIs are HTTP, HTTPS, FTP, FTPS, SFTP, USB and SD.</p> <p>To flash from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". To determine the device name, insert your device and in the web ui, go to "chassis", "storage", "removable", OR, in the cli, type "show chassis". Note that only one single partition is supported for either data medium.</p> <p>For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".</p>

---

**Note**

If a removable drive is used, do not remove the drive from the device until the upgrade process is complete.

---

6. Click **Perform**. The target software is downloaded to the inactive partition and installed.

The progress of the software upgrade can be monitored in real-time.

For more information, refer to "Monitoring Software Upgrades/Downgrades" (Page 92).

---

**Note**


Rebooting the device is the final stage of the upgrade process. After a successful reboot, the inactive (secondary) partition where the software package was installed is switched to the active (primary) partition.

For information on how to stop/decline the current upgrade, refer to "Stopping/Declining a Software Upgrade" (Page 85)

---

7. When the software upgrade is complete, reboot the device. For more information about rebooting the device, refer to "Rebooting the Device" (Page 58).

#### 4.12.2.6 Downgrading Software

 <b>NOTICE</b>
<b>Restriction</b>
Downgrading to a version lower than v2.16.0 is not permitted.

To downgrade the RUGGEDCOM ROX II software to an earlier version, do the following:

---

**Note**

When downgrading to an older version, the software is installed on the inactive partition with factory default settings. The software configuration and feature keys on the active partition are not copied to the inactive partition.

---

1. Obtain a link to or a copy of the software packages.  
For more information about obtaining a software release, refer to "Obtaining a Software Release" (Page 84).
2. If the software will be installed from a removable USB flash drive, insert the drive into the USB port.  
For more information, refer to the "Installation Manual".
3. Navigate to the **ROX Flash** tab under **Administration » Firmware Management**.
4. Under **Download a ROX II Image from Specified URL and Flash it to the Alternate Partition**, click **Perform**. A confirmation dialog box appears. Click **OK** to proceed.
5. Configure the following parameter:

**Note**

For downgrades via HTTPS (SSL), a custom or trusted Certificate Authority (CA) must be configured on the device. For more information, refer to "Adding a CA Certificate and CRL" (Page 179).

**Note**

For downgrades via FTPS, if the URL includes the port value **990** or no port is specified, the connection to the remote FTPS server will use **Implicit FTPS** mode. If a port value other than **990** is used, the connection will use **Explicit FTPS** mode.

Parameter	Description
ROX II Image URL	<p><b>Synopsis:</b> A string up to 256 characters long</p> <p>The URL of the ROX II image to download. Supported URIs are HTTP, HTTPS, FTP, FTPS, SFTP, USB and SD.</p> <p>To flash from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". To determine the device name, insert your device and in the web ui, go to "chassis", "storage", "removable", OR, in the cli, type "show chassis". Note that only one single partition is supported for either data medium.</p> <p>For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".</p>

**Note**

If a removable drive is used, do not remove the drive from the device until the upgrade process is complete.

- Click **OK**. The target software is downloaded to the inactive partition and installed.

The progress of the software upgrade can be monitored in real-time.

For more information, refer to "Monitoring Software Upgrades/Downgrades" (Page 92).

**Note**

Rebooting the device is the final stage of the upgrade process. After a successful reboot, the inactive partition where the software package was installed is switched to the active (primary) partition.

For information on how to stop/decline the current upgrade, refer to "Stopping/Declining a Software Upgrade" (Page 85)

- When the software downgrade is complete, reboot the device.

For more information about rebooting the device, refer to "Rebooting the Device" (Page 58).

#### 4.12.2.7 Rolling Back a Software Upgrade

To activate a previous version of the RUGGEDCOM ROX II software stored on the inactive (secondary) partition, do the following:

1. Navigate to the **Upgrade** tab under **Administration » Firmware Management**.
2. Under **Rollback software upgrade**, click **Perform**. The device is automatically rebooted. Once the reboot is complete, the previously inactive partition containing the older software version is changed to an active state.

#### 4.12.2.8 Monitoring Software Upgrades/Downgrades

To monitor the real-time progress of an active software upgrade or downgrade, navigate to the **Monitor** tab under **Administration » Firmware Management**.

The following information is displayed:

Parameter	Description
Flash Phase	<p><b>Synopsis:</b> [ Inactive   Downloading image   Imaging partition   Unknown state   Completed successfully   Failed   Validating database   Copying configuration   Declined   Imaging app ]</p> <p>The current phase or state of the ROXflash operation. It is always one of the following: Inactive, Imaging partition, Unknown state, Completed successfully, or Failed. These phrases do not vary, and may be used programatically for ascertaining state.</p>
Flash Status	<p><b>Synopsis:</b> A string up to 1024 characters long</p> <p>Detailed messages about ROXflash progress or errors.</p>
Image Flashing (% complete)	<p><b>Synopsis:</b> An integer between 0 and 100</p> <p>Indicates the imaging progress and the percentage that is complete.</p>

### 4.13 Monitoring Firmware Integrity

RUGGEDCOM ROX II can perform an integrity check to verify the integrity of running programs and installed files. The integrity check can be invoked in the following ways:

- automatically at system start-up
- as a scheduled job
- on demand via the user interface

If an unauthorized/unexpected modification is detected during the integrity check, an alarm is triggered and each offending file or program is logged.

---

**Note**

RUGGEDCOM ROX II validates the authenticity and integrity of the firmware. Software upgrades are cryptographically signed at the factory by Siemens and cannot be falsified. The firmware upgrade package is validated cryptographically at the time of the upgrade. During operation, the integrity of the installed files is verified and all running programs are verified to be part of the validated installation.

---

 **NOTICE****Security hazard – risk of unauthorized access and/or exploitation**

For the firmware integrity check to be meaningful, appropriate care must be taken to protect the device. Make sure physical access to the device is restricted to authorized personnel only and that administrator login credentials are kept secure.

---

**Note**

The firmware integrity check only analyzes RUGGEDCOM ROX II operating system files. It does not detect additional files that may have been placed by a malicious user, unless they are program binary files that are running at the time of the integrity check.

---

### 4.13.1 Enabling/Disabling the Boot Time Firmware Integrity

The boot time integrity check is disabled by default. When enabled though, the check occurs whenever the device is restarted or powered on.

To enable or disable this feature, do the following:

1. Navigate to the **Bootup/Shutdown** tab under **Administration » System**.
2. Under **Boot time firmware integrity check**, select **Enabled** to enable the boot time integrity check, or clear the check box to disable the feature.
3. Commit the change.

### 4.13.2 Checking the Firmware Integrity

To check the firmware integrity manually, do the following:

1. Navigate to the **Bootup/Shutdown** tab under **Administration » System**.
2. Under **Check the integrity of the system files**, click **Perform** and allow a few seconds for the integrity check to complete. If no unauthorized/unexpected modifications were detected, the message **Success** is displayed.

If the integrity check fails, the following message is displayed:



FAILURE. The firmware integrity check has failed. This may indicate that some operating system files have been modified or tampered with. For assistance, contact Siemens Customer Support.

### 4.13.3 Scheduling a Recurring Firmware Integrity Check

Using the RUGGEDCOM ROX II scheduler, the firmware integrity check can be scheduled to run automatically at a specific time and date, either once or on a recurring schedule. For more information about scheduling the firmware integrity check, refer to "Scheduling Jobs" (Page 123).

### 4.13.4 Viewing the Status of the Firmware Integrity Check

To view the status of the last firmware integrity check, navigate to the **Chassis Status** tab under **Administration » System » Chassis » System**. The results of the last integrity check are detailed.

If the integrity check is successful, the following message is displayed:

Success

If the integrity check failed, the following message is displayed:

FAILURE. The firmware integrity check has failed. This may indicate that some operating system files have been modified or tampered with. For assistance, contact Siemens Customer Support.

## 4.14 Managing the Fan Controller

RUGGEDCOM MX5000RE devices may be equipped with an optional fan module to monitor and control the temperature of the device. When the internal temperature meets or exceeds a user-specified value, one of the two fan arrays will activate automatically.

### 4.14.1 Viewing the Fan Controller Status

RUGGEDCOM ROX II monitors the status of the fan controller and the individual fan banks.

#### Viewing the Overall Status

To view the overall status of the fan controller, navigate to the **Controller** tab under **Administration » System » Chassis » System**.

The following information is displayed for the fan controller:

Parameter	Description
Fan Module Temperature (C)	<b>Synopsis:</b> An integer between -50 and 120 The external temperature reading adjacent to the fans.
Fan Modules Status	The overall status of the fan modules. Possible values include: <ul style="list-style-type: none"> <li>• <b>Failed</b> – Insufficient cooling from both fan banks (two or more fans failed in each bank)</li> <li>• <b>Failing</b> – Insufficient cooling from one fan bank (two or more fans failed on one bank) or a temperature sensor has failed</li> <li>• <b>Operating</b> – Both fan banks are reporting sufficient cooling</li> </ul>

**Note**

For information about the status of individual fan banks, refer "Viewing Only the Status of the Fan Banks" (Page 95).

**Viewing Only the Status of the Fan Banks**

To view only the status of the fan banks, navigate to the **Controller** tab under **Administration » System » Chassis » System**.

**Note**

Only fan banks that are connected are displayed

The following information is displayed for the individual fan banks:

Parameter	Description
Fan ID	<b>Synopsis:</b> A string up to 31 characters long The name of the fan module as it appears on the device.
Fan State	<b>Synopsis:</b> [ failed   standby   off   on ] The operational state of the fan. Possible values include: <ul style="list-style-type: none"> <li>• <b>on</b> – The fan bank is on</li> <li>• <b>off</b> – The fan bank is off</li> <li>• <b>standby</b> – The fan is in standby mode</li> <li>• <b>failed</b> – Insufficient cooling from the fan bank</li> </ul>
Fan Status	Additional fan-specific status descriptions. Possible values include: <ul style="list-style-type: none"> <li>• <b>n/a</b> – The fan banks are off</li> <li>• <b>Normal (RPM)</b> – The TACH input line is functioning and FMD is using in TACH mode</li> <li>• <b>Normal (Current)</b> – The TACH input line is not functioning and FMD is in DC-Current mode</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>{ Number } fan(s) inoperative (RPM)</b> – The number of fan(s) that are not functioning in TACH mode</li> <li>• <b>Fans inoperative (Current)</b> – TACHs and current measurement have failed for the fan bank</li> <li>• <b>{ Number } of 2 temperature sensors failed</b> – The number of temperature sensors that have failed</li> <li>• <b>PTC Trip</b> – The overcurrent fuse has tripped and there is no voltage supply to fan</li> </ul>

### Viewing the Individual Status of a Specific Fan Bank

To view individual status of a specific fan bank, navigate to the **Controller** tab under **Administration » System » Chassis » System**, and then select a fan.

### 4.14.2 Configuring the Activation Temperature

The individual fan arrays are activated by the fan controller based on the activation temperature. If the ambient temperature meets or exceeds the set activation temperature, the fan controller activates the fan array that has been idle the longest.

To set the activation temperature for the fan controller, do the following:

1. Navigate to the **Parameters** tab under **Administration » System » Chassis**.
2. Configure the following parameter(s) as required:

Parameter	Description
Activation Temperature (C)	<p><b>Synopsis:</b> An integer between 25 and 85</p> <p><b>Default:</b> 50</p> <p>The temperature above which the fans will be activated. The minimum and maximum values of this parameter are 25C and 85C.</p>

3. Commit the change.

### 4.15 Managing Fixed Modules

This section describes how to manage non-field replaceable modules, such as the control module.

## 4.15.1 Viewing a List of Fixed Module Configurations

To view a list of fixed module configurations, navigate to the **Modules** tab under **Administration » System » Chassis**. If fixed modules have been configured, the **Fixed Modules** table appears.

## 4.16 Managing Line Modules

RUGGEDCOM RX5000/MX5000/MX5000RE devices feature slots for field-replaceable line modules, which can be used to expand and customize the capabilities of the device to suit specific applications. A variety of modules are available, each featuring a specific type of communication port. For information about available line modules, refer to the "Modules Catalog" for the device family.

This section describes how to properly remove, install and configure line modules.

### 4.16.1 Removing a Line Module

To remove a line module from the chassis, do the following:

1. Shut down the device. The device will shutdown for a period of time before rebooting and restarting. The default time-out period is 300 seconds (five minutes). If more time is required to complete the procedure, disconnect power from the device during the time-out period. For more information on how to shutdown the device, refer to "Shutting Down the Device" (Page 58).
2. Remove the line module from the device.

### 4.16.2 Installing a New Line Module

Line modules are hot-swappable and can be replaced with modules of the same type without powering down the device.

To install a new line module in the chassis, do the following:

1. If equipped, remove the line module currently installed in the slot. For more information, refer to "Removing a Line Module" (Page 97).
2. Navigate to the **Modules** tab under **Administration » System » Chassis**. The **Line Modules** form appears.
3. Under **Module Type**, select **none** from the list. This allows RUGGEDCOM ROX II to automatically detect the new module during the next startup.
4. Commit the changes.
5. Insert the new line module into the empty slot in the chassis.
6. Reboot the device. For more information, refer to "Rebooting the Device" (Page 58).

### 4.16.3 Viewing a List of Line Module Configurations

After the device is rebooted, the new line module is automatically detected and operational.

7. If the line module is different from the previous module installed in the same slot, configure the new line module. For more information, refer to "Configuring a Line Module" (Page 98).

### 4.16.3 Viewing a List of Line Module Configurations

To view a list of line module configurations, navigate to the **Modules** tab under **Administration » System » Chassis**. If line modules have been configured, the **Line Modules** table appears.

If no line modules have been configured, install line module as needed. For more information, refer to "Installing a New Line Module" (Page 97).

### 4.16.4 Configuring a Line Module

To configure a line module, do the following:

1. Navigate to the **Modules** tab under **Administration » System » Chassis**. The **Line Modules** form appears.
2. Select the line module to configure.
3. Configure the following parameter(s) as required:

Parameter	Description
Detected Module	<b>Synopsis:</b> A string up to 60 characters long The installed module's type specifier.
Module Type	<b>Synopsis:</b> A string up to 60 characters long Sets the module type to be used in this slot.
Admin State	Sets the administrative state for a module. Enabling the module powers it on.

4. Commit the changes.

#### Note

Upon committing the new line module configuration, *Internal Configuration Error* alarms may be generated. These can be safely ignored and cleared in this context.

## 4.17 Managing SFP Transceivers (RUGGEDCOM RX5000 Only)

RUGGEDCOM ROX II supports a wide variety of Small Form-factor Pluggable (SFP) transceivers to help expand the capabilities of the device. For a full list of Siemens-approved SFP transceivers, refer to the [RUGGEDCOM SFP Transceivers Catalog \[https://support.industry.siemens.com/cs/ww/en/view/109482309\]](https://support.industry.siemens.com/cs/ww/en/view/109482309).

### NOTICE

It is strongly recommended to use SFP transceiver models approved by Siemens only. Siemens performs extensive testing on these transceivers to make sure they can withstand harsh conditions. If a different SFP transceiver model is used, it is the user's responsibility to verify it meets environmental and usage requirements.

### 4.17.1 SFP Transceiver Support

RUGGEDCOM ROX II offers the following support for SFP transceivers.

#### Hot Swappable

All SFP transceivers are hot swappable, meaning they can be removed and inserted while the device is operating. Only a previously established link on that port is affected while the socket is empty.

#### Automatic Detection

RUGGEDCOM ROX II actively monitors each SFP transceiver port to determine when an SFP transceiver has been inserted or removed. Each event is logged in the syslog.

#### Smart SFP For Select Transceivers

Smart SFP mode is available for any port on the RX5000PN LM 4FG50 line module. This mode is enabled by default.

Smart SFP enables RUGGEDCOM ROX II to automatically configure the speed and auto-negotiation settings for the socket to match the transceiver. Settings are based on the capabilities read from the SFP transceivers EEPROM.

### NOTICE

All SFP transceivers approved by Siemens support Smart SFP mode. SFP transceivers that do not support Smart SFP mode may be disabled upon insertion and marked as *Unidentified*. If this occurs, attempt to disable Smart SFP and configure the speed and auto-negotiation settings for the port manually.

For information about disabling (or enabling) Smart SFP mode, refer to "Enabling/Disabling Smart SFP Mode (RUGGEDCOM RX5000 Only)" (Page 100).

## 4.17.2 Viewing SFP Information

To view information about a specific Small Form-Factor Pluggable (SFP) transceiver in a line module, do the following:

---

### Note

Some SFPs may not make information about themselves available. In these cases, a message similar to the following will appear:

```
ID: Unknown FF
```

---

1. Navigate to the **Port Status** tab under **Interface » Switch Ports**.
2. Click **Get** for the desired line module. A dialog box appears.
3. Select the SFP Parameter information to be displayed, and then click **OK**. The technical specifications of the selected transceiver are displayed.

## 4.17.3 Enabling/Disabling Smart SFP Mode (RUGGEDCOM RX5000 Only)

Smart SFP mode can be disabled for SFP transceivers that do not support Smart SFP. These transceivers are disabled automatically upon insertion and marked as *Unidentified*.

---

### Note

Smart SFP mode is only available for any port on the RUGGEDCOM RX5000PN LM 4FG50 line module.

---

### Note

To determine if an SFP transceiver has been marked as *Unidentified*, refer to the **Media** parameter on the **Switched Ethernet Port Status** form associated with the port. For more information, refer to "Viewing the Status of a Switched Ethernet Port" (Page 284). The parameter will display the following if the SFP transceiver is marked as *Unidentified*:

```
SFP - Unidentified
```

The SFP transceiver is not marked as *Unidentified*, the **Media** displays information about the SFP transceiver. For example:

```
SFP 1000LX SM LC 10 km
```

---

### Note

If an SFP transceiver remains marked as *Unidentified* after disabling Smart SFP mode, contact Siemens Customer Support.

---

To enable or disable Smart SFP mode for an SFP transceiver, do the following:

1. Navigate to the **Port Parameters** tab under **Interface » Switch Ports**.

2. Select **Smart SFP Mode** for the desired SFP transceiver to enable Smart SFP mode, or clear the check box to disable the feature.
3. If Smart SFP mode is disabled, review the configuration for the SFP transceiver socket. Some settings may need to be adjusted manually to suit the capabilities of the installed SFP transceiver. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276).
4. Commit the changes.

## 4.18 Managing Routable Ethernet Ports

This section describes how to configure routable Ethernet Ports, including the assignment of VLANs.

### 4.18.1 Viewing a List of Routable Ethernet Ports

To view a list of routable Ethernet ports, navigate to the **Port Parameters - { interface }** tab under **Interface » Eth**, where { interface } is the routable Ethernet port.

### 4.18.2 Configuring a Routable Ethernet Port

To configure a routable Ethernet port, do the following:

1. Navigate to the **Port Parameters - { interface }** tab under **Interface » Eth**, where { interface } is the routable Ethernet port.
2. Configure the following parameters as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables/Disables the network communications on this port.</p>
AutoN	<p>Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results.</p>
Speed	<p><b>Synopsis:</b> [ 10   100   1000 ]</p> <p>Speed (in Megabit-per-second or Gigabit-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes.</p>



Parameter	Description
Duplex	<b>Synopsis:</b> [ half   full ]  If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes.
Link Alarms	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true  Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
IP Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static  Determines whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces.
IPv6 Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static  Determines whether the IPv6 address is static or dynamically assigned via DHCPv6. The DYNAMIC option is a common case of a dynamically assigned IPv6 address. This must be static for non-management interfaces.
Proxy ARP	Enables/Disables whether the port will respond to ARP requests for hosts other than itself.
On Demand	This interface is up or down on demand of link fail over.
Alias	<b>Synopsis:</b> A string up to 64 characters long  The SNMP alias name of the interface

3. Add a VLAN ID (VID) for the port. For more information, refer to "Adding a VLAN to a Routable Ethernet Port" (Page 103).
4. Commit the changes.

### 4.18.3 Managing VLANs for Routable Ethernet Ports

This section describes how to manage VLANs for routable Ethernet ports.

### 4.18.3.1 Viewing a List of VLANs for Routable Ethernet Ports

To view a list of VLANs configured for a routable Ethernet port, navigate to the **VLANs** tab under **Interface » Eth**. If VLANs have been configured, the **VLANs** table appears.

If no VLANs have been configured, add VLANs as needed. For more information about configuring VLANs for either a routable Ethernet port or virtual switch, refer to "Adding a VLAN to a Routable Ethernet Port" (Page 103).

### 4.18.3.2 Adding a VLAN to a Routable Ethernet Port

To add a VLAN to a routable Ethernet port, do the following:

1. Navigate to the **VLANs** tab under **Interface » Eth**.
2. Click **Add Entry**. A dialog box appears.
3. Configure the following parameter(s) as required:

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 The VLAN ID for this routable logical interface.

4. Click **OK** to create the new VLAN.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces.
IPv6 Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IPv6 address is static or dynamically assigned via DHCPv6. Option DYNAMIC is a common case of a dynamically assigned IPv6 address. This must be static for non-management interfaces.
On Demand	This interface is up or down on the demand of the link failover.

6. Add a QoS map for the VLAN. For more information, refer to "Adding a QoS Map" (Page 743).
7. Commit the changes.

### 4.18.3.3 Deleting a VLAN for a Routable Ethernet Port

To delete a VLAN configured for either a routable Ethernet port or virtual switch, do the following:

1. Navigate to the **VLANs** tab under **Interface » Eth**.
2. Select the desired VLAN, and then click **Delete Entry**.
3. Commit the change.

## System Administration

This chapter describes how to perform various administrative tasks related to device identification, user permissions, alarm configuration, certificates and keys, and more.

### 5.1 Configuring the System Name and Location

To configure the system name and location of the device, do the following:

1. Navigate to the **System Name** tab under **Administration » System**.
2. Configure the following parameter(s) as required:

Parameter	Description
System Name	<p><b>Synopsis:</b> A string up to 255 characters long  <b>Default:</b> System Name</p> <p>An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.</p>
Location	<p><b>Synopsis:</b> A string up to 255 characters long  <b>Default:</b> Location</p> <p>The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string.</p>
Contact	<p><b>Synopsis:</b> A string up to 255 characters long  <b>Default:</b> Contact</p> <p>The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.</p>

3. Commit the changes.

### 5.2 Configuring the Host Name

To configure the host name for the device, do the following:

1. Navigate to the **Hostname** tab under **Administration » System**.
2. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string between 1 and 63 characters long</p> <p><b>Default:</b> ruggedcom</p> <p>The host name for the device. This name appears in the command line prompt. The host name must not contain special characters (i.e. !@#\$%^&amp;*()_+~={} ;:'.&lt;.&gt;/?\ `~).</p>
Domain	<p><b>Synopsis:</b> A string between 1 and 253 characters long</p> <p><b>Default:</b> localdomain</p> <p>The domain name associated with the device. This name is appended to the end of unqualified names (e.g. ruggedcom.example.com).</p>

3. Commit the changes.

## 5.3 Customizing the Welcome Screen

A custom welcome message for both the Web and CLI interfaces can be displayed at the login prompt.

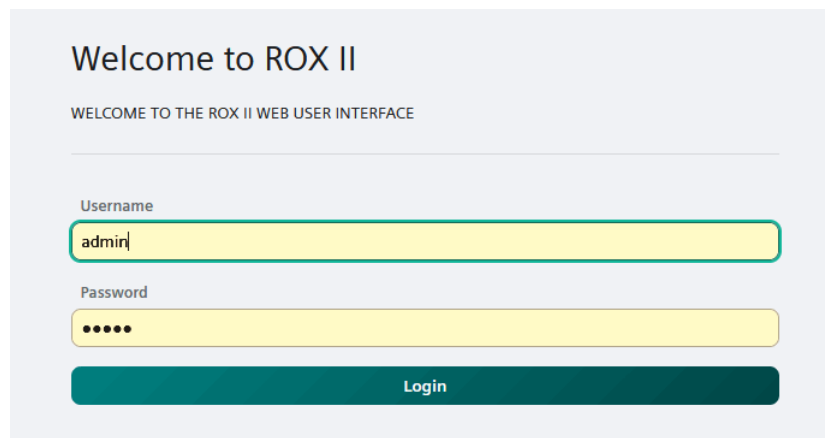


Figure 5.1 A Customized Welcome Screen

To add a custom welcome message, do the following:

1. Navigate to the **General** tab under **Administration » System » Authentication**.
2. Under **Banner**, type the welcome message.
3. Commit the change.

## 5.4 Setting the Maximum Number of Sessions

To set the maximum number of sessions that can be open at one time, do the following:

1. Navigate to the **General** tab under **Administration » Session Config**.
2. Configure the following parameter(s) as required:

Parameter	Description
Maximum Sessions Total	<p><b>Synopsis:</b> An integer  <b>Default:</b> 70</p> <p>Puts a limit on the total number of concurrent sessions to ROX.</p>

3. Commit the change.

## 5.5 Enabling and Configuring WWW Interface Sessions

To enable and configure WWW interface sessions, do the following:

1. Navigate to the **WWW Interface Sessions** tab under **Administration » Session Config**.
2. Configure the following parameter(s):

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]  <b>Default:</b> true</p> <p>Provides the ability to configure WebUI features on the device.</p>
Listen IP	<p><b>Synopsis:</b> A string  <b>Default:</b> 0.0.0.0</p> <p>The IP Address the CLI will listen on for WebUI requests.</p>
Listen Port	<p><b>Synopsis:</b> An integer between 0 and 65535  <b>Default:</b> 443</p> <p>The port on which the WebUI listens for WebUI requests.</p>
Extra IP Ports	<p><b>Synopsis:</b> A string</p> <p>The WebUI will also listen on these IP Addresses. For port values, add '#' to set non-default port value. (ie. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). If using the default address, do not specify another listen address with the same port.</p>
Maximum Number of WebUI Sessions	<p><b>Synopsis:</b> An integer  <b>Default:</b> 20</p> <p>The maximum number of concurrent WebUI sessions</p>

Parameter	Description
Idle Timeout	<p><b>Synopsis:</b> A string  <b>Default:</b> PT30M</p> <p>The maximum idle time before terminating a WebUI session. If the session is waiting for notifications, or has a pending confirmed commit, the idle timeout is not used. A value of 0 means no timeout. PT30M means 30 minutes.</p>
SSL Redirect Enabled	<p><b>Synopsis:</b> [ true   false ]  <b>Default:</b> true</p> <p>Redirects traffic from port 80 to port 443. If disabled, port 80 will be closed.</p>
Client Certificate Verification	<p><b>Synopsis:</b> [ none   peer   fail-if-no-peer-cert ]  <b>Default:</b> none</p> <p>Level of verification the server does on client certificates</p> <ul style="list-style-type: none"> <li>• none - It does not do any verification.</li> <li>• peer - The server will ask the client for a client-certificate but not fail if the client does not supply a client-certificate.</li> <li>• fail-if-no-peer-cert - The server requires the client to supply a client certificate.</li> </ul>

3. Commit the changes.

## 5.6 Enabling/Disabling Remote Access Through a VRF Interface

A VRF interface can be used to remotely access the CLI and Web interface, or as an interface for SNMP. This capability is available on a per-interface basis and is disabled by default.

### NOTICE

This feature does not support some services. Note the following restrictions:

- DHCP is not supported. As such, the VRF interface must not derive its IP address from an DHCP server.
- HTTP redirects to HTTPS are not supported. As such, HTTPS must be entered explicitly when accessing the Web user interface via a browser (e.g. https://x.x.x.x).
- HTTP is not supported on SNMP connections.

To enable or disable this function on a VRF instance, do the following:

1. Make sure at least one VRF instance has been configured. For information about configuring a VRF instance, refer to "Configuring VRF" (Page 559).
2. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**.

3. Select the **Remote Administration** check box for the target VRF to enable the feature, or clear the check box to disable the feature.

---

**Note**

The parameters **SNMP Administration** and **SNMP Listen Port** are only available when SNMP sessions are enabled. For information about how to enable SNMP sessions, refer to "Enabling and Configuring SNMP Sessions" (Page 704).

---

4. Configure the following parameters:

Parameter	Description
Web UI Administration	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Enables access to the Web user interface over the VRF interface.
Web UI Listen Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 443 The port the Web user interface will listen on for incoming connections over a VRF interface.
CLI Administration	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Enables access to the CLI over the VRF interface.
CLI Listen Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 22 The port the CLI will listen on for incoming connections over a VRF interface.
SNMP Administration	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Enables SNMP access over the VRF interface.
SNMP Listen Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 161 The port SNMP will listen on for incoming connections over a VRF interface.

5. Commit the changes.

---

**Note**

Remote access through a VRF interface relies on Network Address Translation (NAT) rules to send frames through the VRF interface to the intended service running in the global namespace. In the case of SNMP, NAT rules are unaware of any listen IP address. As such, the listen IP address for SNMP sessions must be set to **0.0.0.0** to allow the session to connect to services in the global namespace.

---



6. If the VRF instance is to be used as a listen IP address for SNMP, make sure the **Listen IP** parameter for SNMP sessions is set to **0.0.0.0**. For more information, refer to "Enabling and Configuring SNMP Sessions" (Page 704).

## 5.7 Managing Alarms

The alarm system in RUGGEDCOM ROX II notifies users when events of interest occur. The system is highly configurable, allowing users to:

- Enable/disable most alarms, with the exception of mandatory alarms
- Configure whether or not an alarm triggers the failsafe relay and illuminates the alarm indicator LED on the device
- Configure the severity of most alarms (i.e. emergency, alert, critical, error, etc.), with the exception of some where the severity is fixed

Each alarm is categorized by its type (or subsystem):

Alarm Type	Description
Admin	Admin alarms are for administrative aspects of the device, such as feature-key problems.
Chassis	Chassis alarms are for physical or electrical problems, or similar events of interest. This includes irregular voltages at the power supply or the insertion or removal of a module.
Switch	Switch alarms are for link up/down events on switch interfaces.
Eth	Eth alarms are for fe-cm and fe-em port related events, such as link up/down events.
WAN	WAN alarms are for T1/E1 and DDS interface related events, such as link up/down events.
Cellmodem	Cellular alarms are for cellular interface related events, such as link up/down events.
Security	Security alarms are for security-related events, such as Brute Force Attacks (BFA), firmware integrity, and certificate expiry. This includes warnings 30 days before a certificate is set to expire and when an expired certificate is installed.
Services	Service alarms are for events related to RUGGEDCOM ROX II services, such as Dynamic Domain Name Server (DNS), IPsec connections, and GRE tunnels.

### 5.7.1 Pre-Configured Alarms

RUGGEDCOM ROX II is equipped with a series of pre-configured alarms designed to monitor and protect the device.

For a full list of alarms, including user-configurable alarms, refer to "List of Alarms" (Page 115).

## Admin

Name	Severity	Description	Suggested Resolution
Featurekey mismatch	Alert	The featurekey does not match the serial numbers for the control module and backplane hardware.	Move the featurekey to the correct device with the matching hardware or request an updated key from Siemens Customer Support.
Featurekey partial mismatch	Warning	The featurekey does not match the serial number for either the control module or backplane hardware.	Move the featurekey to the correct device with the matching hardware or request an updated key from Siemens Customer Support.

## Chassis

Name	Severity	Description	Suggested Resolution
PM1 bad supply	Critical	Input power to the power module is outside nominal operating range.	Make sure the input power operating range meets the device requirements.
PM2 bad supply	Critical	Input power to the power module is outside nominal operating range.	Make sure the input power operating range meets the device requirements.
PM1 MOV protection bad	Critical	The Metal Oxide Varistor (MOV) protection component within the PM1 power module is damaged.	Contact Siemens Customer Support to return the power module.
PM2 MOV protection bad	Critical	The Metal Oxide Varistor (MOV) protection component within the PM2 power module is damaged.	Contact Siemens Customer Support to return the power module.
Real-time clock battery low	Warning	The Real-Time Clock (RTC) battery in the control module is depleted.	Contact Siemens Customer Support to return the device for repair.
LM Watchdog Failure	Alert	The specified line module has stopped sending its heartbeat message to the control module.	Inspect the line module to make sure it is functioning properly.
Fan-Controller Hardware Failure (For MX5000RE Only)	Alert	The fan tray is damaged. One or more fans may stop spinning.	Contact Siemens Customer Support to return the fan module.
Fan-Controller Overtemp (For MX5000RE Only)	Alert	The ambient temperature within the enclosure has exceeded the maximum operating temperature range of the device.	Power down the device until the ambient temperature has cooled.

Name	Severity	Description	Suggested Resolution
Module Type Mismatch	Warning	The configured module type does not match the detected module type.	Updated the chassis configuration or install the correct module type.
Line Module Removed	Critical	The specified line module has either been removed or lost contact with the chassis.	Inspect the line module.
Line Module Inserted	Notice	A new line module has been inserted in the specified slot.	

### Switch

Name	Severity	Description	Suggested Resolution
Link Up	Notice		
Link Down	Alert		
Internal Configuration Error	Alert		

### Ethernet (Eth)

Name	Severity	Description	Suggested Resolution
Link Up	Notice		
Link Down	Alert		
Internal Configuration Error	Alert		

### WAN

Name	Severity	Description	Suggested Resolution
Link Up	Notice		
Link Down	Alert		
Internal Configuration Error	Alert		
DS1 Line Status Change	Alert		

### Security

Name	Severity	Description	Suggested Resolution
Certificate Expiration	Notice	The root certificate has expired.	Update the root certificate.

Name	Severity	Description	Suggested Resolution
Brute Force Attack	Alert	A brute force attack has been attempted.	Review the <b>Auth.log</b> file to determine the IP address of the host attempting to access the device. For more information, refer to "Enabling/Disabling Brute Force Attack Protection" (Page 128).
Firmware Integrity	Security	The firmware has failed the binary integrity check, indicating that one or more operating system files have been modified or tampered with.	Contact Siemens Customer Support.

## Services

Name	Severity	Description	Suggested Resolution
DDNS Bad Response	Warning		
IPsec Connection Up	Notice		
IPsec Connection Down	Warning		

### 5.7.2 Viewing a List of Active Alarms

To view a list of active alarms, navigate to the **Alarm Viewer** tab under **Administration » System » Alarms**. If any alarms are currently active, a list appears.

For information on how to clear or acknowledge an active alarm, refer to "Clearing and Acknowledging Alarms" (Page 113).

### 5.7.3 Clearing and Acknowledging Alarms

There are two types of alarms: conditional and non-conditional. Conditional alarms are generated when the condition is true and cleared when the condition is resolved and the incident is acknowledged by the user. Non-conditional alarms, however, are simply generated when the event occurs (a notification) and it is the responsibility of the user to clear the alarm.

An example of a conditional alarm is a *link down* alarm. When the condition is resolved (i.e. the link comes up), the LED and alarm relay are both disabled, if the **Auto Clear** option is enabled.

Examples of non-conditional alarms are *link up* and internal configuration errors.

### 5.7.3.1 Clearing Alarms

Non-conditional alarms must be cleared by the user. Conditional alarms, when configured, are cleared automatically.

To clear all clear-able, non-conditional alarms, do the following:

1. Navigate to the **Alarm Viewer** tab under **Administration » System » Alarms**. If any alarms are currently active, a list appears.
2. Under **Clear All Alarms**, click **Perform** to clear all clear-able alarms.

Alternatively, to clear an individual non-conditional alarm, do the following:

- In the **Clear Alarm** column of table, click the **Clear** button for the individual alarm to be cleared.

### 5.7.3.2 Acknowledging Alarms

To acknowledge all active alarms, do the following:

1. Navigate to the **Alarm Viewer** tab under **Administration » System » Alarms**. If any alarms are currently active, a list appears.
2. Under **Acknowledge All Alarms**, click **Perform** to acknowledge all active alarms.

Alternatively, to acknowledge an individual alarm, do the following:

- In the **Ack Alarm** column of table, click the **Acknowledge** button for the individual alarm to be acknowledged.

## 5.7.4 Configuring an Alarm

While all alarms are pre-configured on the device, some alarms can be modified to suit the application. This includes changing the severity and enabling/disabling certain features.

---

### Note

The **Failrelay Enable** and **LED Enable** parameters are non-configurable for *link up* alarms.

---

To configure an alarm, do the following:

1. Navigate to the **Alarm Configuration** tab under **Administration » System » Alarms**.

---

### Note

Depending on the alarm type, some of the parameters shown are not available.

---

2. Configure the following parameters as required:

**Note**

Alarm descriptions are not configurable.

Parameter	Description
Severity	<b>Synopsis:</b> [ emergency   alert   critical   error   warning   notice   info   debug ]  The severity level can be one of emergency, alert, critical, error, warning, notice, info, and debug. This cannot be changed for some alarms.
Admin Enable	If disabled, the alarm is not reported in the active list and does not actuate LED/failrelay.
Failrelay Enable	If enabled, this alarm will assert the failrelay.
LED Enable	If enabled, the main 'Alarm' LED light will be red when this alarm is asserted. If disabled, the main 'Alarm' LED light is not affected by this alarm.
Auto Clear	If enabled, the LED and failrelay will be cleared automatically when condition is met.

3. Commit the changes.

## 5.7.5 List of Alarms

The following table lists alarms in RUGGEDCOM ROX II, including their default status and whether or not the alarm is user configurable.

For more information about configuring alarms, refer to "Configuring an Alarm" (Page 114).

Group	Name	Level	Failrelay Enable	LED Enable	User Configurable	Trap	Log
Admin	Featurekey mismatch	Alert	Enabled	Enabled	Yes	Yes	Yes
Admin	Featurekey partial match	Warning	Disabled	Enabled	Yes	Yes	Yes
Chassis	PM1 bad supply	Critical	Enabled	Enabled	Yes	Yes	Yes
Chassis	PM2 bad supply	Critical	Enabled	Enabled	Yes	Yes	Yes
Chassis	PM1 MOV protection bad	Critical	Enabled	Enabled	Yes	Yes	Yes
Chassis	PM2 MOV protection bad	Critical	Enabled	Enabled	Yes	Yes	Yes
Chassis	Real-time clock battery low	Warning	Enabled	Enabled	Yes	Yes	Yes
Chassis	LM Watchdog Failure	Alert	Enabled	Enabled	Yes	No	Yes
Chassis	Fan-controller Hardware Failure	Alert	Enabled	Enabled	Yes	Yes	Yes
Chassis	Fan-controller Overtemp	Alert	Enabled	Enabled	Yes	Yes	Yes

Group	Name	Level	Failrelay Enable	LED Enable	User Configurable	Trap	Log
Chassis	Module Type Mismatch	Warning	Enabled	Enabled	Yes	Yes	Yes
Chassis	Line Module Removed	Critical	Enabled	Enabled	Yes	Yes	Yes
Chassis	Line Module Inserted	Notice	Disabled	Disabled	Yes	Yes	Yes
Switch	Link Up	Notice	---	---	Yes	Yes	Yes
Switch	Link Down	Warning	Enabled	Enabled	Yes	Yes	Yes
Switch	Internal Configuration Error	Alert	Enabled	Enabled	No	No	Yes
Switch	RMON Threshold Rising Alert	Alert	Enabled	Enabled	Yes	Yes	Yes
Eth	Link Up	Notice	---	---	Yes	Yes	Yes
Eth	Link Down	Warning	Enabled	Enabled	Yes	Yes	Yes
Eth	Internal Configuration Error	Alert	Enabled	Enabled	Yes	No	Yes
Security	Certificate Expiration	Notice	Enabled	Enabled	Yes	Yes	Yes
Security	Brute Force Attack	Alert	Enabled	Enabled	Yes	No	Yes
Security	Firmware Integrity	emergency	Enabled	Enabled	Yes	No	Yes
Services	DDNS Bad Response: Bad host name bad authentication https error	Warning	Enabled	Enabled	Yes	No	Yes
Services	IPsec Connection Up	Notice	Disabled	Enabled	Yes	Yes	Yes
Services	IPsec Connection Down	Warning	Enabled	Enabled	Yes	Yes	Yes
Services	GRE Tunnel Up	Notice	Disabled	Disabled	Yes	Yes	Yes
Services	GRE Tunnel Down	Warning	Enabled	Enabled	Yes	Yes	Yes

## 5.8 Managing Users

RUGGEDCOM ROX II allows for up to three user profiles to be configured locally on the device. Each profile corresponds to one of the following access levels:

- Guest
- Operator
- Admin

The access levels provide or restrict the user's ability to change settings and execute various commands.

Rights	User Type		
	Guest	Operator	Admin
View Settings	✓	✓	✓
Clear Logs	✓	✓	✓
Reset Alarms	✗	✓	✓
Clear Statistics	✗	✓	✓
Change Basic Settings	✗	✓	✓

Rights	User Type		
	Guest	Operator	Admin
Change Advanced Settings	✗	✗	✓
Run Commands	✗	✗	✓

 **NOTICE**

**Security hazard – risk of unauthorized access and/or exploitation**

To prevent unauthorized access to the device, make sure to change the default passwords for all users before commissioning the device. For more information, refer to "Setting a User Password/Passphrase" (Page 120).

## 5.8.1 Viewing a List of Users

To view a list of user accounts, navigate to the **Users** tab under **Administration » Users**. If users have been configured, a list appears.

If no user accounts have been configured, add user accounts as needed. For more information, refer to "Adding a User" (Page 117).

## 5.8.2 Adding a User

To add a new user account, do the following:

1. Navigate to the **Users** tab under **Administration » Users**.
2. Click the **Add Entry** button. A dialog box appears.
3. Configure the following parameter(s) as required:

Parameter	Description
User Name	<b>Synopsis:</b> A string between 1 and 128 characters long The name of the user.

4. Under **Role**, select the user's role (i.e. administrator, operator or guest).
5. Set the user's password. For more information, refer to "Setting a User Password/Passphrase" (Page 120).
6. Commit the change.
7. [Optional] Assign a user authentication key to the user account, allowing the user to access the device via SSH without having to provide a password/passphrase. For more information, refer to "Managing User Authentication Keys" (Page 143).



### 5.8.3 Deleting a User

To delete a user account, do the following:

1. Navigate to the **Users** tab under **Administration » Users**. The **Users** table appears.
2. Select the user name to delete and then click **Delete Entry**.
3. Commit the change.

### 5.8.4 Monitoring Users

Users currently logged in to the device are monitored by RUGGEDCOM ROX II and can be viewed on the **Users** screen. RUGGEDCOM ROX II allows administrators to monitor users, log users out, and broadcast messages to all users.

To view a list of users currently logged in to the device, navigate to the **Users** tab under **Tools**. The **Users** screen appears.

#### 5.8.4.1 Logging Out Users from a Session

To log a user out of the device, do the following:

1. Navigate to the **Users** tab under **Tools**. The **Users** screen appears.
2. Select the user profile to be deleted then click **Logout**.

#### 5.8.4.2 Sending Messages to Users

To broadcast a message to all users or a specific user, do the following:

1. Navigate to the **Users** tab under **Tools**. The **Users** screen appears.
2. Type a message in the **Message** box and click **Send**.
3. [Optional] Click the **Clear** button to remove the message history.

## 5.9 Managing Passwords and Passphrases

RUGGEDCOM ROX II requires separate passwords or passphrases for logging into the various device modes, such as normal, boot, service and maintenance modes. Default passwords are configured for each user type initially. It is strongly recommended that these be changed before the device is commissioned.

---

### Note

For a list of default passwords, refer to "Default User Names and Passwords" (Page 23).

---

The complexity of each password/passphrase can be chosen by the user or enforced through the device by an administrator. If a user's password/passphrase does not meet the password requirements, an error message is displayed.

In general, passwords/passphrases should consist of:

- One lower case character
- One upper case character
- One number
- One special character (i.e. !@#\$%^&\*()\_+={}|;:'.<.>/?|\`~)

---

#### Note

User authentication can also be verified through a RADIUS or TACACS+ server. When enabled for authentication and authorization, the RADIUS or TACACS+ server will be used. For more information about configuring a RADIUS or TACACS+ server, refer to "Managing RADIUS Authentication" (Page 145) and "Configuring TACACS+ Authentication" (Page 150).

 <b>NOTICE</b>
---

<b>Security hazard – risk of unauthorized access and/or exploitation</b>
--

To prevent unauthorized access to the device, change the default passwords before commissioning the device.
---

 <b>NOTICE</b>
---

<b>Accessibility hazard – risk of data loss</b>
---

Do not forget the passwords for the device. If both the maintenance and boot passwords are forgotten, the device must be returned to Siemens Canada Ltd. for repair. This service is not covered under warranty. Depending on the action that must be taken to regain access to the device, data may be lost.
---

## 5.9.1 Configuring Password/Passphrase Complexity Rules

Special rules for password/passphrase complexity can be configured. These include setting the password/passphrase length and enabling requirements for special characters.

To configure the password/passphrase complexity rules for all passwords/passphrases, do the following:

---

#### Note

Password/passphrase complexity rules do not apply to passwords/passphrases previously configured on the device.

1. Navigate to the **Password Complexity** tab under **Administration » System » Authentication**.

- Configure the following parameter(s):

Parameter	Description
Minimum Length	<b>Synopsis:</b> An integer between 1 and 128 <b>Default:</b> 12 Minimum password length.
Maximum Length	<b>Synopsis:</b> An integer between 1 and 128 <b>Default:</b> 128 Maximum password length.
Uppercase Characters Required	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Requires the password to have at least one uppercase letter.
Lowercase Characters Required	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Requires the password to have at least one lowercase letter.
Digits Required	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Requires the password to have at least one numerical digit.
Special Characters Required	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Requires the password to have at least one non-alphanumeric character. Allowed characters include "!@#%&*( )_+={ } [ ] ; : ' , < . > / ? \   ` ~ " .

- Commit the changes.

## 5.9.2 Setting a User Password/Passphrase

To set the password/passphrase for a user profile, do the following:

### Note

RUGGEDCOM ROX II supports the following special characters in passwords/passphrases: !@#%&\*( )\_+={ } [ ] ; : ' , < . > / ? \ | ` ~ .

- Navigate to the **Users** tab under **Administration » Users**.
- Click the **Set Password** button for the selected user. The **Set or Update User Password { user }** form appears.
- Configure the following parameters:

Parameter	Description
Password	<b>Synopsis:</b> A string between 1 and 128 characters long  The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
Confirm Password	<b>Synopsis:</b> A string between 1 and 128 characters long  The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.

4. Click **OK**.
5. Commit the changes.

### 5.9.3 Setting the Boot Password/Passphrase

The boot password/passphrase grants access to BIST mode and service mode, which are only accessible through the Command Line Interface (CLI). For more information about these modes, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".

#### NOTICE

##### **Security hazard – risk of unauthorized access and/or exploitation**

User authentication is not required to access BIST mode. Configure a boot password/passphrase to control initial access to the device.

#### **Note**

The boot password/passphrase is only supported by version 2010.09RR16 or later of the U-Boot binary. For information about determining and/or upgrading the U-Boot version installed on the device, refer to "[How to Upgrade the U-Boot Binary \[https://support.industry.siemens.com/cs/ww/en/view/109738243\]](https://support.industry.siemens.com/cs/ww/en/view/109738243)" available on <https://www.siemens.com>.

To set the boot password/passphrase, do the following:

1. Navigate to the **Set Password** tab under **Administration » System » Authentication**.
2. Under **Set Boot Password**, configure the following parameters:


Parameter	Description
New Password	<b>Synopsis:</b> A string between 0 and 128 characters long  The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.

Parameter	Description
New Password Repeat	<b>Synopsis:</b> A string between 0 and 128 characters long  The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
Old Password	<b>Synopsis:</b> A string between 0 and 128 characters long  Specify the old password if there is currently a boot password set, otherwise leave it empty.

3. Click **Perform**.

## 5.9.4 Setting the Maintenance Password/Passphrase

The maintenance password/passphrase grants access to the maintenance mode, which is only accessible through the Command Line Interface (CLI). For more information about this mode, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".

 <b>NOTICE</b>
<b>Configuration hazard – risk of data corruption</b>
Maintenance mode is provided for troubleshooting purposes and should only be used by Siemens technicians. As such, this mode is not fully documented. Misuse of maintenance mode commands can corrupt the operational state of the device and render it inaccessible.

To set the maintenance password, do the following:

1. Navigate to the **Set Password** tab under **Administration » System » Authentication**.
2. Under **Set Maint Password** form, configure the following parameters:

Parameter	Description
New Password	<b>Synopsis:</b> A string between 1 and 128 characters long  The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
New Password Repeat	<b>Synopsis:</b> A string between 1 and 128 characters long  The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
Old Password	<b>Synopsis:</b> A string between 1 and 128 characters long  Specify the old password.

3. Click **Perform**.

## 5.9.5 Resetting Passwords and Passphrases

If either the admin, boot or maintenance password/passphrase is lost, the only method for resetting the password/passphrase is to physically connect to the device and reset the password/passphrase through the Command Line Interface (CLI). For information about resetting passwords/passphrases, refer to the "RUGGEDCOM ROX II v2.16 CLI Configuration Manual".

## 5.10 Scheduling Jobs

The RUGGEDCOM ROX II scheduler allows users to create jobs that execute command line interface (CLI) commands at a specific date and time, or in response to specific configuration changes. Typical applications include scheduling the regular clearing of system logs, or performing periodic file transfers to remote servers.

There are two types of scheduled jobs:

- **Periodic jobs** are executed at a specified date and time.
- **Config change jobs** are executed only when a specific.

### 5.10.1 Viewing a List of Scheduled Jobs

To view a list of scheduled jobs, navigate to **Administration » Scheduler**. If jobs have been configured, a list appears.

If no jobs have been configured, add jobs as needed. For more information, refer to "Adding a Scheduled Job" (Page 123).

### 5.10.2 Adding a Scheduled Job

To add a scheduled job, do the following:

1. Navigate to **Administration » Scheduler**, and then click **Add Entry**.
2. Configure the following parameter(s) as required:

Parameter	Description
Job Name	<b>Synopsis:</b> A string up to 64 characters long The name of the scheduled job. The name can be up to 64 characters in length.

3. Click **OK**.
4. Configure the following parameter(s) as required:

Parameter	Description
Job Type	<p><b>Synopsis:</b> [ configchange   periodic ]</p> <p><b>Default:</b> periodic</p> <p>Determines when to launch the scheduled job:</p> <ul style="list-style-type: none"> <li>• periodic: The job launches at a set date and time.</li> <li>• configchange: The job launches when the configuration changes.</li> </ul>
Minute	<p><b>Synopsis:</b> A string up to 128 characters long</p> <p><b>Default:</b> 0</p> <p>For periodic jobs, sets the minutes portion of the job launch time. Valid values are in the range of 0 to 59. If no value is set, the scheduler uses the default value of 0 and launches the job every hour on the the hour.</p> <ul style="list-style-type: none"> <li>• To specify a single value, enter the value in the field. For example, to launch the job 10 minutes past the hour, enter 10.</li> <li>• To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 15, 30, and 45 minutes past the hour, enter 15,30,45.</li> <li>• To specify a range of values, enter the range as comma-separated values. For example, to launch the job every minute between 30 and 45 minutes past the hour, enter 30-45.</li> </ul> <p>This parameter is not required for configchange jobs.</p>
Hour	<p><b>Synopsis:</b> A string up to 64 characters long</p> <p>For periodic jobs, sets the hour portion of the job launch time, in the 24-hour clock format. Valid values are in the range of 0 to 23. If no value is set, the job launches every hour at the time set in the Minute field.</p> <ul style="list-style-type: none"> <li>• To specify a single value, enter the value in the field. For example, to launch the job at 5:00 pm, enter 17.</li> <li>• To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 9:00 am, 12:00 pm, and 5:00 pm, enter 9,12,17.</li> <li>• To specify a range of values, enter the range as comma-separated values. For example, to launch the job every hour between 9:00 am and 5:00 pm, enter 9-17.</li> </ul> <p>This parameter is not required for configchange jobs.</p>
Day of Month	<p><b>Synopsis:</b> A string up to 64 characters long</p> <p>For periodic jobs, sets the day of the month on which to run the scheduled job. Valid values are in the range of 1 to 31. If no value is set, the job launches every day.</p> <ul style="list-style-type: none"> <li>• To specify a single value, enter the value in the field. For example, to launch the job on the tenth day of the month, enter 10.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>To specify a list of values, enter the values as a comma-separated list. For example, to launch the job on the first, fifteenth, and thirtieth days of the month, enter 10,15,30.</li> <li>To specify a range of values, enter the range as comma-separated values. For example, to launch the job on days one through fifteen, enter 1-15.</li> </ul> <p>This parameter is not required for configchange jobs.</p>
Month	<p><b>Synopsis:</b> A string up to 32 characters long</p> <p>For periodic jobs, sets the month in which to run the scheduled job. Valid values are in the range of 1 to 12. If no value is set, the job launches every day.</p> <ul style="list-style-type: none"> <li>To specify a single value, enter the value in the field. For example, to set the month to February, enter 2.</li> <li>To specify a list of values, enter the values as a comma-separated list. For example, to set the months to January, June, and December, enter 1,6,12.</li> <li>To specify a range of values, enter the range as comma-separated values. For example, to set the months to January through June, enter 1-6.</li> </ul> <p>This parameter is not required for configchange jobs.</p>
Day of Week	<p><b>Synopsis:</b> A string up to 16 characters long</p> <p>For periodic jobs, sets the day of the week on which to run the scheduled job. Valid entries are in the range of 0 to 6, where 0 represents Sunday, 1 represents Monday, and so on. If no value is set, the job launches every day.</p> <ul style="list-style-type: none"> <li>To specify a single value, enter the value in the field. For example, to set the day to Monday, enter 1.</li> <li>To specify a list of values, enter the values as a comma-separated list. For example, to set the days to Friday, Saturday, and Sunday, enter 5,6,0.</li> <li>To specify a range of values, enter the range as comma-separated values. For example, to set the days to Monday through Friday, enter 1-5.</li> </ul> <p>This parameter is not required for configchange jobs.</p>
Command	<p><b>Synopsis:</b> A string up to 1024 characters long</p> <p>One or more commands to execute at the scheduled time. For example, this command saves the running configuration to a file name 'myconfig': show running-config   save myconfig.</p> <p>Do not use interactive commands or commands that require a manual response or confirmation.</p> <p>When entered in the CLI, the command string must be enclosed in quotation marks. When entered in the WebUI, the command string must not be enclosed in quotation marks.</p>

## 5. Commit the changes.



### 5.10.3 Deleting a Scheduled Job

To delete a scheduled Job, do the following:

1. Navigate to **Administration » Scheduler**.
2. Select the job to be deleted, then click **Delete Entry**.
3. Commit the change.

## Security

This chapter describes how to configure and manage the security-related features of RUGGEDCOM ROX II.

### 6.1 Enabling and Configuring CLI Sessions

To enable and configure CLI sessions, do the following:

1. Navigate to the **CLI Sessions** tab under **Administration » Session Config**, and then click **SSH General**.
2. Configure the following parameter(s):

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>When enabled, a command line interface (CLI) may be used to configure the device. A secure shell (SSH) client or serial console may be used to access the CLI.</p>
Listen IP	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> 0.0.0.0</p> <p>The IPv4 or IPv6 address on which the CLI will listen for requests from the device. The default value (i.e. 0.0.0.0) enables the CLI to receive requests via any IP address with which it is associated.</p>
Listen Port	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p><b>Default:</b> 22</p> <p>The default port on which the CLI will listen for requests from the device. The port corresponds with the IP address specified by the <b>Listen IP (listen-ip)</b> parameter.</p>
Extra IP Ports	<p><b>Synopsis:</b> A string</p> <p>Additional IPv4 or IPv6 addresses and their associated ports on which the CLI will listen for requests from the device. IPv4 addresses and port numbers must be separated by a colon (e.g. 192.168.0.2: 19343). IPv6 addresses and port numbers must be separated by square brackets and a colon (e.g. [2001:db8:2728::2200]:[19343]).</p> <p>If the <b>Listen IP (listen-ip)</b> parameter is set to a value other than <b>0.0.0.0</b>, the port specified by the <b>Listen Port (port)</b> parameter must not be associated with any additional addresses.</p>

Parameter	Description
Maximum Number of CLI Sessions	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 10</p> <p>The maximum number of concurrent CLI sessions.</p>
Idle Timeout	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> PT30M</p> <p>The maximum period of time that a CLI session may remain idle. After this period of time, the session is terminated. Values are expressed in durations of years, months, weeks, days, hours, minutes, and/or seconds in ISO 8601 format (e.g. P1Y1M2W3DT2H3M30S corresponds with 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30 seconds).</p> <p>A session is not considered idle if the CLI is waiting for notifications or if commits are pending. If the value of this parameter is changed during a session, the change will not take effect until the next session.</p>
Greeting	<p><b>Synopsis:</b> A string between 1 and 8192 characters long</p> <p>A greeting message presented to users when they log in to the CLI.</p>

3. Commit the changes.

## 6.2 Enabling/Disabling Brute Force Attack Protection

RUGGEDCOM ROX II features a Brute Force Attack (BFA) protection mechanism to prevent attacks via the CLI, Web interface and NETCONF. This mechanism analyzes the behavior of external hosts trying to access the SSH port, specifically the number of failed logins. After 15 failed login attempts, the IP address of the host will be blocked for 720 seconds or 12 minutes. The range of 15 failed login attempts exists to take into account various methods of accessing the device, notably when the same or different ports are used across a series of failed logins.

---

### Note

The BFA protection system is not applicable to SNMP. Follow proper security practices for configuring SNMP. For example:

- Do not use SNMP over the Internet
- Use a firewall to limit access to SNMP
- Do not use SNMPv1

---

### Note

Failed logins must happen within 10 minutes of each other to be considered malicious behavior.

---

Once the time has expired, the host will be allowed to access the device again. If the malicious behavior continues from the same IP address (e.g. another 15 failed login attempts), and then the IP address will be blocked again, but the time blocked will increase by a factor of 1.5. This will continue as long as the host repeats the same behavior.

---

**Note**

Enabling, disabling or making a configuration change to the firewall will reset – but not disable – the BFA protection mechanism. Any hosts that were previously blocked will be allowed to log in again. If multiple hosts are actively attacking at the time, this could result in reduced system performance.

---

When BFA protection is started, the following Syslog entry is displayed:

```
Jun  5 09:36:34 ruggedcom firewallmgr[3644]: Enabling Brute Force Attack Protection
```

When a host fails to login, an entry is logged in **auth.log**. For example:

```
Jun  5 10:12:52 ruggedcom confd[3386]: audit user: admin/0 Provided bad password
Jun  5 10:12:52 ruggedcom rmfmgr[3512]: login failed, reason='Bad password', user
ipaddr='172.11.150.1'
Jun  5 10:12:52 ruggedcom confd[3386]: audit user: admin/0 Failed to login over
ssh: Bad password
```

**Auth.log** also details which IP addresses are currently being blocked:

```
Jun  5 14:43:04 ruggedrouter sshguard[24720]: Blocking 172.59.9.1:4 for >630secs:
60 danger in 5 attacks
over 70 seconds (all: 60d in 1 abuses over 70s).
```

---

**Note**

For information about how to view **auth.log**, refer to "Viewing Logs" (Page 65).

---

When the default alarm for brute force attacks is enabled, a host that exceeds the maximum number of failed login attempts will trigger an alarm. The alarm will be listed on the list of active alarms until the alarm is resolved and acknowledged.

To enable/disable the BFA protection mechanism, do the following:

1. Navigate to the **General** tab under **Administration » Session Config**.
2. Under **Brute Force Attack Protection**, select the check box to enable the BFA protection mechanism, or clear it to disable the mechanism.
3. Commit the changes.
4. [Optional] Enable or disable the default alarm for brute force attacks. For more information, refer to "Configuring an Alarm" (Page 114).

## 6.3 Enabling/Disabling Compact Flash Card Removal Detection

RUGGEDCOM ROX II features a detection mechanism to notify users when the compact flash card is removed during operation. When enabled, the system will immediately reboot and generate a failsafe alarm when the card is removed.

This feature is disabled by default.

To enable/disable the compact flash card removal detection mechanism, do the following:

1. Navigate to the **Bootup/Shutdown** tab under **Administration » System**.
2. Select the check box under **CF card removal detection and reboot** to enable the compact flash card removal protection mechanism, or clear it to disable the mechanism.
3. Commit the change.

## 6.4 Enabling/Disabling SYN Cookies

RUGGEDCOM ROX II can be configured to transmit SYN cookies when the SYN backlog queue of a socket begins to overflow. This is a technique used to resist SYN flood attacks.

To enable or disable the transmission of SYN cookies, do the following:

1. Navigate to the **ICMP** tab under **Administration » System**.
2. Under **TCP Syn Cookies**, select the checkbox to enable SYN cookies, or clear the checkbox to disable SYN cookies.
3. Commit the changes.

## 6.5 Managing Cipher Suites

Cipher suites are used by the Secure Socket Layer (SSL) protocol to authenticate server and client connections, transmit certificates, and establish session keys.

RUGGEDCOM ROX II uses grade 4 ciphers and above by default.

It is recommended to always use the strongest cipher suites. However, depending on the SSL version used, some clients and servers may use different ciphers. In these cases, it may be necessary to downgrade select cipher suites to successfully negotiate an SSL handshake between RUGGEDCOM ROX II and the client/server.

For a list of supported ciphers, refer to "Supported Cipher Suites" (Page 862).

### 6.5.1 Viewing Active SSH Server Algorithms

To view which algorithms are currently enabled for the SSH server, do the following:

1. Navigate to **Tools » CLI** and then click **Start**.

2. [Optional] Click **Pop Out** to open the console in a separate dialog box.
3. In the dialog box, enter `config` to enable Configuration mode.
4. Enter the following command to enable a specific algorithm:

```
show running-config admin ssh-config
```

### Example

```
ruggedcom# show running-config admin ssh-config
admin
ssh-config kex-algorithms diffie-hellman-group18-sha512
!
ssh-config kex-algorithms diffie-hellman-group14-sha1
!
ssh-config mac-algorithms hmac-sha2-512
!
ssh-config mac-algorithms hmac-sha2-256
!
ssh-config encryption-algorithms aes256-ctr
!
ssh-config encryption-algorithms aes192-ctr
!
ssh-config encryption-algorithms aes128-ctr
!
ssh-config server-hostkey-algorithms ssh-ed25519
!
!
```

## 6.5.2 Enabling SSH Server and NETCONF Algorithms

To enable an algorithm for the SSH server and NETCONF, do the following:

1. Navigate to **Tools » CLI** and then click **Start**.
2. [Optional] Click **Pop Out** to open the console in a separate dialog box.
3. In the dialog box, enter `config` to enable Configuration mode.
4. Enter the following command to enable a specific cipher suite:

```
admin ssh-config [ encryption-algorithms | kex-algorithms
| mac-algorithms | server-hostkey-algorithms ] { algo
rithm }
```

For a list of cipher suite options, refer to "Service: SSH (TCP/22), NETCONF (TCP/830)" (Page 862).

5. Enter `commit`.

If downgrading to an algorithm lower than grade 4, the following warning will appear:

```
The following warnings were generated:
'admin ssh-config': Warning! You are about to use a weak SSH kex algorithm:
{ algorithms }. Do you want
to continue?
Proceed? [yes, no]
```

Enter **yes** to continue.

6. Enter `top` to return to the top level of the command hierarchy.
7. Enter the following command to reboot the device and enable the selected cipher:

```
admin reboot
```

### Example

```
ruggedcom(config)# admin ssh-config kex-algorithms diffie-hellman-group14-sha1
ruggedcom(config-kex-algorithms-diffie-hellman-group14-sha1)# commit
The following warnings were generated:
'admin ssh-config': Warning! You are about to use a weak SSH kex algorithm:
'diffie-hellman-group14-sha256' or 'diffie-hellman-group14-sha1'. Do you want
to continue?
Proceed? [yes, no] yes
Commit complete.
ruggedcom(config-kex-algorithms-diffie-hellman-group14-sha1)# top
ruggedcom(config)# admin reboot
```

## 6.5.3 Enabling TLS Algorithms

To enable an algorithm for TLS, do the following:

1. Navigate to **Tools » CLI** and then click **Start**.
2. [Optional] Click **Pop Out** to open the console in a separate dialog box.
3. In the dialog box, enter `config` to enable Configuration mode.
4. Enter the following command to enable a specific cipher suite:

```
admin webui tls-config [ cipher-suites | elliptic-curve-
cipher-suites | protocols ] { algorithm }
```

For a list of cipher suite options, refer to "Service: HTTPS Server (TCP/443)" (Page 862).

5. Enter `commit`.

If downgrading to an algorithm lower than grade 4, the following warning will appear:

```
The following warnings were generated:
'admin ssh-config': Warning! You are about to use a weak SSH kex algorithm:
{ algorithms }. Do you want
to continue?
Proceed? [yes, no]
```

Enter **yes** to continue.

6. Enter `top` to return to the top level of the command hierarchy.

**Example**

```
ruggedcom(config)# admin webui tls-config protocols tlsv1.0
ruggedcom(config-protocols-tlsv1.0)# commit
The following warnings were generated:
'admin webui tls-config protocols tlsv1.0': Weak TLS protocol(s) configured:
tlsv1.0 . Proceed with commit?
Proceed? [yes,no] yes
Commit complete.
ruggedcom(config-protocols-tlsv1.0)# top
```

**6.5.4 Configuring the Diffie-Hellman Key Exchange Length**

The Diffie-Hellman key exchange length determines modulus bit size to use when encrypting/decrypting packets exchanged with a client or server.

The default minimal and maximal lengths when not configured are as follows:

	Minimal	Maximal
Default length	2048 bits	4096 bits

These values are sufficient for most users. Increasing the lengths will increase security at a minor cost to network performance.

**Setting the Minimal Key Length**

To set the minimal key length, do the following:

1. Navigate to **Tools » CLI** and then click **Start**.
2. [Optional] Click **Pop Out** to open the console in a separate dialog box.
3. In the dialog box, enter `config` to enable Configuration mode.
4. Enter the following command to set the minimal key length:

```
admin ssh-config dhGroup minSize [ 1024 | 2048 | 4096 |
8192 ]
```

The minimal key length must be less than the maximal key length.

5. Commit the change.

**Setting the Maximal Key Length**

To set the maximal key length, do the following:

1. Navigate to **Tools » CLI** and then click **Start**.
2. [Optional] Click **Pop Out** to open the console in a separate dialog box.
3. In the dialog box, enter `config` to enable Configuration mode.
4. Enter the following command to set the minimal key length:

```
admin ssh-config dhGroup maxSize [ 1024 | 2048 | 4096 |
8192 ]
```



The maximal key length must be greater than the minimal key length.

5. Commit the change.

## 6.6 Managing SFTP Sessions

RUGGEDCOM ROX II supports secure file transfers using the SSH File Transfer Protocol (SFTP). This section describes how to enable and configure SFTP server and client functionality.

### 6.6.1 Enabling and Configuring SFTP Sessions

To enable and configure SFTP server functionality, do the following:

1. Navigate to the **SFTP Sessions** tab under **Administration » Session Config**.
2. Configure the following parameter(s):

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>When enabled, a Secure File Transfer Protocol (SFTP) server may be used to transfer files to and from the device.</p>
Listen IP	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> 0.0.0.0</p> <p>An IPv4 or IPv6 address on which the SFTP server will listen for requests from clients. The default value (i.e. 0.0.0.0) enables the SFTP server to listen for requests via any IP address associated with the server</p>
Listen Port	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p><b>Default:</b> 2222</p> <p>A port on which the SFTP server will listen for requests from clients.</p>
Extra IP Ports	<p><b>Synopsis:</b> A string</p> <p>Additional IPv4 or IPv6 addresses and their associated ports on which the SFTP server will listen for requests from clients. IPv4 addresses and port numbers must be separated by a colon (e.g. 192.168.0.2: 19343). IPv6 addresses and port numbers must be separated by square brackets and a colon (e.g. [2001:db8:2728::2200]:[19343]).</p> <p>If the <b>Listen IP (listen ip)</b> parameter is set to a value other than 0.0.0.0, the port specified by the <b>Listen Port (port)</b> parameter must not be associated with any additional addresses.</p>

Parameter	Description
Maximum Number of SFTP Sessions	<b>Synopsis:</b> An integer <b>Default:</b> 10

3. Add the private key from the SFTP server to the device. For more information, refer to "Adding a Private Key" (Page 180).
4. Commit the changes.

## 6.6.2 Adding an SFTP Server's Public Key

When RUGGEDCOM ROX II is the SFTP client, in order to authenticate the remote server, the public key presented by the server must be added to the device and listed as a known host.

---

### Note

For more information about how SSH client services utilize the known hosts trust store, refer to "Managing Known Hosts" (Page 185).

---

To add an SFTP server's public SSH key, do the following:

1. Determine the server's public SSH key.
2. Take the server's public SSH key and add it to the device. For more information, refer to "Adding a Public Key" (Page 182).
3. Add a new known host to the configuration and associate it with the new public SSH key. For more information, refer to "Adding a Known Host" (Page 186).

## 6.7 Managing Port Security

Port security (or Port Access Control) provides the ability to authenticate access through individual ports, either through IEEE 802.1x authentication, static MAC address-based authorization, or both.

Using IEEE 802.1x authentication, RUGGEDCOM ROX II authenticates a source device against a remote RADIUS authentication server. Access is granted if the source device provides the proper credentials.

Using static MAC address-based authorization, RUGGEDCOM ROX II authenticates the source device based on its MAC address. Access is granted if the MAC address appears on the Static MAC Address table.

---

### Note

RUGGEDCOM ROX II only supports the authentication of one host per port that has the port security mode set to **802.1x** or **802.1x/MAC-Auth**.

---

**Note**

RUGGEDCOM ROX II supports both PEAP and EAP-MD5. PEAP is more secure and is recommended over EAP-MD5.

**⚠ NOTICE**

Do not apply port security on core switch connections. Port security is applied at the end of the network to restrict admission to specific devices.

## 6.7.1 Port Security Concepts

This section describes some of the concepts important to the implementation of port security in RUGGEDCOM ROX II.

### 6.7.1.1 Static MAC Address-Based Authentication

In this method, the device validates the source MAC addresses of received frames against the contents in the Static MAC Address Table. RUGGEDCOM ROX II also supports a highly flexible Port Security configuration that provides a convenient means for network administrators to use the feature in various network scenarios.

A Static MAC address can be configured without a port number being explicitly specified. In this case, the configured MAC address will be automatically authorized on the port where it is detected. This allows devices to be connected to any secure port on the switch without requiring any reconfiguration.

The device can also be programmed to learn (and, thus, authorize) a pre-configured number of the first source MAC addresses encountered on a secure port. This enables the capture of the appropriate secure addresses when first configuring MAC address-based authorization on a port. Those MAC addresses are automatically inserted into the Static MAC Address Table and remain there until explicitly removed by the user.

### 6.7.1.2 Static MAC Address-Based Authentication in an MRP Ring

When port security is configured on a Media Redundancy Client (MRC), the MAC address of the Media Redundancy Manager's (MRM's) ring ports must be configured in the **Static MAC Addresses** table for the ring to remain closed.

To allow communication (i.e. ping) between Media Redundancy Protocol (MRP) devices in a ring, each device with port security enabled on its MRP ports must contain the MAC addresses of all devices in the ring in its **Static MAC Addresses** table.

For information about configuring MRP, refer to "Managing the Media Redundancy Protocol (MRP)" (Page 683).

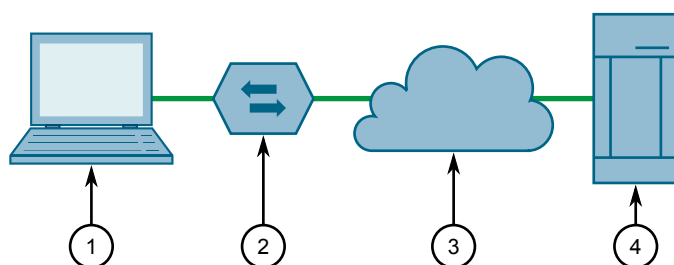
For information about configuring a static MAC address, refer to "Adding a Static MAC Address" (Page 296).

### 6.7.1.3 IEEE 802.1x Authentication

The IEEE 802.1x standard defines a mechanism for port-based network access control and provides a means of authenticating and authorizing devices attached to LAN ports.

Although IEEE 802.1x is mostly used in wireless networks, this method is also implemented in wired switches.

The IEEE 802.1x standard defines three major components of the authentication method: Supplicant, Authenticator and Authentication server. RUGGEDCOM ROX II supports the Authenticator component.



- ① Supplicant
- ② Authenticator Device
- ③ LAN
- ④ Authentication Server

Figure 6.1 IEEE 802.1x General Topology

#### **NOTICE**

RUGGEDCOM ROX II supports both Protected Extensible Authentication Protocol (PEAP) and EAP-MD5. PEAP is more secure and is recommended if available in the supplicant.

IEEE 802.1x makes use of the Extensible Authentication Protocol (EAP), which is a generic PPP authentication protocol that supports various authentication methods. IEEE 802.1x defines a protocol for communication between the Supplicant and the Authenticator, referred to as EAP over LAN (EAPOL).

RUGGEDCOM ROX II communicates with the Authentication Server using EAP over RADIUS. For more information about configuring RADIUS authentication, refer to "Configuring RADIUS Authentication for Switched Ethernet Ports" (Page 149).

#### **Note**

The device supports authentication of one host per port.

**Note**

If the host's MAC address is configured in the Static MAC Address Table, it will be authorized, even if the host authentication is rejected by the authentication server.

---

**6.7.1.4 IEEE 802.1X Authentication with MAC Address-Based Authentication**

This method, also referred to as MAB (MAC-Authentication Bypass), is commonly used for devices, such as VoIP phones and Ethernet printers, that do not support the IEEE 802.1x protocol. This method allows such devices to be authenticated using the same database infrastructure as that used in IEEE 802.1x.

IEEE 802.1x with MAC-Authentication Bypass works as follows:

1. The device connects to a switch port.
2. The switch learns the device MAC address upon receiving the first frame from the device (the device usually sends out a DHCP request message when first connected).
3. The switch sends an EAP Request message to the device, attempting to start IEEE 802.1X authentication.
4. The switch times out while waiting for the EAP reply, because the device does not support IEEE 802.1x.
5. The switch sends an authentication message to the authentication server, using the device MAC address as the username and password.
6. The switch authenticates or rejects the device based on the reply from the authentication server.

**6.7.1.5 Assigning VLANs with Tunnel Attributes**

RUGGEDCOM ROX II supports assigning a VLAN to an authorized port using tunnel attributes, as defined in RFC 3580 [<http://tools.ietf.org/html/rfc3580>], when the Port Security mode is set to **802.1x** or **802.1x/MAC-Auth**.

In some cases, it may be desirable to allow a port to be placed into a particular VLAN, based on the authentication result. For example:

- To allow a particular device, based on its MAC address, to remain on the same VLAN as it moves within a network, configure the switches for 802.1X/MAC-Auth mode
- To allow a particular user, based on the user's login credentials, to remain on the same VLAN when the user logs in from different locations, configure the switches for 802.1X mode

If the RADIUS server wants to use this feature, it indicates the desired VLAN by including tunnel attributes in the Access-Accept message. The RADIUS server uses the following tunnel attributes for VLAN assignment:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note that VLANID is 12-bits and takes a value between 1 and 4094, inclusive. The Tunnel-Private-Group-ID is a string as defined in RFC 2868 [<http://tools.ietf.org/html/rfc2868>], so the VLANID integer value is encoded as a string.

If the tunnel attributes are not returned by the authentication server, the VLAN assigned to the switch port remains unchanged.

## 6.7.2 Configuring Port Security

To configure port security for a switched Ethernet port, do the following:

### Note

Port security can only be configured for switched Ethernet ports. For more information about converting a port to a switched Ethernet port (switchport), refer to "Configuring a Switched Ethernet Port" (Page 276).

1. Navigate to the **Parameters** tab under **Layer 2 » Port Security**, and then click **Port - { interface }**, where { interface } is the switched Ethernet port.

### Note

**Quarantine VID** is only available when **Security Mode** is set to either **dot1x** or **dot1x\_max\_auth**.

**Guest VID** is only available when **Security Mode** is set to **dot1x**.

2. Configure the following parameter(s) as required:

### Note

If **Shutdown Enable** is enabled and **Shutdown Time** is not defined, the port will remain disabled following a security violation until manually reset.

Parameter	Description
Security Mode	<p><b>Synopsis:</b> [ dot1x_mac_auth   dot1x   per_macaddress   off ]</p> <p><b>Default:</b> off</p> <p>The security mode for the port. Options include:</p> <ul style="list-style-type: none"> <li>• <b>dot1x_mac_auth</b> - IEEE 802.1X with MAC authentication protocols are applied to the port. Until the client is authenticated by an IEEE 802.1X server, only EAPoL packets or packets from other network control protocols are forwarded. If the client does not support IEEE 802.1X supplicant functionality, the router sends the client's MAC address to server as the username and password for authentication.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>dot1x</b> - IEEE 802.1X authentication protocols are applied to the port. Until the client is authenticated by an IEEE 802.1X server, only EAPoL packets or packets from other network control protocols are forwarded.</li> <li><b>per_macaddress</b> - Only packets from authorized MAC addresses are forwarded. Authorized MAC addresses are either preconfigured in the static MAC address table or learned dynamically.</li> <li><b>off</b> - Disables security on the port</li> </ul>
Quarantine VID	<p><b>Synopsis:</b> An integer between 1 and 4094</p> <p>The VLAN identifier for the Quarantine VLAN.</p> <p>Only applicable when Security Mode has been set to dot1x or dot1x_mac_auth. The port will be placed in Quarantine VLAN mode if a client cannot be authenticated.</p>
Guest VID	<p><b>Synopsis:</b> An integer between 1 and 4094</p> <p>The VLAN identifier for the Guest VLAN.</p> <p>Only applicable when Security Mode has been set to dot1x. The port will be placed in Guest VLAN mode if a client does not support the 802.1x standard.</p>
Auto Learn	<p><b>Synopsis:</b> An integer between 0 and 16</p> <p><b>Default:</b> 0</p> <p>The maximum number of MAC addresses that can be learned dynamically by the port. This includes static MAC addresses defined in the <b>Static MAC Address</b> table. Therefore, the actual number of learned MAC addresses is this number minus the number of addresses defined in the <b>Static MAC Address</b> table.</p> <p><b>Security Mode</b> must be set to either <b>per_macaddress</b> or <b>dot1x_mac_auth</b>.</p>
Shutdown Time	<p><b>Synopsis:</b> An integer between 1 and 86400</p> <p>The time in seconds (s) the port will be disabled if a security violation occurs.</p> <p><b>Shutdown Enable</b> must be enabled.</p>
Shutdown Enable	<p>When enabled, the port is automatically shut down if a security violation occurs. The port is enabled automatically after the period of time specified by <b>Shutdown Time</b>.</p>

- Click **802.1x**.
- Configure the following parameter(s) as required:

Parameter	Description
Transmission Period	<p><b>Synopsis:</b> An integer between 1 and 65535</p> <p><b>Default:</b> 30</p> <p>The maximum time in seconds (s) allowed for one full set of packets to be transferred between the port and its client.</p>

Parameter	Description
Quiet Period	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p><b>Default:</b> 60</p> <p>The time in seconds (s) to wait before retransmitting EAPoL packets to the client after a failed authentication session.</p>
Reauthorization	<p>When enabled, the port will attempt to reauthenticate the client periodically. The period of time between each reauthentication attempt is specified by <b>Reauthentication Period</b>.</p> <p>The port is considered unauthorized when the maximum number of reauthentication attempts (as defined by <b>Reauthentication Max Attempts</b>) is exceeded.</p>
Reauthorization Period	<p><b>Synopsis:</b> An integer between 60 and 86400</p> <p><b>Default:</b> 3600</p> <p>The period of time in seconds (s) the port will wait before attempting to reauthenticate the client.</p> <p><b>Reauthentication</b> must be enabled.</p>
Reauthorization Max Attempts	<p><b>Synopsis:</b> An integer between 1 and 10</p> <p><b>Default:</b> 2</p> <p>The maximum number of unsuccessful reauthentication attempts allowed, after which the client is considered unauthorized.</p> <p><b>Reauthentication</b> must be enabled.</p>
Supplicant Timeout	<p><b>Synopsis:</b> An integer between 1 and 300</p> <p><b>Default:</b> 30</p> <p>The period of time in seconds (s) the port will wait to receive the client's response to the authentication server's request. If no response is received by the end of this period, the authentication session fails.</p>
Server Timeout	<p><b>Synopsis:</b> An integer between 1 and 300</p> <p><b>Default:</b> 30</p> <p>The period of time in seconds (s) the port will wait to receive the authentication server's response to the client's request. If no response is received by the end of this period, the authentication session fails.</p>
Max Requests	<p><b>Synopsis:</b> An integer between 1 and 10</p> <p><b>Default:</b> 2</p> <p>The maximum number of times the port will attempt to forward the authentication server's request to the client. If none of these attempts are successful, the authentication session fails.</p>

5. If IEEE 802.1x standard authentication or IEEE 802.1x with MAC authentication is selected, configure a primary and secondary RADIUS server. For more



information, refer to "Configuring RADIUS Authentication for Switched Ethernet Ports" (Page 149).

6. Commit the changes.

### 6.7.3 Viewing the Security Status of Switched Ethernet Ports

To view the current security status of a switched Ethernet port, navigate to the **Status** tab under **Layer 2 » Port Security**.

The security status of each port is displayed in the **Status** column.

## 6.8 Managing User Authentication

This section describes the various methods for authenticating users.

### 6.8.1 Setting the User Authentication Mode

The user authentication mode controls whether user log in attempts are authenticated locally, by a RADIUS server, or by a TACACS+ server.

 <b>NOTICE</b>
---

The RADIUS client uses only the Password Authentication Protocol (PAP) protocol to verify access. No other authentication protocol is supported.
--

To set the authentication mode, do the following:

1. Navigate to the **General** tab under **Administration » System » Authentication**.
2. Under **Mode**, select the authentication method.

---

#### Note

A RADIUS server is considered *unreachable* when:

- The server is unavailable at the specified IP address (wrong address configured in the server profile)
  - The server is available, but not listening on the specified port (wrong port configured in the server profile)
  - The server is reachable, but the RADIUS service is not running
  - The server is reachable, but refuses to authenticate the user
- 
- If **localonly** is selected, users will be authenticated locally, regardless of whether or not a RADIUS or TACACS+ server has been configured.

- If **radius\_local** is selected, users will be authenticated against the configured RADIUS server. If the RADIUS server is unreachable, users will be authenticated locally.
  - If **radius\_only** is selected, users will be authenticated against the configured RADIUS server. If the primary RADIUS server is unreachable, the secondary RADIUS server is attempted. If the user still cannot be authenticated, authentication is considered failed and no further authentication is attempted. For console access, if server(s) are unreachable, users will be authenticated locally.
  - If **radius\_then\_local** is selected, users will be authenticated first against the configured RADIUS server. If the user cannot be authenticated, they will then be authenticated locally.
  - If **tacacsplus\_local** is selected, users will be authenticated against the configured TACACS+ server. If the user cannot be authenticated, they will then be authenticated locally.
  - If **tacacsplus\_only** is selected, users will be authenticated against the configured TACACS+ server. If the user cannot be authenticated, authentication is considered failed and no further authentication is attempted.
3. Commit the changes.

## 6.8.2 Managing User Authentication Keys

A user authentication key is the public key in an SSH key pair. When using a RUGGEDCOM ROX II user account associated with an authentication key, users can access the device via Secure Shell (SSH) without having to provide a password/passphrase, as long as their workstation holds the matching private key.

### NOTICE

RUGGEDCOM ROX II only accepts SSH2 RSA public keys. SSH1 or DSA keys are not supported.

### 6.8.2.1 Determining Which Keys are Associated to a User

To list the user authentication keys associated with a user account, Navigate to the **SSH Authorized Keys** tab under **Administration » Users**. A list of user accounts and their associated SSH authorized keys is displayed.

For information about associating keys with user accounts, refer to "Associating/Disassociating a User Authentication Key" (Page 145).

### 6.8.2.2 Adding a User Authentication Key

To add a user authentication key to the device, do the following:

 <b>NOTICE</b>
<b>Security hazard – risk of unauthorized access and/or exploitation</b>
Do not share the private key outside the organization or with untrusted personnel. The private key is used to decrypt all encrypted correspondences with the associated public key.

#### Note

It is strongly recommended to apply an encryption passphrase during the key creation process. The passphrase will be applied to the private key and prevent malicious users from accessing its contents.

#### Note

Only SSH-2 RSA keys are supported.

1. On the workstation that will access the device, create a pair of RSA-based public and private SSH keys.
2. Open the public key and copy its contents.
3. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 23).
4. Navigate to the **Authorized Key** tab under **Administration » Security » Cryptography**.
5. Click **Add Entry**.
6. Configure the following parameter(s) as required:

Parameter	Description
Key Name	<b>Synopsis:</b> A string between 1 and 255 characters long The name of the key.

7. Click **OK**.
8. Paste the contents of the public key into the **Contents** column.
9. Commit the changes.
10. Associate the new authentication key with one or more user accounts. For more information, refer to "Associating/Disassociating a User Authentication Key" (Page 145).

### 6.8.2.3 Deleting a User Authentication Key

To delete a user authentication key from the device, do the following::

1. Navigate to the **Authorized Key** tab under **Administration » Security » Cryptography**.
2. Select the key then click **Delete Entry**.
3. Commit the change.

### 6.8.2.4 Associating/Disassociating a User Authentication Key

One or more user authentication keys can be associated with a single user account, allowing users to access the device from different workstations when needed.

#### NOTICE

The matching public key must reside on the user's workstation for them to log in to the device without a password/passphrase.

### Associating an Authentication Key

To associate one of the authentication keys available on the device with a user account, do the following:

1. Navigate to the **SSH Authorized Keys** tab under **Administration » Users**.
2. For the desired user profile, select the desired authentication key in the **SSH Authorized Keys** column.

If the desired authentication key is not present, add the key. For more information, refer to "Adding a User Authentication Key" (Page 144).

3. Commit the change.

### Disassociating an Authentication Key

To disassociate one of the authentication keys from a user account, do the following:

1. Navigate to the **SSH Authorized Keys** tab under **Administration » Users**.
2. For the desired user profile, click **x** next to the desired authentication key.
3. Commit the change.

## 6.8.3 Managing RADIUS Authentication

RADIUS is a UDP-based protocol used for carrying authentication, authorization and configuration information between a Network Access Server (NAS) that desires to authenticate its links and a shared authentication server. It provides centralized authentication and authorization for network access.

RADIUS is also widely used in conjunction with the IEEE 802.1x standard for port security using the Extensible Authentication Protocol (EAP).

#### Note

For more information about the RADIUS protocol, refer to [RFC 2865 \[http://tools.ietf.org/html/rfc2865\]](http://tools.ietf.org/html/rfc2865).

For more information about the Extensible Authentication Protocol (EAP), refer to [RFC 3748 \[http://tools.ietf.org/html/rfc3748\]](http://tools.ietf.org/html/rfc3748).

#### NOTICE

The user authentication mode must be set to **radius\_local** for users to be authenticated against the RADIUS server. For more information about setting the authentication mode, refer to "Setting the User Authentication Mode" (Page 142).

#### NOTICE

RADIUS messages are sent as UDP messages. The switch and the RADIUS server must use the same authentication and encryption key.

In a RADIUS access request, the following attributes and values are typically sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ Guest, Operator, Admin }
User-Password	{ password }
Service-Type	1
Vendor-Specific	<b>Vendor-ID</b> – 15004 <b>Type</b> – 1 <b>Length</b> – 11 <b>String</b> – RuggedCom

A RADIUS server may also be used to authenticate access on ports with IEEE 802.1x security enabled. When this is required, the following attributes are sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ The user name as derived from the client's EAP identity response }
NAS-IP-Address	{ The Network Access Server IP address }
Service-Type	2
Frame-MTU	1500
EAP-Message <sup>a</sup>	{ A message(s) received from the authenticating peer }

<sup>a</sup> EAP-Message is an extension attribute for RADIUS, as defined by [RFC 2869 \[http://freeradius.org/rfc/rfc2869.html#EAP-Message\]](http://freeradius.org/rfc/rfc2869.html#EAP-Message).

Primary and secondary RADIUS servers, typically operating from a common database, can be configured for redundancy. If the first server does not respond to an authentication request, the request will be forwarded to the second server until a positive/negative acknowledgment is received.

**Note**

RADIUS authentication activity is logged to the authentication log file **var/log/auth.log**. Details of each authentication including the time of occurrence, source and result are included. For more information about the authentication log file, refer to "Viewing Logs" (Page 65).

RUGGEDCOM ROX II supports RADIUS authentication for the LOGIN and PPP services. Different RADIUS servers can be configured to authenticate both services separately or in combination.

The LOGIN services consist of the following access types:

- Local console logins via the serial port
- Remote shell logins via SSH and HTTPS
- Secure file transfers using HTTPS, SCP and SFTP (based on SSH)

Authentication requests for LOGIN services will attempt to use RADIUS first and any local authentication settings will be ignored. Only when there is no response (positive/negative) from any of the configured RADIUS servers will RUGGEDCOM ROX II authenticate users locally.

The PPP service represents incoming PPP connections via a modem. Authentication requests to the PPP service use RADIUS only. In the event that no response is received from any configured RADIUS server, RUGGEDCOM ROX II will not complete the authentication request.

### 6.8.3.1 Configuring RADIUS Authentication for LOGIN Services

To configure RADIUS authentication for LOGIN services, do the following:

 <b>NOTICE</b>
---

Passwords are case-sensitive.
-------------------------------

1. Navigate to the **Remote Logins** tab under **Administration » Security » AAA Servers**.
2. [Optional] If port security is enabled on any ports, under **RADIUS Settings**, configure the following parameters as required to avoid conflicts with firewall rules/policies:

Parameter	Description
NAS IP Address	<p><b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long</p> <p>The NAS-IP-Address. Set this to the primary IP address of the unit.</p>

Parameter	Description
NAS Identifier	<b>Synopsis:</b> A string up to 64 characters long  The NAS-Identifier. If not set, the hostname will be used as the NAS-Identifier.

- Under **Primary Radius Server** and **Secondary Radius Server**, configure the following parameters as required:

Parameter	Description
Primary Radius Server Address	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The IP address of the server.
Primary Radius Server Port UDP	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812  The network port of the server.
Primary Radius Server Password	<b>Synopsis:</b> A string  The password of the RADIUS server.

#### Note

Alternatively, configuring RADIUS authentication for local login, PPP services and switch ports can be combined using the **Populate RADIUS Server** button.

### 6.8.3.2 Configuring RADIUS Authentication for PPP Services

To configure RADIUS authentication for PPP services, do the following:

 <b>NOTICE</b>
Passwords are case-sensitive.

- Navigate to the **PPP** tab under **Administration » Security » AAA Servers**.
- Under **Primary Radius Server**, configure the following parameters as required:

Parameter	Description
Primary Radius Server Address	<b>Synopsis:</b> A string between 7 and 15 characters long  The IPv4 address of the server.
Primary Radius Server Port UDP	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812
Primary Radius Server Password	<b>Synopsis:</b> A string

- Under **Secondary Radius Server**, configure the following parameters as required:

Parameter	Description
Secondary Radius Server Address	<b>Synopsis:</b> A string between 7 and 15 characters long The IPv4 address of the server.
Secondary Radius Server Port UDP	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812
Secondary Radius Server Password	<b>Synopsis:</b> A string

#### Note

Alternatively, configuring RADIUS authentication for local login, PPP services and switch ports can be combined using the **Populate RADIUS Server** button.

### 6.8.3.3 Configuring RADIUS Authentication for Switched Ethernet Ports

To configure RADIUS authentication for switched Ethernet ports, do the following:

#### NOTICE

Passwords are case-sensitive.

- Navigate to the **Switch Ports** tab under **Administration » Security » AAA Servers**.
- Under **Primary Radius Server**, configure the following parameters as required:

Parameter	Description
Primary Radius Server Address	<b>Synopsis:</b> A string between 7 and 15 characters long The IPv4 address of the server.
Primary Radius Server Port UDP	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812
Primary Radius Server Password	<b>Synopsis:</b> A string

- Under **Secondary Radius Server**, configure the following parameters as required:

Parameter	Description
Secondary Radius Server Address	<b>Synopsis:</b> A string between 7 and 15 characters long The IPv4 address of the server.



Parameter	Description
Secondary Radius Server Port UDP	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812
Secondary Radius Server Password	<b>Synopsis:</b> A string

**Note**

Alternatively, configuring RADIUS authentication for local login, PPP services and switch ports can be combined using the **Populate RADIUS Server** button.

## 6.8.4 Configuring TACACS+ Authentication

TACACS+ (Terminal Access Controller Access-Control System Plus) is a TCP-based protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Primary and secondary TACACS+ servers, typically operating from a common database, can be configured for redundancy. If the first server does not respond to an authentication request, the request will be forwarded to the second server until a positive/negate acknowledgment is received.

 **NOTICE**

The user authentication mode must be set to **tacacsplus\_local** or **tacacsplus\_only** for users to be authenticated against the TACACS+ server. For more information about setting the authentication mode, refer to "Setting the User Authentication Mode" (Page 142).

To configure TACACS+ authentication, do the following:

 **NOTICE**

Passwords are case-sensitive.

1. Navigate to the **Remote Logins** tab under **Administration » Security » AAA Servers**.
2. Under **Tacacs+ Settings**, configure the following parameters as required:

Parameter	Description
Admin Privilege Levels	<b>Synopsis:</b> A string up to 5 characters long <b>Default:</b> 15  The privilege level(s) for administrator (admin) users. Options include any number between 0 and 15, or a range (e.g. 4-12).

Parameter	Description
Operator Privilege Levels	<p><b>Synopsis:</b> A string up to 5 characters long  <b>Default:</b> 2-14</p> <p>The privilege level(s) for operator (oper) users. Options include any number between 0 and 15, or a range (e.g. 4-12).</p>
Guest Privilege Levels	<p><b>Synopsis:</b> A string up to 5 characters long  <b>Default:</b> 1</p> <p>The privilege level(s) for guest users. Options include any number between 0 and 15, or a range (e.g. 4-12).</p>

3. Under **Primary TACACS+ Server**, configure the following parameters as required:

Parameter	Description
Primary Tacacs+ Server Address	<p><b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long</p> <p>The IP address of the TACACS+ server.</p>
Primary TACACS+ Server TCP Port	<p><b>Synopsis:</b> An integer between 1 and 65535  <b>Default:</b> 49</p> <p>The TCP port to use when connecting the TACACS+ server. The default port is 49.</p>
Primary TACACS+ Server Authentication Key	<p><b>Synopsis:</b> A string</p> <p>The authentication key to use for encrypting and decrypting TACACS+ traffic. Use only ASCII characters.</p>

4. Under **Secondary TACACS Server**, configure the following parameters as required:

Parameter	Description
Secondary Tacacs+ Server Address	<p><b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long</p> <p>The IP address of the TACACS+ server.</p>
Secondary TACACS+ Server TCP Port	<p><b>Synopsis:</b> An integer between 1 and 65535  <b>Default:</b> 49</p> <p>The TCP port to use when connecting the TACACS+ server. The default port is 49.</p>
Secondary TACACS+ Server Authentication Key	<p><b>Synopsis:</b> A string</p> <p>The authentication key to use for encrypting and decrypting TACACS+ traffic. Use only ASCII characters.</p>

---

**Note**

Alternatively, configuring primary and secondary TACACS+ authentication can be combined using the **Populate TACACS+ Server** button.

---

## 6.9 Managing Certificates and Keys

RUGGEDCOM ROX II uses X.509v3 certificates and keys to establish secure connections for remote logins (SSH) and Web access (SSL).

To allow for initial configuration, all RUGGEDCOM ROX II devices are shipped from the factory with a pair of pre-installed default certificates and keys. Certificates and keys for TLS and SSH are also auto-generated during initial boot-up and can be replaced by user-defined certificates and keys. Auto-generated certificates are self-signed.

**Siemens recommends that all certificates be replaced by ones signed by a trusted Certificate Authority (CA).**

---

**Note**

Only admin users can read/write certificates and keys on the device.

---

### 6.9.1 Viewing the Local Host SSH/RSA Public Key

To view the local host SSH/RSA public key, navigate to the **Localhost SSH RSA Public Key** tab under **Administration » Security » Cryptography**. The **Localhost SSH RSA Public Key** contents are displayed.

### 6.9.2 Configuring Session Security

To provide secure SSH management access (TCP/22), SFTP server access (TCP/2222), and/or HTTPS access TCP/443, certificates and private keys must be selected.

To configure select certificates and private keys, do the following:

1. Navigate to the **General** tab under **Administration » Session Config**.

---

**Note**

Only SSH RSA private keys can be selected for SSH/SFTP server access.

---

2. Under **Session Security**, configure the following parameters as required:

Parameter	Description
Certificate/Private Key	<b>Synopsis:</b> A string between 1 and 255 characters long The certificate name for SSL connections and associated private keys.
Certificate/Private Key	<b>Synopsis:</b> A string between 1 and 255 characters long
SSH RSA Private Key	<b>Synopsis:</b> A string between 1 and 255 characters long The RSA key used for ssh security (SFTP)
ssh-ed25519-private-key	<b>Synopsis:</b> A string between 1 and 255 characters long The ED25519 key used for ssh security (CLI, NETCONF, SFTP)
SSH DSA Private Key	<b>Synopsis:</b> A string between 1 and 255 characters long The DSA key used for ssh security (CLI, NETCONF, SFTP)

For information about adding certificates, refer to "Adding a Certificate" (Page 184).

For information about adding private keys, refer to "Adding a Private Key" (Page 180).

3. Commit the changes.

## 6.9.3 Managing the Trusted Certificate Store

The Trusted Certificate Store includes an extensive collection of publically available X.509 v3 root certificates. Once enabled and associated with one or more Certified Authorities (CAs), these certificates are available for all HTTPS or FTPS operations.

For a list of root certificates included in the Trusted Certificate Store, refer to "List of Root Certificates in the Trusted Certificate Store" (Page 154).

---

### Note

The Trusted Certificate Store is disabled by default.

---

### Note

Custom certificates may be required for select features, such as IPsec tunnels. For more information about adding a custom certificate, refer to "Adding a Certificate" (Page 184).

---

### 6.9.3.1 Configuring the Trusted Certificate Store


To configure the Trusted Certificate Store, do the following:

1. Make sure the required CA certificates and CRLs are configured. For more information, refer to "Adding a CA Certificate and CRL" (Page 179).

### 6.9.3 Managing the Trusted Certificate Store

2. Enable the Trusted Certificate Store. For more information, refer to "Enabling/Disabling the Trusted Certificate Store" (Page 154).
3. Add CA certificates to the Store to validate the authenticity of the root certificates. For more information, refer to "Adding a CA Certificate to the Trusted Certificate Store" (Page 177).

#### 6.9.3.2 Enabling/Disabling the Trusted Certificate Store

 <b>NOTICE</b>
Although the use of the Public CA Store is provided for convenience, it is not recommended for optimal security. Instead, it is recommended to configure the required CAs as system CAs to limit the size of the trust store used by RUGGEDCOM ROX II.
For more information about adding a certificate to the Trusted Certificate Store, refer to "Adding a CA Certificate to the Trusted Certificate Store" (Page 177).

The Trusted Certificate Store is disabled by default.

To enable or disable the Trusted Certificate Store, do the following:

1. Navigate to the **System CA Certificate** tab under **Administration » Security » Cryptography**.
2. Under **Use Public CA Store**, click **Enabled** to enable the Trusted Certificate Store, or clear **Enabled** to disable the Store.
3. Commit the changes.

#### 6.9.3.3 List of Root Certificates in the Trusted Certificate Store

The Trusted Certificate Store adds the following X.509 v3 root certificates when enabled:

- **Entrust.net\_Premium\_2048\_Secure\_Server\_CA.crt**

<b>Subject Name:</b>	O = Entrust.net, OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), OU = (c) 1999 Entrust.net Limited, CN = Entrust.net Certification Authority (2048)
<b>Fingerprint:</b>	6D:C4:71:72:E0:1C:BC:B0:BF:62:58:0D:89:5F:E2:B8:AC:9A:D4:F8:73:80:1E:0C:10:B9:C8:37:D2:1E:B1:77
<b>Issued:</b>	Dec 24 17:50:51 1999 GMT
<b>Expires:</b>	Jul 24 14:15:12 2029 GMT

- **Go\_Daddy\_Class\_2\_CA.crt**

<b>Subject Name:</b>	C = US, O = "The Go Daddy Group, Inc.", OU = Go Daddy Class 2 Certification Authority
<b>Fingerprint:</b>	C3:84:6B:F2:4B:9E:93:CA:64:27:4C:0E:C6:7C:1E:CC:5E:02:4F:FC:AC:D2:D7:40:19:35:0E:81:FE:54:6A:E4
<b>Issued:</b>	Jun 29 17:06:20 2004 GMT

Expires:	Jun 29 17:06:20 2034 GMT
----------	--------------------------

- **Amazon\_Root\_CA\_2.crt**

Subject Name:	C = US, O = Amazon, CN = Amazon Root CA 2
Fingerprint:	1B:A5:B2:AA:8C:65:40:1A:82:96:01:18:F8:0B:EC:4F:62:30:4D:83:CE: C4:71:3A:19:C3:9C:01:1E:A4:6D:B4
Issued:	May 26 00:00:00 2015 GMT
Expires:	May 26 00:00:00 2040 GMT

- **UCA\_Global\_G2\_Root.crt**

Subject Name:	C = CN, O = UniTrust, CN = UCA Global G2 Root
Fingerprint:	9B:EA:11:C9:76:FE:01:47:64:C1:BE:56:A6:F9:14:B5:A5:60:31:7A:BD: 99:88:39:33:82:E5:16:1A:A0:49:3C
Issued:	Mar 11 00:00:00 2016 GMT
Expires:	Dec 31 00:00:00 2040 GMT

- **TrustCor\_RootCert\_CA-1.crt**

Subject Name:	C = PA, ST = Panama, L = Panama City, O = TrustCor Systems S. de R.L., OU = TrustCor Certificate Authority, CN = TrustCor RootCert CA-1
Fingerprint:	D4:0E:9C:86:CD:8F:E4:68:C1:77:69:59:F4:9E:A7:74:FA:54:86:84:B6: C4:06:F3:90:92:61:F4:DC:E2:57:5C
Issued:	Feb 4 12:32:16 2016 GMT
Expires:	Dec 31 17:23:16 2029 GMT

- **SwissSign\_Gold\_CA\_-\_G2.crt**

Subject Name:	C = CH, O = SwissSign AG, CN = SwissSign Gold CA - G2
Fingerprint:	62:DD:0B:E9:B9:F5:0A:16:3E:A0:F8:E7:5C:05:3B:1E:CA:57:EA:55:C8: 68:8F:64:7C:68:81:F2:C8:35:7B:95
Issued:	Oct 25 08:30:35 2006 GMT
Expires:	Oct 25 08:30:35 2036 GMT

- **Cybertrust\_Global\_Root.crt**

Subject Name:	O = "Cybertrust, Inc", CN = Cybertrust Global Root
Fingerprint:	96:0A:DF:00:63:E9:63:56:75:0C:29:65:DD:0A:08:67:DA:0B:9C:BD:6E: 77:71:4A:EA:FB:23:49:AB:39:3D:A3
Issued:	Dec 15 08:00:00 2006 GMT
Expires:	Dec 15 08:00:00 2021 GMT

- **Chambers\_of\_Commerce\_Root\_-\_2008.crt**

Subject Name:	C = EU, L = Madrid (see current address at <a href="http://www.camerfirma.com/">www.camerfirma.com/</a> address), serialNumber = A82743287, O = AC Camerfirma S.A., CN = Chambers of Commerce Root - 2008
Fingerprint:	06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94: 4E:10:A7:93:7E:E2:9D:96:93:C0
Issued:	Aug 1 12:29:50 2008 GMT
Expires:	Jul 31 12:29:50 2038 GMT

- **emSign\_ECC\_Root\_CA\_-\_G3.crt**

<b>Subject Name:</b>	C = IN, OU = emSign PKI, O = eMudhra Technologies Limited, CN = emSign ECC Root CA - G3
<b>Fingerprint:</b>	86:A1:EC:BA:08:9C:4A:8D:3B:BE:27:34:C6:12:BA:34:1D:81:3E:04:3C:F9:E8:A8:62:CD:5C:57:A3:6B:BE:6B
<b>Issued:</b>	Feb 18 18:30:00 2018 GMT
<b>Expires:</b>	Feb 18 18:30:00 2043 GMT

- **AffirmTrust\_Premium\_ECC.crt**

<b>Subject Name:</b>	C = US, O = AffirmTrust, CN = AffirmTrust Premium ECC
<b>Fingerprint:</b>	BD:71:FD:F6:DA:97:E4:CF:62:D1:64:7A:DD:25:81:B0:7D:79:AD:F8:39:7E:B4:EC:BA:9C:5E:84:88:82:14:23
<b>Issued:</b>	Jan 29 14:20:24 2010 GMT
<b>Expires:</b>	Dec 31 14:20:24 2040 GMT

- **Microsec\_e-Szigno\_Root\_CA\_2009.crt**

<b>Subject Name:</b>	C = HU, L = Budapest, O = Microsec Ltd., CN = Microsec e-Szigno Root CA 2009, emailAddress = info@e-szigno.hu
<b>Fingerprint:</b>	3C:5F:81:FE:A5:FA:B8:2C:64:BF:A2:EA:EC:AF:CD:E8:E0:77:FC:86:20:A7:CA:E5:37:16:3D:F3:6E:DB:F3:78
<b>Issued:</b>	Jun 16 11:30:18 2009 GMT
<b>Expires:</b>	Dec 30 11:30:18 2029 GMT

- **Network\_Solutions\_Certificate\_Authority.crt**

<b>Subject Name:</b>	C = US, O = Network Solutions L.L.C., CN = Network Solutions Certificate Authority
<b>Fingerprint:</b>	15:F0:BA:00:A3:AC:7A:F3:AC:88:4C:07:2B:10:11:A0:77:BD:77:C0:97:F4:01:64:B2:F8:59:8A:BD:83:86:0C
<b>Issued:</b>	Dec 1 00:00:00 2006 GMT
<b>Expires:</b>	Dec 31 23:59:59 2029 GMT

- **D-TRUST\_Root\_Class\_3\_CA\_2\_EV\_2009.crt**

<b>Subject Name:</b>	C = DE, O = D-Trust GmbH, CN = D-TRUST Root Class 3 CA 2 EV 2009
<b>Fingerprint:</b>	EE:C5:49:6B:98:8C:E9:86:25:B9:34:09:2E:EC:29:08:BE:D0:B0:F3:16:C2:D4:73:0C:84:EA:F1:F3:D3:48:81
<b>Issued:</b>	Nov 5 08:50:46 2009 GMT
<b>Expires:</b>	Nov 5 08:50:46 2029 GMT

- **COMODO\_RSA\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority
<b>Fingerprint:</b>	52:F0:E1:C4:E5:8E:C6:29:29:1B:60:31:7F:07:46:71:B8:5D:7E:A8:0D:5B:07:27:34:63:53:4B:32:B4:02:34
<b>Issued:</b>	Jan 19 00:00:00 2010 GMT
<b>Expires:</b>	Jan 18 23:59:59 2038 GMT

- **QuoVadis\_Root\_CA.crt**

<b>Subject Name:</b>	C = BM, O = QuoVadis Limited, OU = Root Certification Authority, CN = QuoVadis Root Certification Authority
<b>Fingerprint:</b>	A4:5E:DE:3B:BB:F0:9C:8A:E1:5C:72:EF:C0:72:68:D6:93:A2:1C:99:6F:D5:1E:67:CA:07:94:60:FD:6D:88:73
<b>Issued:</b>	Mar 19 18:33:33 2001 GMT
<b>Expires:</b>	Mar 17 18:33:33 2021 GMT

- **IdenTrust\_Commercial\_Root\_CA\_1.crt**

<b>Subject Name:</b>	C = US, O = IdenTrust, CN = IdenTrust Commercial Root CA 1
<b>Fingerprint:</b>	5D:56:49:9B:E4:D2:E0:8B:CF:CA:D0:8A:3E:38:72:3D:50:50:3B:DE:70:69:48:E4:2F:55:60:30:19:E5:28:AE
<b>Issued:</b>	Jan 16 18:12:23 2014 GMT
<b>Expires:</b>	Jan 16 18:12:23 2034 GMT

- **DigiCert\_High\_Assurance\_EV\_Root\_CA.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert High Assurance EV Root CA
<b>Fingerprint:</b>	74:31:E5:F4:C3:C1:CE:46:90:77:4F:0B:61:E0:54:40:88:3B:A9:A0:1E:D0:0B:A6:AB:D7:80:6E:D3:B1:18:CF
<b>Issued:</b>	Nov 10 00:00:00 2006 GMT
<b>Expires:</b>	Nov 10 00:00:00 2031 GMT

- **TrustCor\_RootCert\_CA-2.crt**

<b>Subject Name:</b>	C = PA, ST = Panama, L = Panama City, O = TrustCor Systems S. de R.L., OU = TrustCor Certificate Authority, CN = TrustCor RootCert CA-2
<b>Fingerprint:</b>	07:53:E9:40:37:8C:1B:D5:E3:83:6E:39:5D:AE:A5:CB:83:9E:50:46:F1:BD:0E:AE:19:51:CF:10:FE:C7:C9:65
<b>Issued:</b>	Feb 4 12:32:23 2016 GMT
<b>Expires:</b>	Dec 31 17:26:39 2034 GMT

- **USERTrust\_RSA\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust RSA Certification Authority
<b>Fingerprint:</b>	E7:93:C9:B0:2F:D8:AA:13:E2:1C:31:22:8A:CC:B0:81:19:64:3B:74:9C:89:89:64:B1:74:6D:46:C3:D4:CB:D2
<b>Issued:</b>	Feb 1 00:00:00 2010 GMT
<b>Expires:</b>	Jan 18 23:59:59 2038 GMT

- **GlobalSign\_Root\_CA\_-\_R3.crt**

<b>Subject Name:</b>	OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
<b>Fingerprint:</b>	CB:B5:22:D7:B7:F1:27:AD:6A:01:13:86:5B:DF:1C:D4:10:2E:7D:07:59:AF:63:5A:7C:F4:72:0D:C9:63:C5:3B
<b>Issued:</b>	Mar 18 10:00:00 2009 GMT
<b>Expires:</b>	Mar 18 10:00:00 2029 GMT



- **XRamp\_Global\_CA\_Root.crt**

<b>Subject Name:</b>	C = US, OU = www.xrampsecurity.com, O = XRamp Security Services Inc, CN = XRamp Global Certification Authority
<b>Fingerprint:</b>	CE:CD:DC:90:50:99:D8:DA:DF:C5:B1:D2:09:B7:37:CB:E2:C1:8C:FB:2C:10:C0:FF:0B:CF:0D:32:86:FC:1A:A2
<b>Issued:</b>	Nov 1 17:14:04 2004 GMT
<b>Expires:</b>	Jan 1 05:37:19 2035 GMT

- **GlobalSign\_Root\_CA\_-\_R2.crt**

<b>Subject Name:</b>	OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
<b>Fingerprint:</b>	CA:42:DD:41:74:5F:D0:B8:1E:B9:02:36:2C:F9:D8:BF:71:9D:A1:BD:1B:1E:FC:94:6F:5B:4C:99:F4:2C:1B:9E
<b>Issued:</b>	Dec 15 08:00:00 2006 GMT
<b>Expires:</b>	Dec 15 08:00:00 2021 GMT

- **E-Tugra\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = TR, L = Ankara, O = E-Tu\C4\9Fra EBG Bili\C5\9Fim Teknolojileri ve Hizmetleri A.\C5\9E., OU = E-Tugra Sertifikasyon Merkezi, CN = E-Tugra Certification Authority
<b>Fingerprint:</b>	B0:BF:D5:2B:B0:D7:D9:BD:92:BF:5D:4D:C1:3D:A2:55:C0:2C:54:2F:37:83:65:EA:89:39:11:F5:5E:55:F2:3C
<b>Issued:</b>	Mar 5 12:09:48 2013 GMT
<b>Expires:</b>	Mar 3 12:09:48 2023 GMT

- **EE\_Certification\_Centre\_Root\_CA.crt**

<b>Subject Name:</b>	C = EE, O = AS Sertifitseerimiskeskus, CN = EE Certification Centre Root CA, emailAddress = pki@sk.ee
<b>Fingerprint:</b>	3E:84:BA:43:42:90:85:16:E7:75:73:C0:99:2F:09:79:CA:08:4E:46:85:68:1F:F1:95:CC:BA:8A:22:9B:8A:76
<b>Issued:</b>	Oct 30 10:10:30 2010 GMT
<b>Expires:</b>	Dec 17 23:59:59 2030 GMT

- **GeoTrust\_Primary\_Certification\_Authority\_-\_G3.crt**

<b>Subject Name:</b>	C = US, O = GeoTrust Inc., OU = (c) 2008 GeoTrust Inc. - For authorized use only, CN = GeoTrust Primary Certification Authority - G3
<b>Fingerprint:</b>	B4:78:B8:12:25:0D:F8:78:63:5C:2A:A7:EC:7D:15:5E:AA:62:5E:E8:29:16:E2:CD:29:43:61:88:6C:D1:FB:D4
<b>Issued:</b>	Apr 2 00:00:00 2008 GMT
<b>Expires:</b>	Dec 1 23:59:59 2037 GMT

- **Staat\_der\_Nederlanden\_Root\_CA\_-\_G3.crt**

<b>Subject Name:</b>	C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden Root CA - G3
<b>Fingerprint:</b>	3C:4F:B0:B9:5A:B8:B3:00:32:F4:32:B8:6F:53:5F:E1:72:C1:85:D0:FD:39:86:58:37:CF:36:18:7F:A6:F4:28
<b>Issued:</b>	Nov 14 11:28:42 2013 GMT
<b>Expires:</b>	Nov 13 23:00:00 2028 GMT

- **SSL.com\_EV\_Root\_Certification\_Authority\_ECC.crt**

<b>Subject Name:</b>	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com EV Root Certification Authority ECC
<b>Fingerprint:</b>	22:A2:C1:F7:BD:ED:70:4C:C1:E7:01:B5:F4:08:C3:10:88:0F:E9:56:B5:DE:2A:4A:44:F9:9C:87:3A:25:A7:C8
<b>Issued:</b>	Feb 12 18:15:23 2016 GMT
<b>Expires:</b>	Feb 12 18:15:23 2041 GMT

- **Entrust\_Root\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = US, O = "Entrust, Inc.", OU = www.entrust.net/CPS is incorporated by reference, OU = "(c) 2006 Entrust, Inc.", CN = Entrust Root Certification Authority
<b>Fingerprint:</b>	73:C1:76:43:4F:1B:C6:D5:AD:F4:5B:0E:76:E7:27:28:7C:8D:E5:76:16:C1:E6:E6:14:1A:2B:2C:BC:7D:8E:4C
<b>Issued:</b>	Nov 27 20:23:42 2006 GMT
<b>Expires:</b>	Nov 27 20:53:42 2026 GMT

- **QuoVadis\_Root\_CA\_1\_G3.crt**

<b>Subject Name:</b>	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 1 G3
<b>Fingerprint:</b>	8A:86:6F:D1:B2:76:B5:7E:57:8E:92:1C:65:82:8A:2B:ED:58:E9:F2:F2:88:05:41:34:B7:F1:F4:BF:C9:CC:74
<b>Issued:</b>	Jan 12 17:27:44 2012 GMT
<b>Expires:</b>	Jan 12 17:27:44 2042 GMT

- **Entrust\_Root\_Certification\_Authority\_-\_EC1.crt**

<b>Subject Name:</b>	C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c) 2012 Entrust, Inc. - for authorized use only", CN = Entrust Root Certification Authority - EC1
<b>Fingerprint:</b>	02:ED:0E:B2:8C:14:DA:45:16:5C:56:67:91:70:0D:64:51:D7:FB:56:F0:B2:AB:1D:3B:8E:B0:70:E5:6E:DF:F5
<b>Issued:</b>	Dec 18 15:25:36 2012 GMT
<b>Expires:</b>	Dec 18 15:55:36 2037 GMT

- **GTS\_Root\_R4.crt**

<b>Subject Name:</b>	C = US, O = Google Trust Services LLC, CN = GTS Root R4
<b>Fingerprint:</b>	71:CC:A5:39:1F:9E:79:4B:04:80:25:30:B3:63:E1:21:DA:8A:30:43:BB:26:66:2F:EA:4D:CA:7F:C9:51:A4:BD
<b>Issued:</b>	Jun 22 00:00:00 2016 GMT
<b>Expires:</b>	Jun 22 00:00:00 2036 GMT

- **thawte\_Primary\_Root\_CA\_-\_G2.crt**

<b>Subject Name:</b>	C = US, O = "thawte, Inc.", OU = "(c) 2007 thawte, Inc. - For authorized use only", CN = thawte Primary Root CA - G2
<b>Fingerprint:</b>	A4:31:0D:50:AF:18:A6:44:71:90:37:2A:86:AF:AF:8B:95:1F:FB:43:1D:83:7F:1E:56:88:B4:59:71:ED:15:57
<b>Issued:</b>	Nov 5 00:00:00 2007 GMT
<b>Expires:</b>	Jan 18 23:59:59 2038 GMT

- **GeoTrust\_Universal\_CA\_2.crt**

<b>Subject Name:</b>	C = US, O = GeoTrust Inc., CN = GeoTrust Universal CA 2
<b>Fingerprint:</b>	A0:23:4F:3B:C8:52:7C:A5:62:8E:EC:81:AD:5D:69:89:5D:A5:68:0D:C9:1D:1C:B8:47:7F:33:F8:78:B9:5B:0B
<b>Issued:</b>	Mar 4 05:00:00 2004 GMT
<b>Expires:</b>	Mar 4 05:00:00 2029 GMT

- **Verisign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G3.crt**

<b>Subject Name:</b>	C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 1999 VeriSign, Inc. - For authorized use only", CN = VeriSign Class 3 Public Primary Certification Authority - G3
<b>Fingerprint:</b>	EB:04:CF:5E:B1:F3:9A:FA:76:2F:2B:B1:20:F2:96:CB:A5:20:C1:B9:7D:B1:58:95:65:B8:1C:B9:A1:7B:72:44
<b>Issued:</b>	Oct 1 00:00:00 1999 GMT
<b>Expires:</b>	Jul 16 23:59:59 2036 GMT

- **GlobalSign\_Root\_CA\_-\_R6.crt**

<b>Subject Name:</b>	OU = GlobalSign Root CA - R6, O = GlobalSign, CN = GlobalSign
<b>Fingerprint:</b>	2C:AB:EA:FE:37:D0:6C:A2:2A:BA:73:91:C0:03:3D:25:98:29:52:C4:53:64:73:49:76:3A:3A:B5:AD:6C:CF:69
<b>Issued:</b>	Dec 10 00:00:00 2014 GMT
<b>Expires:</b>	Dec 10 00:00:00 2034 GMT

- **Buypass\_Class\_3\_Root\_CA.crt**

<b>Subject Name:</b>	C = NO, O = Buypass AS-983163327, CN = Buypass Class 3 Root CA
<b>Fingerprint:</b>	ED:F7:EB:BC:A2:7A:2A:38:4D:38:7B:7D:40:10:C6:66:E2:ED:B4:84:3E:4C:29:B4:AE:1D:5B:93:32:E6:B2:4D
<b>Issued:</b>	Oct 26 08:28:58 2010 GMT
<b>Expires:</b>	Oct 26 08:28:58 2040 GMT

- **GTS\_Root\_R3.crt**

<b>Subject Name:</b>	C = US, O = Google Trust Services LLC, CN = GTS Root R3
<b>Fingerprint:</b>	15:D5:B8:77:46:19:EA:7D:54:CE:1C:A6:D0:B0:C4:03:E0:37:A9:17:F1:31:E8:A0:4E:1E:6B:7A:71:BA:BC:E5
<b>Issued:</b>	Jun 22 00:00:00 2016 GMT
<b>Expires:</b>	Jun 22 00:00:00 2036 GMT

- **VeriSign\_Universal\_Root\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2008 VeriSign, Inc. - For authorized use only", CN = VeriSign Universal Root Certification Authority
<b>Fingerprint:</b>	23:99:56:11:27:A5:71:25:DE:8C:EF:EA:61:0D:DF:2F:A0:78:B5:C8:06:7F:4E:82:82:90:BF:B8:60:E8:4B:3C
<b>Issued:</b>	Apr 2 00:00:00 2008 GMT
<b>Expires:</b>	Dec 1 23:59:59 2037 GMT

- **Entrust\_Root\_Certification\_Authority\_-\_G4.crt**

<b>Subject Name:</b>	C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c) 2015 Entrust, Inc. - for authorized use only", CN = Entrust Root Certification Authority - G4
<b>Fingerprint:</b>	DB:35:17:D1:F6:73:2A:2D:5A:B9:7C:53:3E:C7:07:79:EE:32:70:A6:2F:B4:AC:42:38:37:24:60:E6:F0:1E:88
<b>Issued:</b>	May 27 11:11:16 2015 GMT
<b>Expires:</b>	Dec 27 11:41:16 2037 GMT

- **GlobalSign\_ECC\_Root\_CA\_-\_R5.crt**

<b>Subject Name:</b>	OU = GlobalSign ECC Root CA - R5, O = GlobalSign, CN = GlobalSign
<b>Fingerprint:</b>	17:9F:BC:14:8A:3D:D0:0F:D2:4E:A1:34:58:CC:43:BF:A7:F5:9C:81:82:D7:83:A5:13:F6:EB:EC:10:0C:89:24
<b>Issued:</b>	Nov 13 00:00:00 2012 GMT
<b>Expires:</b>	Jan 19 03:14:07 2038 GMT

- **VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G5.crt**

<b>Subject Name:</b>	C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2006 VeriSign, Inc. - For authorized use only", CN = VeriSign Class 3 Public Primary Certification Authority - G5
<b>Fingerprint:</b>	9A:CF:AB:7E:43:C8:D8:80:D0:6B:26:2A:94:DE:EE:E4:B4:65:99:89:C3:D0:CA:F1:9B:AF:64:05:E4:1A:B7:DF
<b>Issued:</b>	Nov 8 00:00:00 2006 GMT
<b>Expires:</b>	Jul 16 23:59:59 2036 GMT

- **NetLock\_Arany\_=Class\_Gold=\_Főtanúsítvány.crt**

<b>Subject Name:</b>	C = HU, L = Budapest, O = NetLock Kft., OU = Tan\C3\BAs\C3\ADtv\C3\A1nykiad\C3\B3k (Certification Services), CN = NetLock Arany (Class Gold) F\C5\91tan\C3\BAs\C3\ADtv\C3\A1ny
<b>Fingerprint:</b>	6C:61:DA:C3:A2:DE:F0:31:50:6B:E0:36:D2:A6:FE:40:19:94:FB:D1:3D:F9:C8:D4:66:59:92:74:C4:46:EC:98
<b>Issued:</b>	Dec 11 15:08:21 2008 GMT
<b>Expires:</b>	Dec 6 15:08:21 2028 GMT

- **SSL.com\_Root\_Certification\_Authority\_RSA.crt**

<b>Subject Name:</b>	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com Root Certification Authority RSA
<b>Fingerprint:</b>	85:66:6A:56:2E:E0:BE:5C:E9:25:C1:D8:89:0A:6F:76:A8:7E:C1:6D:4D:7D:5F:29:EA:74:19:CF:20:12:3B:69
<b>Issued:</b>	Feb 12 17:39:39 2016 GMT
<b>Expires:</b>	Feb 12 17:39:39 2041 GMT

- **Amazon\_Root\_CA\_1.crt**

<b>Subject Name:</b>	C = US, O = Amazon, CN = Amazon Root CA 1
<b>Fingerprint:</b>	8E:CD:E6:88:4F:3D:87:B1:12:5B:A3:1A:C3:FC:B1:3D:70:16:DE:7F:57:CC:90:4F:E1:CB:97:C6:AE:98:19:6E
<b>Issued:</b>	May 26 00:00:00 2015 GMT
<b>Expires:</b>	Jan 17 00:00:00 2038 GMT

- **thawte\_Primary\_Root\_CA\_-\_G3.crt**

<b>Subject Name:</b>	C = US, O = "thawte, Inc.", OU = Certification Services Division, OU = "(c) 2008 thawte, Inc. - For authorized use only", CN = thawte Primary Root CA - G3
<b>Fingerprint:</b>	4B:03:F4:58:07:AD:70:F2:1B:FC:2C:AE:71:C9:FD:E4:60:4C:06:4C:F5:FF:B6:86:BA:E5:DB:AA:D7:FD:D3:4C
<b>Issued:</b>	Apr 2 00:00:00 2008 GMT
<b>Expires:</b>	Dec 1 23:59:59 2037 GMT

- **QuoVadis\_Root\_CA\_2\_G3.crt**

<b>Subject Name:</b>	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2 G3
<b>Fingerprint:</b>	8F:E4:FB:0A:F9:3A:4D:0D:67:DB:0B:EB:B2:3E:37:C7:1B:F3:25:DC:BC:DD:24:0E:A0:4D:AF:58:B4:7E:18:40
<b>Issued:</b>	Jan 12 18:59:32 2012 GMT
<b>Expires:</b>	Jan 12 18:59:32 2042 GMT

- **DigiCert\_Global\_Root\_CA.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root CA
<b>Fingerprint:</b>	43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61
<b>Issued:</b>	Nov 10 00:00:00 2006 GMT
<b>Expires:</b>	Nov 10 00:00:00 2031 GMT

- **OISTE\_WISeKey\_Global\_Root\_GC\_CA.crt**

<b>Subject Name:</b>	C = CH, O = WISeKey, OU = OISTE Foundation Endorsed, CN = OISTE WISeKey Global Root GC CA
<b>Fingerprint:</b>	85:60:F9:1C:36:24:DA:BA:95:70:B5:FE:A0:DB:E3:6F:F1:1A:83:23:BE:94:86:85:4F:B3:F3:4A:55:71:19:8D
<b>Issued:</b>	May 9 09:48:34 2017 GMT
<b>Expires:</b>	May 9 09:58:33 2042 GMT

- **Security\_Communication\_Root\_CA.crt**

<b>Subject Name:</b>	C = JP, O = SECOM Trust.net, OU = Security Communication RootCA1
<b>Fingerprint:</b>	E7:5E:72:ED:9F:56:0E:EC:6E:B4:80:00:73:A4:3F:C3:AD:19:19:5A:39:22:82:01:78:95:97:4A:99:02:6B:6C
<b>Issued:</b>	Sep 30 04:20:49 2003 GMT
<b>Expires:</b>	Sep 30 04:20:49 2023 GMT

- **TeliaSonera\_Root\_CA\_v1.crt**

<b>Subject Name:</b>	O = TeliaSonera, CN = TeliaSonera Root CA v1
<b>Fingerprint:</b>	DD:69:36:FE:21:F8:F0:77:C1:23:A1:A5:21:C1:22:24:F7:22:55:B7:3E:03:A7:26:06:93:E8:A2:4B:0F:A3:89
<b>Issued:</b>	Oct 18 12:00:50 2007 GMT
<b>Expires:</b>	Oct 18 12:00:50 2032 GMT

- **DigiCert\_Global\_Root\_G2.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
<b>Fingerprint:</b>	CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5F
<b>Issued:</b>	Aug 1 12:00:00 2013 GMT
<b>Expires:</b>	Jan 15 12:00:00 2038 GMT

- **AffirmTrust\_Commercial.crt**

<b>Subject Name:</b>	C = US, O = AffirmTrust, CN = AffirmTrust Commercial
<b>Fingerprint:</b>	03:76:AB:1D:54:C5:F9:80:3C:E4:B2:E2:01:A0:EE:7E:EF:7B:57:B6:36:E8:A9:3C:9B:8D:48:60:C9:6F:5F:A7
<b>Issued:</b>	Jan 29 14:06:06 2010 GMT
<b>Expires:</b>	Dec 31 14:06:06 2030 GMT

- **GeoTrust\_Universal\_CA.crt**

<b>Subject Name:</b>	C = US, O = GeoTrust Inc., CN = GeoTrust Universal CA
<b>Fingerprint:</b>	A0:45:9B:9F:63:B2:25:59:F5:FA:5D:4C:6D:B3:F9:F7:2F:F1:93:42:03:35:78:F0:73:BF:1D:1B:46:CB:B9:12
<b>Issued:</b>	Mar 4 05:00:00 2004 GMT
<b>Expires:</b>	Mar 4 05:00:00 2029 GMT

- **Secure\_Global\_CA.crt**

<b>Subject Name:</b>	C = US, O = SecureTrust Corporation, CN = Secure Global CA
<b>Fingerprint:</b>	42:00:F5:04:3A:C8:59:0E:BB:52:7D:20:9E:D1:50:30:29:FB:CB:D4:1C:A1:B5:06:EC:27:F1:5A:DE:7D:AC:69
<b>Issued:</b>	Nov 7 19:42:28 2006 GMT
<b>Expires:</b>	Dec 31 19:52:06 2029 GMT

- **Sonera\_Class\_2\_Root\_CA.crt**

<b>Subject Name:</b>	C = FI, O = Sonera, CN = Sonera Class2 CA
<b>Fingerprint:</b>	79:08:B4:03:14:C1:38:10:0B:51:8D:07:35:80:7F:FB:FC:F8:51:8A:00:95:33:71:05:BA:38:6B:15:3D:D9:27
<b>Issued:</b>	Apr 6 07:29:40 2001 GMT
<b>Expires:</b>	Apr 6 07:29:40 2021 GMT

- **ACCVRAIZ1.crt**

<b>Subject Name:</b>	CN = ACCVRAIZ1, OU = PKIACCV, O = ACCV, C = ES
<b>Fingerprint:</b>	9A:6E:C0:12:E1:A7:DA:9D:BE:34:19:4D:47:8A:D7:C0:DB:18:22:FB:07:1D:F1:29:81:49:6E:D1:04:38:41:13
<b>Issued:</b>	May 5 09:37:37 2011 GMT
<b>Expires:</b>	Dec 31 09:37:37 2030 GMT

- **SecureTrust\_CA.crt**

<b>Subject Name:</b>	C = US, O = SecureTrust Corporation, CN = SecureTrust CA
<b>Fingerprint:</b>	F1:C1:B5:0A:E5:A2:0D:D8:03:0E:C9:F6:BC:24:82:3D:D3:67:B5:25:57:59:B4:E7:1B:61:FC:E9:F7:37:5D:73

Issued:	Nov 7 19:31:18 2006 GMT
Expires:	Dec 31 19:40:55 2029 GMT

- **Actalis\_Authentication\_Root\_CA.crt**

Subject Name:	C = IT, L = Milan, O = Actalis S.p.A./03358520967, CN = Actalis Authentication Root CA
Fingerprint:	55:92:60:84:EC:96:3A:64:B9:6E:2A:BE:01:CE:0B:A8:6A:64:FB:FE:BC:C7:AA:B5:AF:C1:55:B3:7F:D7:60:66
Issued:	Sep 22 11:22:02 2011 GMT
Expires:	Sep 22 11:22:02 2030 GMT

- **Amazon\_Root\_CA\_4.crt**

Subject Name:	C = US, O = Amazon, CN = Amazon Root CA 4
Fingerprint:	E3:5D:28:41:9E:D0:20:25:CF:A6:90:38:CD:62:39:62:45:8D:A5:C6:95:FB:DE:A3:C2:2B:0B:FB:25:89:70:92
Issued:	May 26 00:00:00 2015 GMT
Expires:	May 26 00:00:00 2040 GMT

- **Certigna.crt**

Subject Name:	C = FR, O = Dhimyotis, CN = Certigna
Fingerprint:	E3:B6:A2:DB:2E:D7:CE:48:84:2F:7A:C5:32:41:C7:B7:1D:54:14:4B:FB:40:C1:1F:3F:1D:0B:42:F5:EE:A1:2D
Issued:	Jun 29 15:13:05 2007 GMT
Expires:	Jun 29 15:13:05 2027 GMT

- **Global\_Chambersign\_Root\_-\_2008.crt**

Subject Name:	C = EU, L = Madrid (see current address at <a href="http://www.camerfirma.com/">www.camerfirma.com/</a> address), serialNumber = A82743287, O = AC Camerfirma S.A., CN = Global Chambersign Root - 2008
Fingerprint:	13:63:35:43:93:34:A7:69:80:16:A0:D3:24:DE:72:28:4E:07:9D:7B:52:20:BB:8F:BD:74:78:16:EE:BE:BA:CA
Issued:	Aug 1 12:31:40 2008 GMT
Expires:	Jul 31 12:31:40 2038 GMT

- **COMODO\_ECC\_Certification\_Authority.crt**

Subject Name:	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO ECC Certification Authority
Fingerprint:	17:93:92:7A:06:14:54:97:89:AD:CE:2F:8F:34:F7:F0:B6:6D:0F:3A:E3:A3:B8:4D:21:EC:15:DB:BA:4F:AD:C7
Issued:	Mar 6 00:00:00 2008 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2011.crt**

Subject Name:	C = GR, O = Hellenic Academic and Research Institutions Cert. Authority, CN = Hellenic Academic and Research Institutions RootCA 2011
Fingerprint:	BC:10:4F:15:A4:8B:E7:09:DC:A5:42:A7:E1:D4:B9:DF:6F:05:45:27:E8:02:EA:A9:2D:59:54:44:25:8A:FE:71
Issued:	Dec 6 13:49:52 2011 GMT

Expires:	Dec 1 13:49:52 2031 GMT
----------	-------------------------

- **Starfield\_Root\_Certificate\_Authority\_-\_G2.crt**

Subject Name:	C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Root Certificate Authority - G2
Fingerprint:	2C:E1:CB:0B:F9:D2:F9:E1:02:99:3F:BE:21:51:52:C3:B2:DD:0C:AB:DE:1C:68:E5:31:9B:83:91:54:DB:B7:F5
Issued:	Sep 1 00:00:00 2009 GMT
Expires:	Dec 31 23:59:59 2037 GMT

- **T-TeleSec\_GlobalRoot\_Class\_2.crt**

Subject Name:	C = DE, O = T-Systems Enterprise Services GmbH, OU = T-Systems Trust Center, CN = T-TeleSec GlobalRoot Class 2
Fingerprint:	91:E2:F5:78:8D:58:10:EB:A7:BA:58:73:7D:E1:54:8A:8E:CA:CD:01:45:98:BC:0B:14:3E:04:1B:17:05:25:52
Issued:	Oct 1 10:40:14 2008 GMT
Expires:	Oct 1 23:59:59 2033 GMT

- **TrustCor\_ECA-1.crt**

Subject Name:	C = PA, ST = Panama, L = Panama City, O = TrustCor Systems S. de R.L., OU = TrustCor Certificate Authority, CN = TrustCor ECA-1
Fingerprint:	5A:88:5D:B1:9C:01:D9:12:C5:75:93:88:93:8C:AF:BB:DF:03:1A:B2:D4:8E:91:EE:15:58:9B:42:97:1D:03:9C
Issued:	Feb 4 12:32:33 2016 GMT
Expires:	Dec 31 17:28:07 2029 GMT

- **ISRG\_Root\_X1.crt**

Subject Name:	C = US, O = Internet Security Research Group, CN = ISRG Root X1
Fingerprint:	96:BC:EC:06:26:49:76:F3:74:60:77:9A:CF:28:C5:A7:CF:E8:A3:C0:AA:E1:1A:8F:FC:EE:05:C0:BD:DF:08:C6
Issued:	Jun 4 11:04:38 2015 GMT
Expires:	Jun 4 11:04:38 2035 GMT

- **Comodo\_AAA\_Services\_root.crt**

Subject Name:	C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = AAA Certificate Services
Fingerprint:	D7:A7:A0:FB:5D:7E:27:31:D7:71:E9:48:4E:BC:DE:F7:1D:5F:0C:3E:0A:29:48:78:2B:C8:3E:E0:EA:69:9E:F4
Issued:	Jan 1 00:00:00 2004 GMT
Expires:	Dec 31 23:59:59 2028 GMT

- **QuoVadis\_Root\_CA\_2.crt**

Subject Name:	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2
Fingerprint:	85:A0:DD:7D:D7:20:AD:B7:FF:05:F8:3D:54:2B:20:9D:C7:FF:45:28:F7:D6:77:B1:83:89:FE:A5:E5:C4:9E:86
Issued:	Nov 24 18:27:00 2006 GMT
Expires:	Nov 24 18:23:33 2031 GMT



- **GeoTrust\_Primary\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = US, O = GeoTrust Inc., CN = GeoTrust Primary Certification Authority
<b>Fingerprint:</b>	37:D5:10:06:C5:12:EA:AB:62:64:21:F1:EC:8C:92:01:3F:C5:F8:2A:E9:8E: E5:33:EB:46:19:B8:DE:B4:D0:6C
<b>Issued:</b>	Nov 27 00:00:00 2006 GMT
<b>Expires:</b>	Jul 16 23:59:59 2036 GMT

- **QuoVadis\_Root\_CA\_3.crt**

<b>Subject Name:</b>	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 3
<b>Fingerprint:</b>	18:F1:FC:7F:20:5D:F8:AD:DD:EB:7F:E0:07:DD:57:E3:AF:37:5A:9C:4D:8D: 73:54:6B:F4:F1:FE:D1:E1:8D:35
<b>Issued:</b>	Nov 24 19:11:23 2006 GMT
<b>Expires:</b>	Nov 24 19:06:44 2031 GMT

- **GlobalSign\_ECC\_Root\_CA\_-\_R4.crt**

<b>Subject Name:</b>	OU = GlobalSign ECC Root CA - R4, O = GlobalSign, CN = GlobalSign
<b>Fingerprint:</b>	BE:C9:49:11:C2:95:56:76:DB:6C:0A:55:09:86:D7:6E:3B:A0:05:66:7C:44: 2C:97:62:B4:FB:B7:73:DE:22:8C
<b>Issued:</b>	Nov 13 00:00:00 2012 GMT
<b>Expires:</b>	Jan 19 03:14:07 2038 GMT

- **COMODO\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO Certification Authority
<b>Fingerprint:</b>	0C:2C:D6:3D:F7:80:6F:A3:99:ED:E8:09:11:6B:57:5B:F8:79:89:F0:65:18: F9:80:8C:86:05:03:17:8B:AF:66
<b>Issued:</b>	Dec 1 00:00:00 2006 GMT
<b>Expires:</b>	Dec 31 23:59:59 2029 GMT

- **OISTE\_WISEKey\_Global\_Root\_GB\_CA.crt**

<b>Subject Name:</b>	C = CH, O = WISEKey, OU = OISTE Foundation Endorsed, CN = OISTE WISEKey Global Root GB CA
<b>Fingerprint:</b>	6B:9C:08:E8:6E:B0:F7:67:CF:AD:65:CD:98:B6:21:49:E5:49:4A:67:F5:84: 5E:7B:D1:ED:01:9F:27:B8:6B:D6
<b>Issued:</b>	Dec 1 15:00:32 2014 GMT
<b>Expires:</b>	Dec 1 15:10:31 2039 GMT

- **USERTrust\_ECC\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust ECC Certification Authority
<b>Fingerprint:</b>	4F:F4:60:D5:4B:9C:86:DA:BF:BC:FC:57:12:E0:40:0D:2B:ED:3F:BC:4D:4F: BD:AA:86:E0:6A:DC:D2:A9:AD:7A
<b>Issued:</b>	Feb 1 00:00:00 2010 GMT
<b>Expires:</b>	Jan 18 23:59:59 2038 GMT

- **DigiCert\_Assured\_ID\_Root\_G3.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root G3
<b>Fingerprint:</b>	7E:37:CB:8B:4C:47:09:0C:AB:36:55:1B:A6:F4:5D:B8:40:68:0F:BA:16:6A:95:2D:B1:00:71:7F:43:05:3F:C2
<b>Issued:</b>	Aug 1 12:00:00 2013 GMT
<b>Expires:</b>	Jan 15 12:00:00 2038 GMT

- **GlobalSign\_Root\_CA.crt**

<b>Subject Name:</b>	C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
<b>Fingerprint:</b>	EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
<b>Issued:</b>	Sep 1 12:00:00 1998 GMT
<b>Expires:</b>	Jan 28 12:00:00 2028 GMT

- **Hongkong\_Post\_Root\_CA\_1.crt**

<b>Subject Name:</b>	C = HK, O = Hongkong Post, CN = Hongkong Post Root CA 1
<b>Fingerprint:</b>	F9:E6:7D:33:6C:51:00:2A:C0:54:C6:32:02:2D:66:DD:A2:E7:E3:FF:F1:0A:D0:61:ED:31:D8:BB:B4:10:CF:B2
<b>Issued:</b>	May 15 05:13:14 2003 GMT
<b>Expires:</b>	May 15 04:52:29 2023 GMT

- **Entrust\_Root\_Certification\_Authority\_-\_G2.crt**

<b>Subject Name:</b>	C = US, O = "Entrust, Inc.", OU = See www.entrust.net/legal-terms, OU = "(c) 2009 Entrust, Inc. - for authorized use only", CN = Entrust Root Certification Authority - G2
<b>Fingerprint:</b>	43:DF:57:74:B0:3E:7F:EF:5F:E4:0D:93:1A:7B:ED:F1:BB:2E:6B:42:73:8C:4E:6D:38:41:10:3D:3A:A7:F3:39
<b>Issued:</b>	Jul 7 17:25:54 2009 GMT
<b>Expires:</b>	Dec 7 17:55:54 2030 GMT

- **T-TeleSec\_GlobalRoot\_Class\_3.crt**

<b>Subject Name:</b>	C = DE, O = T-Systems Enterprise Services GmbH, OU = T-Systems Trust Center, CN = T-TeleSec GlobalRoot Class 3
<b>Fingerprint:</b>	FD:73:DA:D3:1C:64:4F:F1:B4:3B:EF:0C:CD:DA:96:71:0B:9C:D9:87:5E:CA:7E:31:70:7A:F3:E9:6D:52:2B:BD
<b>Issued:</b>	Oct 1 10:29:56 2008 GMT
<b>Expires:</b>	Oct 1 23:59:59 2033 GMT

- **SecureSign\_RootCA11.crt**

<b>Subject Name:</b>	C = JP, O = "Japan Certification Services, Inc.", CN = SecureSign RootCA11
<b>Fingerprint:</b>	BF:0F:EE:FB:9E:3A:58:1A:D5:F9:E9:DB:75:89:98:57:43:D2:61:08:5C:4D:31:4F:6F:5D:72:59:AA:42:16:12
<b>Issued:</b>	Apr 8 04:56:47 2009 GMT
<b>Expires:</b>	Apr 8 04:56:47 2029 GMT

- **DigiCert\_Trusted\_Root\_G4.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Trusted Root G4
<b>Fingerprint:</b>	55:2F:7B:DC:F1:A7:AF:9E:6C:E6:72:01:7F:4F:12:AB:F7:72:40:C7:8E:76:1A:C2:03:D1:D9:D2:0A:C8:99:88
<b>Issued:</b>	Aug 1 12:00:00 2013 GMT
<b>Expires:</b>	Jan 15 12:00:00 2038 GMT

- **LuxTrust\_Global\_Root\_2.crt**

<b>Subject Name:</b>	C = LU, O = LuxTrust S.A., CN = LuxTrust Global Root 2
<b>Fingerprint:</b>	54:45:5F:71:29:C2:0B:14:47:C4:18:F9:97:16:8F:24:C5:8F:C5:02:3B:F5:DA:5B:E2:EB:6E:1D:D8:90:2E:D5
<b>Issued:</b>	Mar 5 13:21:57 2015 GMT
<b>Expires:</b>	Mar 5 13:21:57 2035 GMT

- **SwissSign\_Silver\_CA\_-\_G2.crt**

<b>Subject Name:</b>	C = CH, O = SwissSign AG, CN = SwissSign Silver CA - G2
<b>Fingerprint:</b>	BE:6C:4D:A2:BB:B9:BA:59:B6:F3:93:97:68:37:42:46:C3:C0:05:99:3F:A9:8F:02:0D:1D:ED:BE:D4:8A:81:D5
<b>Issued:</b>	Oct 25 08:32:46 2006 GMT
<b>Expires:</b>	Oct 25 08:32:46 2036 GMT

- **CFCA\_EV\_ROOT.crt**

<b>Subject Name:</b>	C = CN, O = China Financial Certification Authority, CN = CFCA EV ROOT
<b>Fingerprint:</b>	5C:C3:D7:8E:4E:1D:5E:45:54:7A:04:E6:87:3E:64:F9:0C:F9:53:6D:1C:CC:2E:F8:00:F3:55:C4:C5:FD:70:FD
<b>Issued:</b>	Aug 8 03:07:01 2012 GMT
<b>Expires:</b>	Dec 31 03:07:01 2029 GMT

- **certSIGN\_ROOT\_CA.crt**

<b>Subject Name:</b>	C = RO, O = certSIGN, OU = certSIGN ROOT CA
<b>Fingerprint:</b>	EA:A9:62:C4:FA:4A:6B:AF:EB:E4:15:19:6D:35:1C:CD:88:8D:4F:53:F3:FA:8A:E6:D7:C4:66:A9:4E:60:42:BB
<b>Issued:</b>	Jul 4 17:20:04 2006 GMT
<b>Expires:</b>	Jul 4 17:20:04 2031 GMT

- **Starfield\_Services\_Root\_Certificate\_Authority\_-\_G2.crt**

<b>Subject Name:</b>	C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Services Root Certificate Authority - G2
<b>Fingerprint:</b>	56:8D:69:05:A2:C8:87:08:A4:B3:02:51:90:ED:CF:ED:B1:97:4A:60:6A:13:C6:E5:29:0F:CB:2A:E6:3E:DA:B5
<b>Issued:</b>	Sep 1 00:00:00 2009 GMT
<b>Expires:</b>	Dec 31 23:59:59 2037 GMT

- **emSign\_Root\_CA\_-\_C1.crt**

<b>Subject Name:</b>	C = US, OU = emSign PKI, O = eMudhra Inc, CN = emSign Root CA - C1
----------------------	--

<b>Fingerprint:</b>	12:56:09:AA:30:1D:A0:A2:49:B9:7A:82:39:CB:6A:34:21:6F:44:DC:AC:9F:39:54:B1:42:92:F2:E8:C8:60:8F
<b>Issued:</b>	Feb 18 18:30:00 2018 GMT
<b>Expires:</b>	Feb 18 18:30:00 2043 GMT

- **AffirmTrust\_Networking.crt**

<b>Subject Name:</b>	C = US, O = AffirmTrust, CN = AffirmTrust Networking
<b>Fingerprint:</b>	0A:81:EC:5A:92:97:77:F1:45:90:4A:F3:8D:5D:50:9F:66:B5:E2:C5:8F:CD:B5:31:05:8B:0E:17:F3:F0:B4:1B
<b>Issued:</b>	Jan 29 14:08:24 2010 GMT
<b>Expires:</b>	Dec 31 14:08:24 2030 GMT

- **DST\_Root\_CA\_X3.crt**

<b>Subject Name:</b>	O = Digital Signature Trust Co., CN = DST Root CA X3
<b>Fingerprint:</b>	06:87:26:03:31:A7:24:03:D9:09:F1:05:E6:9B:CF:0D:32:E1:BD:24:93:FF:C6:D9:20:6D:11:BC:D6:77:07:39
<b>Issued:</b>	Sep 30 21:12:19 2000 GMT
<b>Expires:</b>	Sep 30 14:01:15 2021 GMT

- **SSL.com\_EV\_Root\_Certification\_Authority\_RSA\_R2.crt**

<b>Subject Name:</b>	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com EV Root Certification Authority RSA R2
<b>Fingerprint:</b>	2E:7B:F1:6C:C2:24:85:A7:BB:E2:AA:86:96:75:07:61:B0:AE:39:BE:3B:2F:E9:D0:CC:6D:4E:F7:34:91:42:5C
<b>Issued:</b>	May 31 18:14:37 2017 GMT
<b>Expires:</b>	May 30 18:14:37 2042 GMT

- **UCA\_Extended\_Validation\_Root.crt**

<b>Subject Name:</b>	C = CN, O = UniTrust, CN = UCA Extended Validation Root
<b>Fingerprint:</b>	D4:3A:F9:B3:54:73:75:5C:96:84:FC:06:D7:D8:CB:70:EE:5C:28:E7:73:FB:29:4E:B4:1E:E7:17:22:92:4D:24
<b>Issued:</b>	Mar 13 00:00:00 2015 GMT
<b>Expires:</b>	Dec 31 00:00:00 2038 GMT

- **emSign\_ECC\_Root\_CA\_-\_C3.crt**

<b>Subject Name:</b>	C = US, OU = emSign PKI, O = eMudhra Inc, CN = emSign ECC Root CA - C3
<b>Fingerprint:</b>	BC:4D:80:9B:15:18:9D:78:DB:3E:1D:8C:F4:F9:72:6A:79:5D:A1:64:3C:A5:F1:35:8E:1D:DB:0E:DC:0D:7E:B3
<b>Issued:</b>	Feb 18 18:30:00 2018 GMT
<b>Expires:</b>	Feb 18 18:30:00 2043 GMT

- **D-TRUST\_Root\_Class\_3\_CA\_2\_2009.crt**

<b>Subject Name:</b>	C = DE, O = D-Trust GmbH, CN = D-TRUST Root Class 3 CA 2 2009
<b>Fingerprint:</b>	49:E7:A4:42:AC:F0:EA:62:87:05:00:54:B5:25:64:B6:50:E4:F4:9E:42:E3:48:D6:AA:38:E0:39:E9:57:B1:C1
<b>Issued:</b>	Nov 5 08:35:58 2009 GMT

Expires:	Nov 5 08:35:58 2029 GMT
----------	-------------------------

- **AC\_RAIZ\_FNMT-RCM.crt**

Subject Name:	C = ES, O = FNMT-RCM, OU = AC RAIZ FNMT-RCM
Fingerprint:	EB:C5:57:0C:29:01:8C:4D:67:B1:AA:12:7B:AF:12:F7:03:B4:61:1E:BC:17: B7:DA:B5:57:38:94:17:9B:93:FA
Issued:	Oct 29 15:59:56 2008 GMT
Expires:	Jan 1 00:00:00 2030 GMT

- **SZAFIR\_ROOT\_CA2.crt**

Subject Name:	C = PL, O = Krajowa Izba Rozliczeniowa S.A., CN = SZAFIR ROOT CA2
Fingerprint:	A1:33:9D:33:28:1A:0B:56:E5:57:D3:D3:2B:1C:E7:F9:36:7E:B0:94:BD:5F: A7:2A:7E:50:04:C8:DE:D7:CA:FE
Issued:	Oct 19 07:43:30 2015 GMT
Expires:	Oct 19 07:43:30 2035 GMT

- **Taiwan\_GRCA.crt**

Subject Name:	C = TW, O = Government Root Certification Authority
Fingerprint:	76:00:29:5E:EF:E8:5B:9E:1F:D6:24:DB:76:06:2A:AA:AE:59:81:8A:54:D2: 77:4C:D4:C0:B2:C0:11:31:E1:B3
Issued:	Dec 5 13:23:33 2002 GMT
Expires:	Dec 5 13:23:33 2032 GMT

- **Izenpe.com.crt**

Subject Name:	C = ES, O = IZENPE S.A., CN = Izenpe.com
Fingerprint:	25:30:CC:8E:98:32:15:02:BA:D9:6F:9B:1F:BA:1B:09:9E:2D:29:9E:0F:45: 48:BB:91:4F:36:3B:C0:D4:53:1F
Issued:	Dec 13 13:08:28 2007 GMT
Expires:	Dec 13 08:27:25 2037 GMT

- **Certum\_Trusted\_Network\_CA\_2.crt**

Subject Name:	C = PL, O = Unizeto Technologies S.A., OU = Certum Certification Authority, CN = Certum Trusted Network CA 2
Fingerprint:	B6:76:F2:ED:DA:E8:77:5C:D3:6C:B0:F6:3C:D1:D4:60:39:61:F4:9E:62:65: BA:01:3A:2F:03:07:B6:D0:B8:04
Issued:	Oct 6 08:39:56 2011 GMT
Expires:	Oct 6 08:39:56 2046 GMT

- **Staat\_der\_Nederlanden\_Root\_CA\_-\_G2.crt**

Subject Name:	C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden Root CA - G2
Fingerprint:	66:8C:83:94:7D:A6:3B:72:4B:EC:E1:74:3C:31:A0:E6:AE:D0:DB:8E:C5:B3: 1B:E3:77:BB:78:4F:91:B6:71:6F
Issued:	Mar 26 11:18:17 2008 GMT
Expires:	Mar 25 11:03:10 2020 GMT

- **GTS\_Root\_R1.crt**

<b>Subject Name:</b>	C = US, O = Google Trust Services LLC, CN = GTS Root R1
<b>Fingerprint:</b>	2A:57:54:71:E3:13:40:BC:21:58:1C:BD:2C:F1:3E:15:84:63:20:3E:CE:94: BC:F9:D3:CC:19:6B:F0:9A:54:72
<b>Issued:</b>	Jun 22 00:00:00 2016 GMT
<b>Expires:</b>	Jun 22 00:00:00 2036 GMT

- **Hellenic\_Academic\_and\_Research\_Institutions\_ECC\_RootCA\_2015.crt**

<b>Subject Name:</b>	C = GR, L = Athens, O = Hellenic Academic and Research Institutions Cert. Authority, CN = Hellenic Academic and Research Institutions ECC RootCA 2015
<b>Fingerprint:</b>	44:B5:45:AA:8A:25:E6:5A:73:CA:15:DC:27:FC:36:D2:4C:1C:B9:95:3A:06: 65:39:B1:15:82:DC:48:7B:48:33
<b>Issued:</b>	Jul 7 10:37:12 2015 GMT
<b>Expires:</b>	Jun 30 10:37:12 2040 GMT

- **ePKI\_Root\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = TW, O = "Chunghwa Telecom Co., Ltd.", OU = ePKI Root Certification Authority
<b>Fingerprint:</b>	C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6A:08:2A:0A:72:DE:35:80:3E:2F: F5:FF:52:7A:E5:D8:72:06:DF:D5
<b>Issued:</b>	Dec 20 02:31:27 2004 GMT
<b>Expires:</b>	Dec 20 02:31:27 2034 GMT

- **GTS\_Root\_R2.crt**

<b>Subject Name:</b>	C = US, O = Google Trust Services LLC, CN = GTS Root R2
<b>Fingerprint:</b>	C4:5D:7B:B0:8E:6D:67:E6:2E:42:35:11:0B:56:4E:5F:78:FD:92:EF:05:8C: 84:0A:EA:4E:64:55:D7:58:5C:60
<b>Issued:</b>	Jun 22 00:00:00 2016 GMT
<b>Expires:</b>	Jun 22 00:00:00 2036 GMT

- **VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G4.crt**

<b>Subject Name:</b>	C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2007 VeriSign, Inc. - For authorized use only", CN = VeriSign Class 3 Public Primary Certification Authority - G4
<b>Fingerprint:</b>	69:DD:D7:EA:90:BB:57:C9:3E:13:5D:C8:5E:A6:FC:D5:48:0B:60:32:39:BD: C4:54:FC:75:8B:2A:26:CF:7F:79
<b>Issued:</b>	Nov 5 00:00:00 2007 GMT
<b>Expires:</b>	Jan 18 23:59:59 2038 GMT

- **DigiCert\_Global\_Root\_G3.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3
<b>Fingerprint:</b>	31:AD:66:48:F8:10:41:38:C7:38:F3:9E:A4:32:01:33:39:3E:3A:18:CC:02: 29:6E:F9:7C:2A:C9:EF:67:31:D0
<b>Issued:</b>	Aug 1 12:00:00 2013 GMT
<b>Expires:</b>	Jan 15 12:00:00 2038 GMT

- **Starfield\_Class\_2\_CA.crt**

<b>Subject Name:</b>	C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification Authority
<b>Fingerprint:</b>	14:65:FA:20:53:97:B8:76:FA:A6:F0:A9:95:8E:55:90:E4:0F:CC:7F:AA:4F:B7:C2:C8:67:75:21:FB:5F:B6:58
<b>Issued:</b>	Jun 29 17:39:16 2004 GMT
<b>Expires:</b>	Jun 29 17:39:16 2034 GMT

- **IdenTrust\_Public\_Sector\_Root\_CA\_1.crt**

<b>Subject Name:</b>	C = US, O = IdenTrust, CN = IdenTrust Public Sector Root CA 1
<b>Fingerprint:</b>	30:D0:89:5A:9A:44:8A:26:20:91:63:55:22:D1:F5:20:10:B5:86:7A:CA:E1:2C:78:EF:95:8F:D4:F4:38:9F:2F
<b>Issued:</b>	Jan 16 17:53:32 2014 GMT
<b>Expires:</b>	Jan 16 17:53:32 2034 GMT

- **Baltimore\_CyberTrust\_Root.crt**

<b>Subject Name:</b>	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
<b>Fingerprint:</b>	16:AF:57:A9:F6:76:B0:AB:12:60:95:AA:5E:BA:DE:F2:2A:B3:11:19:D6:44:AC:95:CD:4B:93:DB:F3:F2:6A:EB
<b>Issued:</b>	May 12 18:46:00 2000 GMT
<b>Expires:</b>	May 12 23:59:00 2025 GMT

- **EC-ACC.crt**

<b>Subject Name:</b>	C = ES, O = Agencia Catalana de Certificacio (NIF Q-0801176-I), OU = Serveis Publics de Certificacio, OU = Vegeu <a href="https://www.catcert.net/verarrel">https://www.catcert.net/verarrel</a> (c)03, OU = Jerarquia Entitats de Certificacio Catalanes, CN = EC-ACC
<b>Fingerprint:</b>	88:49:7F:01:60:2F:31:54:24:6A:E2:8C:4D:5A:EF:10:F1:D8:7E:BB:76:62:6F:4A:E0:B7:F9:5B:A7:96:87:99
<b>Issued:</b>	Jan 7 23:00:00 2003 GMT
<b>Expires:</b>	Jan 7 22:59:59 2031 GMT

- **TWCA\_Root\_Certification\_Authority.crt**

<b>Subject Name:</b>	C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Root Certification Authority
<b>Fingerprint:</b>	BF:D8:8F:E1:10:1C:41:AE:3E:80:1B:F8:BE:56:35:0E:E9:BA:D1:A6:B9:BD:51:5E:DC:5C:6D:5B:87:11:AC:44
<b>Issued:</b>	Aug 28 07:24:33 2008 GMT
<b>Expires:</b>	Dec 31 15:59:59 2030 GMT

- **DigiCert\_Assured\_ID\_Root\_G2.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root G2
<b>Fingerprint:</b>	7D:05:EB:B6:82:33:9F:8C:94:51:EE:09:4E:EB:FE:FA:79:53:A1:14:ED:B2:F4:49:49:45:2F:AB:7D:2F:C1:85
<b>Issued:</b>	Aug 1 12:00:00 2013 GMT
<b>Expires:</b>	Jan 15 12:00:00 2038 GMT

- **Staat\_der\_Nederlanden\_EV\_Root\_CA.crt**

<b>Subject Name:</b>	C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden EV Root CA
<b>Fingerprint:</b>	4D:24:91:41:4C:FE:95:67:46:EC:4C:EF:A6:CF:6F:72:E2:8A:13:29:43:2F:9D:8A:90:7A:C4:CB:5D:AD:C1:5A
<b>Issued:</b>	Dec 8 11:19:29 2010 GMT
<b>Expires:</b>	Dec 8 11:10:28 2022 GMT

- **TWCA\_Global\_Root\_CA.crt**

<b>Subject Name:</b>	C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Global Root CA
<b>Fingerprint:</b>	59:76:90:07:F7:68:5D:0F:CD:50:87:2F:9F:95:D5:75:5A:5B:2B:45:7D:81:F3:69:2B:61:0A:98:67:2F:0E:1B
<b>Issued:</b>	Jun 27 06:28:33 2012 GMT
<b>Expires:</b>	Dec 31 15:59:59 2030 GMT

- **Trustis\_FPS\_Root\_CA.crt**

<b>Subject Name:</b>	C = GB, O = Trustis Limited, OU = Trustis FPS Root CA
<b>Fingerprint:</b>	C1:B4:82:99:AB:A5:20:8F:E9:63:0A:CE:55:CA:68:A0:3E:DA:5A:51:9C:88:02:A0:D3:A6:73:BE:8F:8E:55:7D
<b>Issued:</b>	Dec 23 12:14:06 2003 GMT
<b>Expires:</b>	Jan 21 11:36:54 2024 GMT

- **Certigna\_Root\_CA.crt**

<b>Subject Name:</b>	C = FR, O = Dhimyotis, OU = 0002 48146308100036, CN = Certigna Root CA
<b>Fingerprint:</b>	D4:8D:3D:23:EE:DB:50:A4:59:E5:51:97:60:1C:27:77:4B:9D:7B:18:C9:4D:5A:05:95:11:A1:02:50:B9:31:68
<b>Issued:</b>	Oct 1 08:32:27 2013 GMT
<b>Expires:</b>	Oct 1 08:32:27 2033 GMT

- **Hongkong\_Post\_Root\_CA\_3.crt**

<b>Subject Name:</b>	C = HK, ST = Hong Kong, L = Hong Kong, O = Hongkong Post, CN = Hongkong Post Root CA 3
<b>Fingerprint:</b>	5A:2F:C0:3F:0C:83:B0:90:BB:FA:40:60:4B:09:88:44:6C:76:36:18:3D:F9:84:6E:17:10:1A:44:7F:B8:EF:D6
<b>Issued:</b>	Jun 3 02:29:46 2017 GMT
<b>Expires:</b>	Jun 3 02:29:46 2042 GMT

- **GeoTrust\_Primary\_Certification\_Authority\_-\_G2.crt**

<b>Subject Name:</b>	C = US, O = GeoTrust Inc., OU = (c) 2007 GeoTrust Inc. - For authorized use only, CN = GeoTrust Primary Certification Authority - G2
<b>Fingerprint:</b>	5E:DB:7A:C4:3B:82:A0:6A:87:61:E8:D7:BE:49:79:EB:F2:61:1F:7D:D7:9B:F9:1C:1C:6B:56:6A:21:9E:D7:66
<b>Issued:</b>	Nov 5 00:00:00 2007 GMT
<b>Expires:</b>	Jan 18 23:59:59 2038 GMT



- **TUBITAK\_Kamu\_SM\_SSL\_Kok\_Sertifikasi\_-\_Surum\_1.crt**

<b>Subject Name:</b>	C = TR, L = Gebze - Kocaeli, O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK, OU = Kamu Sertifikasyon Merkezi - Kamu SM, CN = TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1
<b>Fingerprint:</b>	46:ED:C3:68:90:46:D5:3A:45:3F:B3:10:4A:B8:0D:CA:EC:65:8B:26:60:EA:16:29:DD:7E:86:79:90:64:87:16
<b>Issued:</b>	Nov 25 08:25:55 2013 GMT
<b>Expires:</b>	Oct 25 08:25:55 2043 GMT

- **GDCA\_TrustAUTH\_R5\_ROOT.crt**

<b>Subject Name:</b>	C = CN, O = "GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.", CN = GDCA TrustAUTH R5 ROOT
<b>Fingerprint:</b>	BF:FF:8F:D0:44:33:48:7D:6A:8A:A6:0C:1A:29:76:7A:9F:C2:BB:B0:5E:42:0F:71:3A:13:B9:92:89:1D:38:93
<b>Issued:</b>	Nov 26 05:13:15 2014 GMT
<b>Expires:</b>	Dec 31 15:59:59 2040 GMT

- **Atos\_TrustedRoot\_2011.crt**

<b>Subject Name:</b>	CN = Atos TrustedRoot 2011, O = Atos, C = DE
<b>Fingerprint:</b>	F3:56:BE:A2:44:B7:A9:1E:B3:5D:53:CA:9A:D7:86:4A:CE:01:8E:2D:35:D5:F8:F9:6D:DF:68:A6:F4:1A:A4:74
<b>Issued:</b>	Jul 7 14:58:30 2011 GMT
<b>Expires:</b>	Dec 31 23:59:59 2030 GMT

- **Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2015.crt**

<b>Subject Name:</b>	C = GR, L = Athens, O = Hellenic Academic and Research Institutions Cert. Authority, CN = Hellenic Academic and Research Institutions RootCA 2015
<b>Fingerprint:</b>	A0:40:92:9A:02:CE:53:B4:AC:F4:F2:FF:C6:98:1C:E4:49:6F:75:5E:6D:45:FE:0B:2A:69:2B:CD:52:52:3F:36
<b>Issued:</b>	Jul 7 10:11:21 2015 GMT
<b>Expires:</b>	Jun 30 10:11:21 2040 GMT

- **Go\_Daddy\_Root\_Certificate\_Authority\_-\_G2.crt**

<b>Subject Name:</b>	C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", CN = Go Daddy Root Certificate Authority - G2
<b>Fingerprint:</b>	45:14:0B:32:47:EB:9C:C8:C5:B4:F0:D7:B5:30:91:F7:32:92:08:9E:6E:5A:63:E2:74:9D:D3:AC:A9:19:8E:DA
<b>Issued:</b>	Sep 1 00:00:00 2009 GMT
<b>Expires:</b>	Dec 31 23:59:59 2037 GMT

- **OISTE\_WISeKey\_Global\_Root\_GA\_CA.crt**

<b>Subject Name:</b>	C = CH, O = WISeKey, OU = Copyright (c) 2005, OU = OISTE Foundation Endorsed, CN = OISTE WISeKey Global Root GA CA
<b>Fingerprint:</b>	41:C9:23:86:6A:B4:CA:D6:B7:AD:57:80:81:58:2E:02:07:97:A6:CB:DF:4F:FF:78:CE:83:96:B3:89:37:D7:F5
<b>Issued:</b>	Dec 11 16:03:44 2005 GMT
<b>Expires:</b>	Dec 11 16:09:51 2037 GMT

- **SSL.com\_Root\_Certification\_Authority\_ECC.crt**

<b>Subject Name:</b>	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com Root Certification Authority ECC
<b>Fingerprint:</b>	34:17:BB:06:CC:60:07:DA:1B:96:1C:92:0B:8A:B4:CE:3F:AD:82:0E:4A:A3:0B:9A:CB:C4:A7:4E:BD:CE:BC:65
<b>Issued:</b>	Feb 12 18:14:03 2016 GMT
<b>Expires:</b>	Feb 12 18:14:03 2041 GMT

- **GeoTrust\_Global\_CA.crt**

<b>Subject Name:</b>	C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
<b>Fingerprint:</b>	FF:85:6A:2D:25:1D:CD:88:D3:66:56:F4:50:12:67:98:CF:AB:AA:DE:40:79:9C:72:2D:E4:D2:B5:DB:36:A7:3A
<b>Issued:</b>	May 21 04:00:00 2002 GMT
<b>Expires:</b>	May 21 04:00:00 2022 GMT

- **Buypass\_Class\_2\_Root\_CA.crt**

<b>Subject Name:</b>	C = NO, O = Buypass AS-983163327, CN = Buypass Class 2 Root CA
<b>Fingerprint:</b>	9A:11:40:25:19:7C:5B:B9:5D:94:E6:3D:55:CD:43:79:08:47:B6:46:B2:3C:DF:11:AD:A4:A0:0E:FF:15:FB:48
<b>Issued:</b>	Oct 26 08:38:03 2010 GMT
<b>Expires:</b>	Oct 26 08:38:03 2040 GMT

- **Autoridad\_de\_Certificacion\_Firmaprofesional\_CIF\_A62634068.crt**

<b>Subject Name:</b>	C = ES, CN = Autoridad de Certificacion Firmaprofesional CIF A62634068
<b>Fingerprint:</b>	04:04:80:28:BF:1F:28:64:D4:8F:9A:D4:D8:32:94:36:6A:82:88:56:55:3F:3B:14:30:3F:90:14:7F:5D:40:EF
<b>Issued:</b>	May 20 08:38:15 2009 GMT
<b>Expires:</b>	Dec 31 08:38:15 2030 GMT

- **Amazon\_Root\_CA\_3.crt**

<b>Subject Name:</b>	C = US, O = Amazon, CN = Amazon Root CA 3
<b>Fingerprint:</b>	18:CE:6C:FE:7B:F1:4E:60:B2:E3:47:B8:DF:E8:68:CB:31:D0:2E:BB:3A:DA:27:15:69:F5:03:43:B4:6D:B3:A4
<b>Issued:</b>	May 26 00:00:00 2015 GMT
<b>Expires:</b>	May 26 00:00:00 2040 GMT

- **CA\_Disig\_Root\_R2.crt**

<b>Subject Name:</b>	C = SK, L = Bratislava, O = Disig a.s., CN = CA Disig Root R2
<b>Fingerprint:</b>	E2:3D:4A:03:6D:7B:70:E9:F5:95:B1:42:20:79:D2:B9:1E:DF:BB:1F:B6:51:A0:63:3E:AA:8A:9D:C5:F8:07:03
<b>Issued:</b>	Jul 19 09:15:30 2012 GMT
<b>Expires:</b>	Jul 19 09:15:30 2042 GMT

- **Security\_Communication\_RootCA2.crt**

<b>Subject Name:</b>	C = JP, O = "SECOM Trust Systems CO.,LTD.", OU = Security Communication RootCA2
----------------------	---

<b>Fingerprint:</b>	51:3B:2C:EC:B8:10:D4:CD:E5:DD:85:39:1A:DF:C6:C2:DD:60:D8:7B:B7:36:D2:B5:21:48:4A:A4:7A:0E:BE:F6
<b>Issued:</b>	May 29 05:00:39 2009 GMT
<b>Expires:</b>	May 29 05:00:39 2029 GMT

- **DigiCert\_Assured\_ID\_Root\_CA.crt**

<b>Subject Name:</b>	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root CA
<b>Fingerprint:</b>	3E:90:99:B5:01:5E:8F:48:6C:00:BC:EA:9D:11:1E:E7:21:FA:BA:35:5A:89:BC:F1:DF:69:56:1E:3D:C6:32:5C
<b>Issued:</b>	Nov 10 00:00:00 2006 GMT
<b>Expires:</b>	Nov 10 00:00:00 2031 GMT

- **QuoVadis\_Root\_CA\_3\_G3.crt**

<b>Subject Name:</b>	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 3 G3
<b>Fingerprint:</b>	88:EF:81:DE:20:2E:B0:18:45:2E:43:F8:64:72:5C:EA:5F:BD:1F:C2:D9:D2:05:73:07:09:C5:D8:B8:69:0F:46
<b>Issued:</b>	Jan 12 20:26:32 2012 GMT
<b>Expires:</b>	Jan 12 20:26:32 2042 GMT

- **Certum\_Trusted\_Network\_CA.crt**

<b>Subject Name:</b>	C = PL, O = Unizeto Technologies S.A., OU = Certum Certification Authority, CN = Certum Trusted Network CA
<b>Fingerprint:</b>	5C:58:46:8D:55:F5:8E:49:7E:74:39:82:D2:B5:00:10:B6:D1:65:37:4A:CF:83:A7:D4:A3:2D:B7:68:C4:40:8E
<b>Issued:</b>	Oct 22 12:07:37 2008 GMT
<b>Expires:</b>	Dec 31 12:07:37 2029 GMT

- **emSign\_Root\_CA\_-\_G1.crt**

<b>Subject Name:</b>	C = IN, OU = emSign PKI, O = eMudhra Technologies Limited, CN = emSign Root CA - G1
<b>Fingerprint:</b>	40:F6:AF:03:46:A9:9A:A1:CD:1D:55:5A:4E:9C:CE:62:C7:F9:63:46:03:EE:40:66:15:83:3D:C8:C8:D0:03:67
<b>Issued:</b>	Feb 18 18:30:00 2018 GMT
<b>Expires:</b>	Feb 18 18:30:00 2043 GMT

- **AffirmTrust\_Premium.crt**

<b>Subject Name:</b>	C = US, O = AffirmTrust, CN = AffirmTrust Premium
<b>Fingerprint:</b>	70:A7:3F:7F:37:6B:60:07:42:48:90:45:34:B1:14:82:D5:BF:0E:69:8E:CC:49:8D:F5:25:77:EB:F2:E9:3B:9A
<b>Issued:</b>	Jan 29 14:10:36 2010 GMT
<b>Expires:</b>	Dec 31 14:10:36 2040 GMT

- **thawte\_Primary\_Root\_CA.crt**

<b>Subject Name:</b>	C = US, O = "thawte, Inc.", OU = Certification Services Division, OU = "(c) 2006 thawte, Inc. - For authorized use only", CN = thawte Primary Root CA
----------------------	---

## 6.9.4 Managing CA Certificates for the Trusted Certificate Store

<b>Fingerprint:</b>	8D:72:2F:81:A9:C1:13:C0:79:1D:F1:36:A2:96:6D:B2:6C:95:0A:97:1D:B4:6B:41:99:F4:EA:54:B7:8B:FB:9F
<b>Issued:</b>	Nov 17 00:00:00 2006 GMT
<b>Expires:</b>	Jul 16 23:59:59 2036 GMT

- **NetLock\_Arany\_=Class\_Gold=\_Fotanúsítvány.crt**

<b>Subject Name:</b>	C = HU, L = Budapest, O = NetLock Kft., OU = Tan\C3\BAs\C3\ADtv\C3\A1nykiad\C3\B3k (Certification Services), CN = NetLock Arany (Class Gold) F\C5\91tan\C3\BAs\C3\ADtv\C3\A1ny
<b>Fingerprint:</b>	6C:61:DA:C3:A2:DE:F0:31:50:6B:E0:36:D2:A6:FE:40:19:94:FB:D1:3D:F9:C8:D4:66:59:92:74:C4:46:EC:98
<b>Issued:</b>	Dec 11 15:08:21 2008 GMT
<b>Expires:</b>	Dec 6 15:08:21 2028 GMT

## 6.9.4 Managing CA Certificates for the Trusted Certificate Store

To establish trust between the device and an endpoint (e.g. server, portal, etc.), add the necessary CA certificates to the Trusted Certificate Store.

### 6.9.4.1 Viewing a List of CA Certificates Added to the Trusted Certificate Store

To view a list of CA certificates added to the Trusted Certificate Store, navigate to the **System CA Certificate** tab under **Administration » Security » Cryptography**. If CA certificates have been associated with the Store, the **Configured CAs** table appears.

If no CA certificates have been added to the Store, add certificates as needed. For more information, refer to "Adding a CA Certificate to the Trusted Certificate Store" (Page 177).

### 6.9.4.2 Adding a CA Certificate to the Trusted Certificate Store

To add a CA certificate to the Trusted Certificate Store, do the following:

1. Navigate to the **System CA Certificate** tab under **Administration » Security » Cryptography**.
2. Click **Add Entry**.
3. Under **CA Name**, select one of the available CA certificates configured on the device, and then click **OK**.
4. Commit the change.

### 6.9.4.3 Deleting a CA Certificate from the Trusted Certificate Store

To delete a CA certificate from the Trusted Certificate Store, do the following:

1. Navigate to the **System CA Certificate** tab under **Administration » Security » Cryptography**.
2. Select the CA certificate to be deleted then click **Delete Entry**.
3. Commit the change.

## 6.9.5 Managing CA Certificates and CRLs

This section describes how to view, add and delete Certified Authority (CA) certificates and Certificate Revocation Lists (CRLs) on the device.

### 6.9.5.1 Viewing a List of CA Certificates and CRLs

To view a list of certificates issued by a Certified Authority (CA) and the Certificate Revocation Lists (CRLs) associated with them, navigate to the **CA** tab under **Administration » Security » Cryptography**. If certificates have been configured, the **Certificate Authority Settings** table appears.

If no certificates have been configured, add certificates as needed. For more information, refer to "Adding a CA Certificate and CRL" (Page 179).

### 6.9.5.2 Viewing the Status of a CA Certificate and CRL

To view the status of a CA certificate and its associated Certificate Revocation List (CRL), navigate to the **CA** tab under **Administration » Security » Cryptography**, and then click **Certificate** for the desired certificate.

The **Key Cert Sign Certificate Status** area provides the following information:

Parameter	Description
Issuer	<b>Synopsis:</b> A string
Subject	<b>Synopsis:</b> A string
Not Before	<b>Synopsis:</b> A string This certificate is not valid before this date.
Not After	<b>Synopsis:</b> A string This certificate is not valid after this date.

The **CRL Sign Certificate Status** area provides the following information:

Parameter	Description
Issuer	<b>Synopsis:</b> A string
Subject	<b>Synopsis:</b> A string
Not Before	<b>Synopsis:</b> A string This certificate is not valid before this date.
Not After	<b>Synopsis:</b> A string This certificate is not valid after this date.

The **CRL Status** area provides the following information:

Parameter	Description
Issuer	<b>Synopsis:</b> A string
This Update	<b>Synopsis:</b> A string This CRL was updated at this date and time.
Next Update	<b>Synopsis:</b> A string This CRL must be updated by this date and time.

### 6.9.5.3 Adding a CA Certificate and CRL

To add a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:

#### Note

Only admin users can read/write certificates and keys on the device.

1. Navigate to the **CA** tab under **Administration » Security » Cryptography**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 255 characters long The name of the CA certificate.

4. Click **OK**.
5. Copy the contents of the CA certificate into the **Key Cert Sign Certificate** box.

#### Note

Large CRLs (bigger than 100KB) are not currently supported and may be difficult to add/view in the configuration.

## 6.9.6 Managing Private Keys

6. Add the associated Certificate Revocation List (CRL).
  - If the CRL is signed by a separate certificate, copy the contents of the CRL into the **CRL Sign Certificate** box
  - If the CRL is not signed, copy the contents of the CRL into the **CRL Contents** box
7. Commit the changes.

### 6.9.5.4 Deleting a CA Certificate and CRL

To delete a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:

1. Navigate to the **CA** tab under **Administration » Security » Cryptography**.
2. Select the CA certificate and its associated Certificate Revocation List (CRL) to be deleted then click **Delete Entry**.
3. Commit the change.

## 6.9.6 Managing Private Keys

This section describes how to view, add and delete private keys on the device.

---

### Note

Private keys are automatically encrypted using an AES-CFB-128 cipher to protect them from being viewed by unauthorized users.

---

### 6.9.6.1 Viewing a List of Private Keys

To view a list of unsigned private keys, navigate to the **Private Key** tab under **Administration » Security » Cryptography**. If private keys have been configured, the **Private Key** table appears.

If no private keys have been configured, add keys as needed. For more information, refer to "Adding a Private Key" (Page 180).

### 6.9.6.2 Adding a Private Key

To add an unsigned private key, do the following:

---

### Note

DSA keys are not supported on SSH, NETCONF or WebUI services.

---

**Note**

Private keys for SSH servers or HTTPS access must be in PEM format and **Algorithm** is set to **rsa**.

1. Navigate to the **Private Key** tab under **Administration » Security » Cryptography**.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 255 characters long The name of the key.

4. Click **OK** to create the new private key.
5. Select the newly created entry, and then configure the following parameters as required:

**Note**

When adding a private key when RUGGEDCOM ROX II is acting as an SSH client or TLS server, make sure the key is in the SSH/RSA format and the private key algorithm is set to **rsa**.

Parameter	Description
Algorithm	<b>Synopsis:</b> [ rsa   dsa   ssh-rsa   ssh-ed25519 ] The type of key.
Contents	<b>Synopsis:</b> A string between 1 and 8192 characters long The contents of the unsigned private key.

6. Commit the changes.

**6.9.6.3 Deleting a Private Key**

To delete an unsigned private key, do the following:

1. Navigate to the **Private Key** tab under **Administration » Security » Cryptography**.
2. Select the private key to be deleted then click **Delete Entry**.
3. Commit the changes.



## 6.9.7 Managing Public Keys

This section describes how to manage public keys on the device.

### 6.9.7.1 Viewing a List of Public Keys

To view a list of unsigned public keys, navigate to the **Public Key** tab under **Administration » Security » Cryptography**. If public keys have been configured, the **Public Key** table appears.

If no public keys have been configured, add keys as needed. For more information, refer to "Adding a Public Key" (Page 182).

### 6.9.7.2 Adding a Public Key

To add an unsigned public key, do the following:

---

#### Note

Do not associate the public key with the private key if the public key belongs to another device.

---

1. Make sure the private key associated with the public key has been added. For more information, refer to "Adding a Private Key" (Page 180).
2. Navigate to the **Public Key** tab under **Administration » Security » Cryptography**.
3. Click **Add Entry**.
4. Configure the following parameters as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 255 characters long The name of the key.

5. Click **OK** to create the new public key.
6. Select the newly created entry, and then configure the following parameters as required:

---

#### Note

For added security, consider adding an IPSec-formatted public key. For more information, refer to "Adding an IPSec-Formatted Public Key" (Page 183).

---

#### Note

When adding a public key for a known host when RUGGEDCOM ROX II is acting as an SSH client, make sure the key is in the OpenSSH public key format and the public key algorithm is set to *ssh-rsa*.

---

Parameter	Description
Algorithm	<b>Synopsis:</b> [ rsa   dsa   ssh-rsa   ssh-ed25519 ] The algorithm of the key.
Contents	<b>Synopsis:</b> A string between 1 and 8192 characters long The contents of the key.
Private Key Name	<b>Synopsis:</b> A string between 1 and 255 characters long The private key name associated with this public key.

7. Commit the changes.

### 6.9.7.3 Adding an IPSec-Formatted Public Key

IPSec-formatted public keys from systems that do not support the Privacy-Enhanced Mail (PEM) format, such as RUGGEDCOM ROX devices, can be imported into RUGGEDCOM ROX II and automatically converted.

Once added to the RUGGEDCOM ROX II database, the IPSec-formatted public key is visible via the **System Public Key** form under **tunnel » ipsec » connection » { name } » { end }**, where { name } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end. **Type** must be set to **rsasig** to display the public key.

The public key can be copied from the **System Public Key** form and added to another RUGGEDCOM ROX II device, as described in the following procedure, or to a RUGGEDCOM ROX device.

To add an IPSec-formatted public key and have it converted into PEM format, do the following:

1. Navigate to the **Public Key** tab under **Administration » Security » Cryptography** and select a public key. If the desired key is not available, add it. For more information about adding a public key, refer to "Adding a Public Key" (Page 182).
2. Under **Add IPSec-Formatted Public Key**, click **Perform**.
3. in the **IPSec-Formatted Public Key** box, enter the contents of the public key.
4. Click **OK** to convert the public key to PEM format and add it to RUGGEDCOM ROX II.
5. Commit the changes.

### 6.9.7.4 Deleting a Public Key

To delete an unsigned public key, do the following:

1. Navigate to the **Public Key** tab under **Administration » Security » Cryptography**.

2. Select the public key to be deleted then click **Delete Entry**.
3. Commit the changes.

## 6.9.8 Managing Certificates

This section describes how to manage certificates on the device.

### 6.9.8.1 Viewing a List of Certificates

To view a list of certificates, navigate to the **Certificate** tab under **Administration » Security » Cryptography**. If certificates have been configured, a list appears.

If no certificates have been configured, add certificates as needed. For more information, refer to "Adding a Certificate" (Page 184).

### 6.9.8.2 Viewing the Status of a Certificate

To view the status of a certificate, navigate to the **Certificate** tab under **Administration » Security » Cryptography**.

The table provides the following information:

Parameter	Description
Issuer	<b>Synopsis:</b> A string
Subject	<b>Synopsis:</b> A string
Not Before	<b>Synopsis:</b> A string This certificate is not valid before this date.
Not After	<b>Synopsis:</b> A string This certificate is not valid after this date.

### 6.9.8.3 Adding a Certificate

To add a certificate, do the following:

---

#### Note

Only admin users can read/write certificates and keys on the device.

---

1. Make sure the required CA certificates and/or private keys have been added to the device.
  - For more information about adding CA Certificates, refer to "Adding a CA Certificate and CRL" (Page 179)

- For more information about adding private keys, refer to "Adding a Private Key" (Page 180)
2. Navigate to the **Certificate** tab under **Administration » Security » Cryptography**.
  3. Click **Add Entry**.
  4. Configure the following parameter(s) as required:

Parameter	Description
Certificate Name	<b>Synopsis:</b> A string between 1 and 255 characters long The name of the certificate.

5. Click **OK**.
6. Configure the following parameter(s) as required:

Parameter	Description
Contents	<b>Synopsis:</b> A string between 1 and 8192 characters long The contents of the certificate.
Private Key Name	<b>Synopsis:</b> A string between 1 and 255 characters long The private key associated with this certificate.
CA Name	<b>Synopsis:</b> A string between 1 and 255 characters long The optional CA certificate for this certificate.

7. [Optional] Select the certificate as the certificate to use for SSL/SSH connections. For more information, refer to "Configuring Session Security" (Page 152).
8. Commit the changes.

#### 6.9.8.4 Deleting a Certificate

To delete a certificate, do the following:

1. Navigate to the **Certificate** tab under **Administration » Security » Cryptography**.
2. Select the certificate to be deleted then click **Delete Entry**.
3. Commit the change.

### 6.9.9 Managing Known Hosts

RUGGEDCOM ROX II maintains a Known Hosts list for defining each SSH (SFTP) server the device pulls updates or files from. Servers are identified by their host name or IP address, and authenticated by the known hosts file stored on the device. Users can

further define a specific port on the server designated for SSH communications and/or an SSH/RSA public key.

---

#### Note

Before any interactions with a remote SFTP server can take place (i.e. installing files, backing up files, or upgrading/downgrading the software), the server's public key must be pre-configured as a known host. This updates the trust store and allows RUGGEDCOM ROX II to securely connect to the remote SFTP server.

Other SSH-based client features, such as SCP file transfers and connecting via SSH from the device to another SSH server, will also reference known hosts, but with the following exception:

- RUGGEDCOM ROX II will still access an SCP server even if the server's public key is not pre-configured as a known host. In this case, the server's public key fingerprint is displayed for visual verification in the CLI before the connection is made. This can be removed by pre-configuring the SCP server's public key as a known host.
- 

### 6.9.9.1 Viewing a List of Known Hosts

To view a list of servers defined in the Known Hosts list, navigate to the **CLI Sessions** tab under **Administration » Session Config**, and then click **Hosts List**. A list appears.

If no servers have been configured, add servers as needed. For more information, refer to "Adding a Known Host" (Page 186).

### 6.9.9.2 Adding a Known Host

To add a server to the Known Hosts list, do the following:

1. Make sure the server's public key has been added to the device. For more information, refer to "Managing Public Keys" (Page 182).
2. Navigate to the **CLI Sessions** tab under **Administration » Session Config**, and then click **Hosts List**.
3. Click **Add Entry**.
4. Under **Name**, enter a unique name for the server and then click **OK**.
5. Select the newly created entry, and then configure the following parameters as required:

Parameter	Description
Server ID	<p><b>Synopsis:</b> A string between 1 and 63 characters long</p> <p>The name to identify the remote server. This may be the ASCII hostname of the server or the IPv4 address (xxx.xxx.xxx.xxx) of the server.</p>

Parameter	Description
Server Port	<b>Synopsis:</b> An integer between 0 and 65535  The port number (optional) uniquely identifies the remote SSH server. If no port is specified, then you will be able to access SSH servers on the remote server that are running on different ports.
Server Public Key	<b>Synopsis:</b> A string between 1 and 255 characters long  The name of the authorized ssh-rsa key for the server. The acceptable keys are taken from the list of authorized keys in / security/crypto.
Enabled	Enables remote login to the server when using ssh, scp or sftp. If enabled, the server id and public key are saved in the known_hosts file.

6. Commit the changes.

### 6.9.9.3 Deleting a Known Host

To delete a server from the Known Hosts list, do the following:

1. Navigate to the **CLI Sessions** tab under **Administration » Session Config**, and then click **Hosts List**.
2. Select the server to be deleted then click **Delete Entry**.
3. Commit the change.

## 6.9.10 Managing SCEP

The Simple Certificate Enrollment Protocol (SCEP) is a scalable certificate management protocol for the automatic issuance and renewal of certificates in enterprise environments.

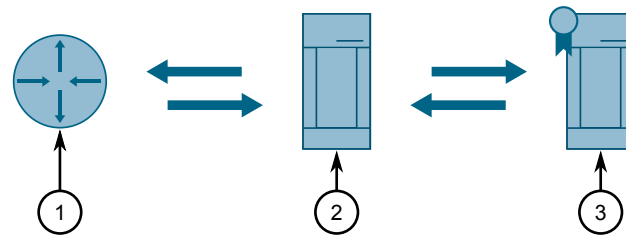
SCEP is used by network administrators to quickly and automatically issue Public Key Infrastructure (PKI) certificates to devices, as opposed to manually managing certificates for each individual device.

SCEP is an open-source protocol described in [RFC 8894 \[https://tools.ietf.org/html/rfc8894\]](https://tools.ietf.org/html/rfc8894).

### 6.9.10.1 Understanding SCEP

In an SCEP environment, there are three entities:

- the SCEP client (or requester)
- the SCEP server
- and a Certificate Authority (CA)



- ① SCEP Client
- ② SCEP Server
- ③ Certificate Authority (CA)

Figure 6.2 SCEP Entities

RUGGEDCOM ROX II devices take the role of SCEP clients.

As an SCEP client, the device can retrieve CA certificates and SCEP certificates from an SCEP server. The server requests CA certificates from a root CA.

Every SCEP client requires a challenge password to authenticate itself with the SCEP server. This is a one-time password (OTP) provided out-of-band (OOB) by the server. When the client requests a new SCEP certificate, it provides the challenge password to the SCEP server, along with a self-generated private key and Certificate Signing Request (CSR). The CSR is derived from the client's configuration settings.

Once retrieved, the SCEP certificate can be used by IPsec.

When an SCEP certificate already exists on the device, the client can renew it automatically before it expires. The challenge password is not required when renewing an existing certificate.

**⚠ NOTICE**

**Security hazard – risk of unauthorized access or exploitation**

SCEP communications between the client and server must be protected within a secure network environment.

**⚠ NOTICE**

**Security hazard – risk of unauthorized access or exploitation**

The CA fingerprint must be obtained out-of-band (OOB) using a secure method. Receiving a fingerprint from a malicious entity could compromise authentication with the SCEP server.

**Note**

Certificate revocation is not available through SCEP. Contact the CA for alternative methods.

SCEP certificates cannot be renewed once they have expired.

### 6.9.10.2 Configuring SCEP

To configure SCEP, do the following:

1. **Configure the SCEP server.**

The FAQ "[How to configure a SCEP server \[https://support.industry.siemens.com/cs/ww/en/view/109811508\]](https://support.industry.siemens.com/cs/ww/en/view/109811508)" provides guidance on how to configure a SCEP server using Windows Server and SICAM GridPass. For other SCEP servers, refer to the server's documentation for instructions.

2. **Obtain information from the SCEP server out-of-band.**

This includes the following:

- Server's URL
- Challenge password (or shared secret)
- CA fingerprint algorithm
- Certificate hash
- Encryption algorithm
- Signature algorithm

 **NOTICE**

**Security hazard – risk of unauthorized access**

Make sure the SCEP server is configured to issue only one challenge password per device and expire passwords after a short period of time. This protects the integrity of the secure network, reducing the risk of rogue devices entering the network.

3. **Configure the SCEP client.**

This includes defining the URL of the SCEP server, CA certificate name and hash, and polling settings.

For more information, refer to "Configuring the SCEP Client" (Page 190).

4. **Configure information that will be included in Certificate Signing Requests (CSRs).**

This includes the subject alternative name, locality, organization, key size, and more.

For more information, refer to "Configuring the SCEP Certificate Signing Requests" (Page 191).

5. **Retrieve a CA certificate from the SCEP server.**

The CA certificate is required before an SCEP certificate can be request.

For more information, refer to "Retrieving an SCEP CA Certificate" (Page 192).

6. **Retrieve the SCEP certificate from the server.**

For more information, refer to "Retrieving an SCEP Certificate" (Page 193).



7. **Configure and enable automatic renewal of the SCEP certificate.**

Once automatic renewal is enabled, the SCEP client will automatically renew SCEP certificate before it expires.

For more information, refer to "Configuring Automatic Certificate Renewal" (Page 193).

8. **[Optional] Verify the CA certificate was added to the device.**

For more information, refer to "Viewing the Status of a Certificate" (Page 184).

### 6.9.10.3 Configuring the SCEP Client

To configure the SCEP client, do the following:

1. Navigate to the **SCEP** tab under **Administration » Security » Cryptography**, and then click **Server Configuration**.
2. Configure the following parameter(s) as required:

---

**Note**

The names of the SCEP CA certificate (**CA Certificate Name**) can only be changed if the certificate does not already exist on the device.

---

Parameter	Description
Server URL	<b>Synopsis:</b> A string between 1 and 1024 characters long The URL of the SCEP server.
CA Certificate Name	<b>Synopsis:</b> A string between 1 and 255 characters long <b>Default:</b> scep-ca The name of the SCEP CA certificate.
CA Certificate Hash Value	<b>Synopsis:</b> A string between 1 and 256 characters long The hash value of the CA certificate obtained from the SCEP server for verification.
CA Certificate Hash Type	<b>Synopsis:</b> [ sha256   sha1   md5 ] <b>Default:</b> md5 The type of the hash value of the CA certificate obtained from the SCEP server.
Maximum Number of Requests	<b>Synopsis:</b> An integer between 1 and 256 <b>Default:</b> 60 The maximum number of SCEP certificate polling requests. Default is 60.

Parameter	Description
Max Polling Time	<p><b>Synopsis:</b> An integer between 1 and 28800</p> <p><b>Default:</b> 3600</p> <p>The maximum SCEP certificate polling time in seconds. Default is 3600.</p>
Polling Interval	<p><b>Synopsis:</b> An integer between 1 and 3600</p> <p><b>Default:</b> 60</p> <p>The interval in seconds between SCEP certificate polling attempts. Default is 60 seconds.</p>

3. Commit the changes.

#### 6.9.10.4 Configuring the SCEP Certificate Signing Requests

To configure information that will be included in SCEP Certificate Signing Requests (CSRs), do the following:

1. Navigate to the **SCEP** tab under **Administration » Security » Cryptography**, and then click **Certificate Configuration**.
2. Configure the following parameter(s) as required:

##### Note

The names of the SCEP certificate (**Certificate Name**) and private key (**Private Key Name**) can only be changed if the associated file does not already exist on the device.

Parameter	Description
Subject Alternative Name	<p><b>Synopsis:</b> A string between 1 and 128 characters long</p> <p>The subject alternative name associated with the SCEP certificate.</p>
Subject Alternative Name Type	<p><b>Synopsis:</b> [ ip   email   dns ]</p> <p><b>Default:</b> dns</p> <p>The subject alternative name type associated with the SCEP certificate. Default is 'dns'.</p>
Country	<p><b>Synopsis:</b> A string</p> <p>The country associated with the SCEP certificate.</p>
State/Province	<p><b>Synopsis:</b> A string up to 128 characters long</p> <p>The state or province name associated with the SCEP certificate.</p>
Locality	<p><b>Synopsis:</b> A string up to 128 characters long</p> <p>The locality associated with the SCEP certificate.</p>

Parameter	Description
Organization	<b>Synopsis:</b> A string up to 64 characters long The organization associated with the SCEP certificate.
Organization Unit	<b>Synopsis:</b> A string up to 64 characters long The organizational unit associated with the SCEP certificate
Key Size	<b>Synopsis:</b> [ 4096   2048   1024 ] <b>Default:</b> 2048 The key size in bits, default is 2048
Certificate Name	<b>Synopsis:</b> A string between 1 and 255 characters long <b>Default:</b> scep-cert The name of the SCEP certificate.
Private Key Name	<b>Synopsis:</b> A string between 1 and 255 characters long <b>Default:</b> scep-rsa The name of the private key.
Encryption Algorithm	<b>Synopsis:</b> [ aes256   aes192   aes128   3des ] <b>Default:</b> aes128 The encryption algorithm.
Signature Algorithm	<b>Synopsis:</b> [ sha512   sha384   sha256   sha224   sha1 ] <b>Default:</b> sha256 The signature algorithm.

3. Commit the changes.

### 6.9.10.5 Retrieving an SCEP CA Certificate

To retrieve an SCEP CA certificate from the SCEP server, do the following:

---

#### Note

A CA certificate is required as part of the Certificate Signing Request (CSR) sent when requesting an SCEP certificate. As such, the CA certificate must be obtained before the SCEP certificate is requested.

---

1. Navigate to the **SCEP** tab under **Administration » Security » Cryptography**, and then click **Certificate Configuration**.
2. Under **Get CA**, click **Perform**.
3. Configure the following parameter:

Parameter	Description
Fingerprint Algorithm	<b>Synopsis:</b> [ sha512   sha384   sha256   sha224   sha1 ] The fingerprint algorithm of the SCEP CA certificate.

- Click **OK**.

The device requests a CA certificate with the selected fingerprint algorithm from the SCEP server. Upon receipt, the certificate is added to the list of CA certificates.

### 6.9.10.6 Retrieving an SCEP Certificate

To retrieve an SCEP certificate, do the following:

- Navigate to the **SCEP** tab under **Administration » Security » Cryptography**, and then click **Certificate Configuration**.
- Under **Get Certificates**, click **Perform**.

---

#### Note

The challenge password is not required if an SCEP certificate already exists on the device.

---

- [Optional] On the **Get Certificate** form, configure the following parameter:

Parameter	Description
Challenge Password	<b>Synopsis:</b> A string up to 128 characters long The challenge password provided by the SCEP server. The password is required to authenticate the device to the SCEP server if the SCEP certificate on the device has expired.

- Click **OK**.

The device generates a private key and Certificate Signing Request (CSR), which it then uses to request an SCEP certificate from the SCEP server. When the certificate is received, it is saved and added to the list of device certificates, along with the private key and CA certificate.

### 6.9.10.7 Configuring Automatic Certificate Renewal

To configure automatic certificate renewal, do the following:

---

#### Note

SCEP certificates cannot be renewed once they have expired.

---

- Navigate to the **SCEP** tab under **Administration » Security » Cryptography**, and then click **Automatic Certificate Renewal**.

2. Configure the following parameter(s) as required:

Parameter	Description
Enable	<b>Synopsis:</b> [ true   false ] When enabled, the SCEP certificate will be automatically renewed at the configured time. Default is false.
Time Before Expiry	<b>Synopsis:</b> An integer between 1 and 365 <b>Default:</b> 14 The number of days or hours before expiry when the SCEP certificate will be automatically renewed. Default is 14.
Unit of Time	<b>Synopsis:</b> [ hours   days ] <b>Default:</b> days The unit of time in which the time before the SCEP certificate expiry is displayed. Default is 'days'.

3. Commit the changes.

#### 6.9.10.8 Renewing an Expired SCEP Certificate

SCEP certificates that have expired must be renewed by the user. Automatic renewal is only available for active certificates.

To renew an expired SCEP certificate, do the following:

1. Obtain a new challenge password (or shared secret) from the SCEP server.
2. Using the new challenge password, retrieve a new SCEP certificate from the SCEP server.

For more information, refer to "Retrieving an SCEP Certificate" (Page 193).

#### 6.9.10.9 Renewing an SCEP CA Certificate

SCEP CA certificates cannot be renewed automatically and, therefore, must be renewed by an administrator before or after they expire.

To renew an expired SCEP CA certificate, do the following:

1. Determine the fingerprint algorithm used by the SCEP server.
2. Retrieve a new SCEP CA certificate from the SCEP server, making sure to specify the correct fingerprint algorithm.

For more information, refer to "Retrieving an SCEP CA Certificate" (Page 192).

## 6.10 Managing Firewalls

Firewalls are software systems designed to prevent unauthorized access to or from private networks. Firewalls are most often used to prevent unauthorized Internet users from accessing private networks (Intranets) connected to the Internet.

When the RUGGEDCOM ROX II firewall is enabled, the router serves as a gateway machine through which all messages entering or leaving the Intranet pass. The router examines each message and blocks those that do not meet the specified security criteria. The router also acts as a proxy, preventing direct communication between computers on the Internet and Intranet. Proxy servers can filter the kinds of communication that are allowed between two computers and perform address translation.

---

### Note

In general, the RUGGEDCOM ROX II firewall implementation will maintain established connections. This applies when adding, deleting, or changing rules, and also when adding, deleting, or changing policies. When applying new, or modified, rules or policies, previous traffic seen by the router might still be considered as having valid connections by the connection tracking table. For instance:

1. A rule for the TCP and UDP protocols is applied.
2. The router sees both TCP and UDP traffic that qualifies for NAT.
3. The rule is then modified to allow only UDP.
4. The router will still see TCP packets (i.e. retransmission packets).

If required, reboot the router to flush all existing connection streams.

---

RUGGEDCOM ROX II employs a stateful firewall system known as netfilter, a subsystem of the Linux kernel that provides the ability to examine IP packets on a per-session basis.

For more information about firewalls, refer to "Firewall Concepts" (Page 195).

### 6.10.1 Firewall Concepts

This section describes some of the concepts important to the implementation of firewalls in RUGGEDCOM ROX II.

#### 6.10.1.1 Stateless vs. Stateful Firewalls

There are two types of firewalls: stateless and stateful.

**Stateless** or static firewalls make decisions about traffic without regard to traffic history. They simply open a path for the traffic type based on a TCP or UDP port number. Stateless firewalls are relatively simple, easily handling Web and e-mail traffic. However, stateless firewalls have some disadvantages. All paths opened in

the firewall are always open, and connections are not opened or closed based on outside criteria. Static IP filters offer no form of authentication.

**Stateful** or session-based firewalls add considerably more complexity to the firewalling process. They track the state of each connection, look at and test each packet (connection tracking), and recognize and manage as a whole traffic from a particular protocol that is on connected sets of TCP/UDP ports.

### 6.10.1.2 Linux netfilter

Netfilter, a subsystem of the Linux kernel, is a stateful firewall that provides the ability to examine IP packets on a per-session basis.

Netfilter uses rulesets, which are collections of packet classification rules that determine the outcome of the examination of a specific packet. The rules are defined by iptables, a generic table structure syntax and utility program for the configuration and control of netfilter.

RUGGEDCOM ROX II implements an IP firewall using a structured user interface to configure iptables rules and netfilter rulesets.

### 6.10.1.3 Network Address Translation

Network Address Translation (NAT) enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. The netfilter NAT function makes all necessary IP address translations as traffic passes between the Intranet and the Internet. NAT is often referred to in Linux as IP Masquerading.

NAT itself provides a type of firewall by hiding internal IP addresses. More importantly, NAT enables a network to use more internal IP addresses. Since they are only used internally, there is no possibility of conflict with IP addresses used by other organizations. Typically, an internal network is configured to use one or more of the reserved address blocks described in RFC1918.

Table 6.1: RFC1918 Reserved IP Address Blocks

IP Network/Mask	Address Range
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

When a packet from a host on the internal network reaches the NAT gateway, its source address and source TCP/UDP port number are recorded. The address and port number is translated to the public IP address and an unused port number on the public interface. When the Internet host replies to the internal host's packet, it is addressed to the NAT gateway's external IP address at the translation port number. The NAT gateway searches its tables and makes the opposite changes it made to the outgoing packet. NAT then forwards the reply packet to the internal host.

Translation of ICMP packets happens in a similar fashion, but without the source port modification.

NAT can be used in static and dynamic modes. Static NAT (SNAT) masks the private IP addresses by translating each internal address to a unique external address. Dynamic NAT translates all internal addresses to one or more external addresses.

#### 6.10.1.4 Port Forwarding

Port forwarding, also known as redirection, allows traffic coming from the Internet to be sent to a host behind the NAT gateway.

Previous examples have described the NAT process when connections are made from the Intranet to the Internet. In those examples, addresses and ports were unambiguous.

When connections are attempted from the Internet to the Intranet, the NAT gateway will have multiple hosts on the Intranet that could accept the connection. It needs additional information to identify the specific host to accept the connection.

Suppose that two hosts, 192.168.1.10 and 192.168.1.20 are located behind a NAT gateway having a public interface of 213.18.101.62. When a connection request for http port 80 arrives at 213.18.101.62, the NAT gateway could forward the request to either of the hosts (or could accept it itself). Port forwarding configuration could be used to redirect the requests to port 80 to the first host.

Port forwarding can also remap port numbers. The second host may also need to answer http requests. As connections to port 80 are directed to the first host, another port number (such as 8080) can be dedicated to the second host. As requests arrive at the gateway for port 8080, the gateway remaps the port number to 80 and forwards the request to the second host.

Port forwarding also takes the source address into account. Another way to solve the above problem could be to dedicate two hosts 200.0.0.1 and 200.0.0.2 and have the NAT gateway forward requests on port 80 from 200.0.0.1 to 192.168.1.10 and from 200.0.0.2 to 192.168.1.20.

#### 6.10.1.5 Protecting Against a SYN Flood Attack

RUGGEDCOM ROX II responds to SYN packets according to the TCP standard by replying with a SYN-ACK packet for open ports and an RST packet for closed ports. If the device is flooded by a high frequency of SYN packets, the port being flooded may become unresponsive.

To prevent SYN flood attacks on closed ports, set the firewall to block all traffic to closed ports. This prevents SYN packets from reaching the kernel.

Siemens also recommends setting the listen ports to include IP addresses on separate interfaces. For example, set the device to listen to an IP address on switch.0001 and fe-cm-1. This will make sure that one port is accessible if the other is flooded.



### 6.10.1.6 Protecting Against IP Spoofing

IP spoofing is a technique where IP packets are created with a false source IP address, with the intent of concealing the identity of the sender or impersonating a trusted host. As a result, unauthorized users can gain access to a network.

In RUGGEDCOM ROX II, IP spoofing can be prevented by enabling the **Route Filter** and **Log Martians** for the firewall interface.

For information about enabling **Route Filter** and **Log Martians**, refer to "Adding an Interface" (Page 205).

### 6.10.1.7 Active and Working Firewall Configurations

To safely make changes to the firewall settings without first disabling the firewall or making changes live during operation, RUGGEDCOM ROX II supports an active and a working configuration. The active configuration is the configuration that will be used when the firewall is enabled. The working configuration is an alternate configuration that can be modified and validated without affecting the current firewall settings.

 <b>NOTICE</b>
<b>Configuration hazard – risk of authorized access</b>
Only make changes to the working firewall configuration and make sure all changes are validated before enabling the working configuration as the new active configuration. Do not make changes to the current active configuration. The firewall will be disabled automatically if any validation errors are detected in the active configuration.

## 6.10.2 Viewing a List of Firewalls

To view a list of firewalls, navigate to **Firewall**. If firewalls have been configured, a list appears.

If no firewalls have been configured, add firewalls as needed. For more information, refer to "Adding a Firewall" (Page 198).

## 6.10.3 Adding a Firewall

To add a new firewall, do the following:

1. Navigate to **Firewall**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Configuration Name	<b>Synopsis:</b> A string

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string An optional description string.

6. Add interfaces associated with the firewall. For more information about adding interfaces, refer to "Adding an Interface" (Page 205).
7. Add network zones for the firewall. Make sure a zone with the type **firewall** exists. For more information about adding network zones, refer to "Adding a Zone" (Page 203).
8. Associate an interface with each zone. For more information about associating interfaces with zones, refer to "Associating an Interface with a Zone" (Page 206).
9. Set the default policies for traffic control between zones. Make sure the policies are as restrictive as possible. For more information about configuring policies, refer to "Managing Policies" (Page 209).
10. Configure the network address translation (NAT), masquerading or static network address translation (SNAT) settings. For more information about configuring NAT settings, refer to "Managing Network Address Translation Settings" (Page 212). For more information about configuring masquerading and/or SNAT settings, refer to "Managing Masquerade and SNAT Settings" (Page 213).
11. If hosts on the network must accept sessions from the Internet, configure the firewall to support Destination Network Address Translation (DNAT). For more information about configuring hosts, refer to "Managing Hosts" (Page 207).
12. If required, configure rules that override the default policies. For more information about configuring rules, refer to "Managing Rules" (Page 215).
13. If required, configure support for a VPN. For more information, refer to:
  - "Configuring the Firewall for a VPN" (Page 200)
  - "Configuring the Firewall for a VPN in a DMZ" (Page 202)
14. Validate the configuration. For more information about validating a firewall configuration, refer to "Validating a Firewall Configuration" (Page 219).
15. Enable the firewall. For more information, refer to "Enabling/Disabling a Firewall" (Page 219).
16. Commit the changes.

### 6.10.4 Deleting a Firewall

To delete a firewall, do the following:

1. Navigate to **Firewall**.
2. Select the firewall to be deleted, and then click **Delete Entry**.
3. Commit the changes.

### 6.10.5 Working with Multiple Firewall Configurations

RUGGEDCOM ROX II allows users to create multiple firewall configurations and work with one configuration while another is active.

To set one configuration as the working configuration and another as the active configuration, do the following:

1. Navigate to **Firewall**.
2. Under **Specify work configuration**, select a firewall configuration from the list to work on. The firewall configuration selected under **Specify active configuration** is the configuration that is actively running.
3. Commit the change.

### 6.10.6 Configuring the Firewall for a VPN

To configure the firewall for a policy-based VPN, do the following:

1. Make sure a basic firewall has been configured. For more information about configuring a firewall, refer to "Adding a Firewall" (Page 198).
2. Navigate to **Firewall** and select the firewall to configure.
3. Make sure zones for local, network and VPN traffic have been configured. For more information about managing zones, refer to "Managing Zones" (Page 203).
4. Make sure a zone called *Any* exists and is of the type IPsec. For more information about managing zones, refer to "Managing Zones" (Page 203).
5. Configure the interface that carries the encrypted IPsec traffic. Make sure it is associated with the *Any* zone, as it will be carrying traffic for all zones. For more information about associating interfaces with zones, refer to "Associating an Interface with a Zone" (Page 206).
6. Configure a host for the interface that carries the unencrypted IPsec traffic. Make sure the VPN zone is associated with the interface. If VPN tunnels to multiple remote sites are required, make sure host entry exists for each or collapse them into a single subnet. For more information about configuring hosts, refer to "Managing Hosts" (Page 207).
7. Configure a second host for the interface that carries the encrypted IPsec traffic. Make sure the interface is associated with the network zone and specify a wider

subnet mask, such as 0.0.0.0/0. For more information about configuring hosts, refer to "Managing Hosts" (Page 207).

---

**Note**

The VPN host must be specified before the network host so the more specific VPN zone subnet can be inspected first.

---

The following are examples of possible host configurations:

Host	Interface	Subnet	IPsec Zone
vpn	W1ppp	192.168.1.0/24	Yes
net	W1ppp	0.0.0.0/0	No

- Configure rules with the following parameter settings for the UDP, Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols:

---

**Note**

The IPsec protocol operates on UDP port 500, using protocols Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols. The firewall must be configured to accept this traffic in order to allow the IPsec protocol.

---

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	net	fw	ah	—
Accept	net	fw	esp	—
Accept	net	fw	udp	500

For more information about configuring rules, refer to "Managing Rules" (Page 215).

- Configure the following rule to allow traffic from Libreswan, the IPsec daemon, to enter the firewall:

---

**Note**

IPsec traffic arriving at the firewall is directed to Libreswan, the IPsec daemon. Libreswan decrypts the traffic and then forwards it back to the firewall on the same interface that originally received it. A rule is required to allow traffic to enter the firewall from this interface.

---

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	vpn	loc	—	—

For more information about configuring rules, refer to "Managing Rules" (Page 215).

## 6.10.7 Configuring the Firewall for a VPN in a DMZ

When the firewall needs to pass VPN traffic through to another device, such as a VPN device in a Demilitarized Zone (DMZ), and then a DMZ zone and special rules are required.

To configure the firewall for a VPN in a DMZ, do the following:

1. Make sure a basic firewall has been configured. For more information about configuring a firewall, refer to "Adding a Firewall" (Page 198).
2. Navigate to **Firewall** and select the firewall to configure.
3. Make sure a zone called *dmz* exists. For more information about managing zones, refer to "Managing Zones" (Page 203).
4. Configure rules with the following parameter settings for the UDP, Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols:

### Note

The IPsec protocol operations on UDP port 500, using protocols Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols. The firewall must be configured to accept this traffic in order to allow the IPsec protocol.

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	Net	dmz	Ah	—
Accept	Net	dmz	Esp	—
Accept	Net	dmz	UDP	500
Accept	dmz	Net	Ah	—
Accept	dmz	Net	Esp	—
Accept	dmz	Net	Udp	500

For more information about configuring rules, refer to "Managing Rules" (Page 215).

## 6.10.8 Configuring Netfilter

To configure Netfilter, do the following:

1. Navigate to **Administration » ICMP**.
2. Under **TCP Established Connection Track Timeout**, set the time in seconds (s) a stale TCP connection can reside in the connection tracking table. The value can be between 300 and 432000 s. The default value is 432000 s, or five days.
3. Commit the change.

## 6.10.9 Managing Zones

A network zone is a collection of interfaces for which forwarding decisions are made. Common zones include:

Zone	Description
Net	The Internet
Loc	The local network
DMZ	Demilitarized zone
Fw	The firewall itself
Vpn1	IPsec connections on w1ppp
Vpn2	IPsec connections on w2ppp

New zones may be defined as needed. For example, if each Ethernet interface is part of the local network zone, disabling traffic from the Internet zone to the local network zone would disable traffic to all Ethernet interfaces. If access to the Internet is required for some Ethernet interfaces, but not others, a new zone may be required for those interfaces.

### 6.10.9.1 Viewing a List of Zones

To view a list of zones, navigate to the **Zone** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If zones have been configured, a list appears.

If no zones have been configured, add zones as needed. For more information, refer to "Adding a Zone" (Page 203).

### 6.10.9.2 Adding a Zone

To add a new zone for a firewall, do the following:

1. Navigate to the **Zone** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Zone Name	<p><b>Synopsis:</b> A string between 0 and 5 characters long</p> <p>A unique name to assign to this zone. Be sure to <b>also create</b> a zone called <b>fw</b> that is of the zone type <b>firewall</b>.</p>

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<p><b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ]</p> <p><b>Default:</b> ipv4</p> <p>Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.</p>
Type	<p><b>Synopsis:</b> [ ipv4   ipsec   firewall ]</p> <p><b>Default:</b> ipv4</p> <p>Zone types are plain IPv4, firewall, or IPSec</p>
Description	<p><b>Synopsis:</b> A string</p> <p>(Optional) The description string for this zone</p>

6. Commit the changes.

### 6.10.9.3 Deleting a Zone

To delete a zone, do the following:

1. Navigate to the **Zone** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the zone to be deleted then click **Delete Entry**.
3. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
4. Commit the changes.

## 6.10.10 Managing Interfaces

Firewall interfaces are the LAN and WAN interfaces available to the router. Each interface must be placed in a network zone. If an interface supports more than one zone, its zone must be marked as *undefined* and the interface must use the zone host's setup to define a zone for each subnet on the interface.

### Example

Interface	Zone
Switch.0001	Loc
Switch.0002	Loc
Switch.0003	Any
Switch.0004	DMZ
W1ppp	net

### 6.10.10.1 Viewing a List of Interfaces

To view a list of interfaces, navigate to the **Interface** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If interfaces have been configured, a list appears.

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an Interface" (Page 205).

### 6.10.10.2 Adding an Interface

To configure an interface for a firewall, do the following:

1. Navigate to **ip** and record the name of the chosen interface.
2. Navigate to the **Interface** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
3. Click **Add Entry**.
4. Configure the following parameter as required:

Parameter	Description
Interface Name	<b>Synopsis:</b> A string Currently active or not - add '+' for the same interfaces: ppp+.

5. Click **OK**.
6. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ] <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Description	<b>Synopsis:</b> A string (Optional) The description string for this interface

7. Click **Interface Options**, and then configure the following parameter(s) as required:

Parameter	Description
ARP Filter	IPv4 ONLY- See additional info. Responds only to ARP requests for configured IP addresses (This is permanently enabled system wide since ROX 2.3.0, and this option no longer has any effect).
Routeback	IPv4 and IPv6 - Interface traffic routed back out that same interface.



Parameter	Description
TCP Flags	IPv4 and IPv6. Illegal combinations of TCP flags dropped and logged at info level.
DHCP	IPv4 and IPv6 - Allows DHCP datagrams to enter and leave the interface.
NORFC1918	Not currently implemented
Route Filter	IPv4 and IPv6 - Enables /rpfiler/ spoofing protection
Proxy ARP	IPv4 ONLY - Enables proxy ARP.
MAC List	Not currently implemented
No Smurfs	IPv4 ONLY - Packets with broadcast address as source dropped and logged at info level.
Log Martians	IPv4 ONLY - Logging of packets with impossible source addresses.

8. Associate the interface with a pre-defined zone or mark the associated zone as undefined. For more information about associating the interface with a zone, refer to "Associating an Interface with a Zone" (Page 206).
9. Configure a broadcast address for the interface. For more information configuring a broadcast address, refer to "Configuring a Broadcast Address" (Page 207).
10. Commit the changes.

### 6.10.10.3 Associating an Interface with a Zone

To associate an interface with a predefined zone or mark the associated zone as undefined, do the following:

1. Navigate to the **Interface - { interface }** tab under **Firewall » { firewall }**, where { interface } is the name of the interface and { firewall } is the name of the firewall.
2. In the **Zone** column, select one of the following options:

Option	Description
<b>A Predefined Zone</b>	Select an available predefined zone.
<b>An Undefined Zone</b>	Select to mark the zone as undefined.

3. Commit the change.

#### 6.10.10.4 Configuring a Broadcast Address

To configure a broadcast address for an interface, do the following:

1. Navigate to the **Interface - { interface }** tab under **Firewall{ firewall }**, where { interface } is the name of the interface and { firewall } is the name of the firewall.
2. Click **Broadcast Address**.
3. Select one of the following options:

Option	Description
<b>IPv4 Address</b>	Enter an IPv4 broadcast address.
<b>Auto Detect</b>	Select to allow ROX to automatically detect the broadcast address(es).
<b>None</b> (default)	Select to not define a broadcast address. This is the default option.

4. Commit the change.

#### 6.10.10.5 Deleting an Interface

To delete an interface, do the following:

1. Navigate to the **Interface** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the interface to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 6.10.11 Managing Hosts

Hosts are used to assign zones to individual hosts or subnets (if the interface supports multiple subnets). This allows the firewall to receive a packet and then redirect it to the same device that received it. This functionality is useful for VPN setups to handle the VPN traffic separately from the other traffic on the interface which carries the VPN traffic.

#### Hosts for the Local and Guests Zones

Zone	Interface	IP Address or Network
Local	Switch.0003	10.0.0.0/8
Guests	Switch.0003	192.168.0.0/24

### 6.10.11.1 Viewing a List of Hosts

To view a list of hosts, navigate to the **Zone Hosts** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If hosts have been configured, the **Hosts** table appears.

If no hosts have been configured, add hosts as needed. For more information, refer to "Adding a Host" (Page 208).

### 6.10.11.2 Adding a Host

To add a new host for a firewall, do the following:

1. Navigate to the **Zone Hosts** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string The name of a host configuration entry.

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
IPSec Zone	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false
IP Type	<b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ] <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Zone	<b>Synopsis:</b> A string between 0 and 5 characters long A pre-defined zone
Interface	<b>Synopsis:</b> A string between 1 and 15 characters long A pre-defined interface to which optional IPs and/or networks can be added.
IP Address List	<b>Synopsis:</b> A string Additional IP addresses or networks - comma separated, or a range in the form of low.address-high.address

Parameter	Description
Description	<b>Synopsis:</b> A string (Optional) The description string for this host.

6. Commit the changes.

### 6.10.11.3 Deleting a Host

To delete a host, do the following:

1. Navigate to the **Zone Hosts** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the host to be deleted then click **Delete Entry**.
3. Commit the change.

## 6.10.12 Managing Policies

Policies define the default actions for establishing a connection between different firewall zones. Each policy consists of a source zone, a destination zone and an action to be performed when a connection request is received.

The following example illustrates the policies for establishing connections between a local network and the Internet.

Policy	Source Zone	Destination Zone	Action
1	Loc	Net	ACCEPT
2	Net	All	DROP
3	All	All	REJECT

Each policy controls the connection between the source and destination zones. The first policy accepts all connection requests from the local network to the Internet. The second policy drops or ignores all connection requests from the Internet to any device on the network. The third policy rejects all other connection requests and sends a TCP RST or an ICMP destination-unreachable packet to the client.

The order of the policies is important. If the last policy in the example above were to be the first policy, the firewall would reject all connection requests.

---

#### Note

The source and destination zones must be configured before a policy can be created. For more information about zones, refer to "Managing Zones" (Page 203).

---

#### Note

Policies for specific hosts or types of traffic can be overridden by rules. For more information about rules, refer to "Managing Rules" (Page 215).

---

### 6.10.12.1 Viewing a List of Policies

To view a list of policies, navigate to the **Policy** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If policies have been configured, a list appears.

If no policies have been configured, add policies as needed. For more information, refer to "Adding a Policy" (Page 210).

### 6.10.12.2 Adding a Policy

To configure a policy for the firewall, do the following:

1. Navigate to the **Policy** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Policy Name	<b>Synopsis:</b> A string Enter a name tag for this policy.

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ] <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Policy	<b>Synopsis:</b> [ accept   drop   reject   continue ] <b>Default:</b> reject A default action for connection establishment between different zones.
Log Level	<b>Synopsis:</b> [ none   debug   info   notice   warning   error   critical   alert   emergency ] <b>Default:</b> none (Optional) Determines whether or not logging will take place and at which logging level.
Description	<b>Synopsis:</b> A string (Optional) The description string for this policy.

6. Configure the source zone for the policy. For more information, refer to "Configuring the Source Zone" (Page 211).

7. Configure the destination zone for the policy. For more information, refer to "Configuring the Destination Zone" (Page 211).
8. Commit the changes.

### 6.10.12.3 Configuring the Source Zone

To configure the source zone for a firewall policy, do the following:

1. Navigate to the **Policy** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select a policy, and then select one of the following options under **Source Pre-Defined Zone**:

Option	Description
<b>A Predefined Zone</b>	Select an available predefined zone.
<b>All</b>	Select to apply the firewall policy to all zones.

3. Commit the changes.

### 6.10.12.4 Configuring the Destination Zone

To configure the destination zone for a firewall policy, do the following:

1. Navigate to the **Policy** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select a policy, and then select one of the following options under **Destination Pre-Defined Zone**:

Option	Description
<b>A Predefined Zone</b>	Select an available predefined zone.
<b>All</b>	Select to apply the firewall policy to all zones.

3. Commit the change.

### 6.10.12.5 Deleting a Policy

To delete a policy, do the following:

1. Navigate to the **Policy** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the policy to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 6.10.13 Managing Network Address Translation Settings

Network address translation entries can be used to set up a one-to-one correspondence between an external address on the firewall and the RFC1918 address of a host behind the firewall. This is often set up to allow connections to an internal server from outside the network.

---

### Note

Destination Network Address Translation (DNAT) can be setup by configuring the destination zone in a rule. For more information on rules, refer to "Managing Rules" (Page 215).

---

### 6.10.13.1 Viewing a List of NAT Settings

To view a list of NAT settings, navigate to the **NAT** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If NAT settings have been configured, a list appears.

If no NAT settings have been configured, add NAT settings as needed. For more information, refer to "Adding a NAT Setting" (Page 212).

### 6.10.13.2 Adding a NAT Setting

To configure a Network Address Translation (NAT) entry, do the following:

1. Navigate to the **NAT** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
NAT Entry Name	<b>Synopsis:</b> A string Enter a name for this NAT entry

4. Click **OK**.
5. Configure the following parameter(s) as required:

---

### Note

ARP or Ping requests for the translated external IP address will be blocked by the unit unless the external IP address is manually added to the device's external interface. For more information about adding IP addresses to routable interfaces, refer to "Managing IP Addresses for Routable Interfaces" (Page 223).

---

Parameter	Description
External IP Address	<b>Synopsis:</b> A string The external IP Address. The address must not be a DNS name. External IP addresses must be manually added to the interface.
Interface	<b>Synopsis:</b> A string between 1 and 15 characters long An interface that has an external IP address.
IP Alias	Create IP Alias for NAT rule.
Internal Address	<b>Synopsis:</b> A string The internal IP address. The address must not be a DNS Name.
Limit Interface	Translation only effective from the defined interface.
Local	Translation effective from the firewall system.
Description	<b>Synopsis:</b> A string (Optional) The description string for this NAT entry.

6. Commit the change.

### 6.10.13.3 Deleting a NAT Setting

To delete a network address translation entry, do the following:

1. Navigate to the **NAT** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the NAT setting to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 6.10.14 Managing Masquerade and SNAT Settings

Masquerading and Source Network Address Translation (SNAT) are forms of dynamic Network Address Translation (NAT). Both hide a subnetwork behind a single public IP address.

Masquerading is used when the ISP provides a dynamic IP address. SNAT is used when the ISP provides a static IP address.

### 6.10.14.1 Viewing a List of Masquerade and SNAT Settings

To view a list of masquerade and SNAT settings, navigate to the **MASQ** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If masquerade or SNAT settings have been configured, a list appears.



If no masquerade or SNAT settings have been configured, add masquerade or SNAT settings as needed. For more information, refer to "Adding Masquerade or SNAT Settings" (Page 214).

### 6.10.14.2 Adding Masquerade or SNAT Settings

To add rules for masquerading or SNAT, do the following:

#### Note

Masquerading requires that the IP address being used to masquerade must belong to the router. When configuring the SNAT address under masquerading, the SNAT address must be one of the IP addresses on the outbound interface.

1. Navigate to the **MASQ** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Entry Name	<b>Synopsis:</b> A string A name for this masquerading configuration entry.

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ] <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Outgoing Interface	<b>Synopsis:</b> A string An outgoing interface list - usually the internet interface.
Outgoing Interface Specifics	<b>Synopsis:</b> A string (Optional) An outgoing interface list - specific IP destinations for the out-interface.
IP Alias	Create IP Alias for NAT rule.
Source Hosts	<b>Synopsis:</b> A string Subnet range or comma-separated list of hosts (IPs)

Parameter	Description
SNAT Address	<b>Synopsis:</b> A string  (Optional) By specifying an address here, SNAT will be used and this will be the source address.
Description	<b>Synopsis:</b> A string  (Optional) The description string for this masq entry.

6. Commit the changes.

### 6.10.14.3 Deleting a Masquerade or SNAT Setting

To delete a masquerade or SNAT setting, do the following:

1. Navigate to the **MASQ** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the SNAT setting to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 6.10.15 Managing Rules

Rules establish exceptions to the default firewall policies for certain types of traffic, sources or destinations. Each rule defines specific criteria. If an incoming packet matches that criteria, the default policy is overridden and the action defined by the rule is applied.

### 6.10.15.1 Viewing a List of Rules

To view a list of rules, navigate to the **Rule** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall. If rules have been configured, a list appears.

If no rules have been configured, add rules as needed. For more information, refer to "Adding a Rule" (Page 215).

### 6.10.15.2 Adding a Rule

To configure a rule for a firewall, do the following:

1. Navigate to the **Rule** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Rule Name	<b>Synopsis:</b> A string Enter a unique name that identifies this rule.

4. Click **OK**.
5. Configure the following parameter(s) as required:

---

#### Note

When applying new rules, previous traffic seen by the router might still be considered as having valid connections by the connection tracking table. For instance:

1. A rule for the TCP and UDP protocols is applied.
2. The router sees both TCP and UDP traffic that qualifies for NAT.
3. The rule is then modified to allow only UDP.
4. The router will still see TCP packets (i.e. retransmission packets).

If required, reboot the router to flush all existing connection streams.

---

Parameter	Description
IP Type	<b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ] <b>Default:</b> ipv4  Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Action	<b>Synopsis:</b> [ accept   drop   reject   continue   redirect   dnat-   dnat   copy-dnat ] <b>Default:</b> reject  The final action to take on incoming packets matching this rule. Options include: <ul style="list-style-type: none"> <li>• accept: Allows the connection request to proceed.</li> <li>• continue: Passes the connection request past any other rules.</li> <li>• copy-dnat: Sends a copy to a second system using a DNAT rule. Protocol must be set to 'udp', and Original Destination must be defined.</li> <li>• dnat: Forwards the request to another system and (optionally) another port.</li> <li>• dnat-: Only generates the DNAT IPtables rule and not the companion ACCEPT rule.</li> <li>• drop: The connection request is ignored. No notification is sent.</li> <li>• redirect: Redirects the request to a local TCP port number on the local firewall.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>reject: Rejects the connection with an RST (TCP) or ICMP destination-unreachable.</li> </ul>
Source Zone Hosts	<p><b>Synopsis:</b> A string</p> <p>(Optional) Add comma-separated host IPs to a predefined source-zone.</p>
Destination Zone Hosts	<p><b>Synopsis:</b> A string</p> <p>(Optional) Add comma-separated host IPs to the destination-zone - may include :port for DNAT or REDIRECT.</p>
Log Level	<p><b>Synopsis:</b> [ none   debug   info   notice   warning   error   critical   alert   emergency ]</p> <p><b>Default:</b> none</p> <p>(Optional) Determines whether or not logging will take place and at which logging level.</p>
Protocol	<p><b>Synopsis:</b> A string or [ tcp   udp   icmp   all ]</p> <p><b>Default:</b> all</p> <p>The protocol to match for this rule - must be 'udp' for rules using copy-dnat actions.</p>
Source Port	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> none</p> <p>(Optional) The TCP/UDP port(s) the connection originated from. Default: all ports. Add a single port or a list of comma-separated ports</p>
Destination Port	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> none</p> <p>(Optional) The TCP/UDP port(s) the connection is destined for. Default: all ports. Add a single port or a list of comma-separated ports</p>
Original Destination	<p><b>Synopsis:</b> A string or [ None ]</p> <p><b>Default:</b> none</p> <p>(Optional) The destination IP address in the connection request as it was received by the firewall - (mandatory) for rules using copy-dnat actions.</p>
Helper	<p><b>Synopsis:</b> [ none   ftp ]</p> <p><b>Default:</b> none</p> <p>The Netfilter Helper to associate with this rule.</p>
Description	<p><b>Synopsis:</b> A string</p> <p>(Optional) The description string for this rule.</p>

- Configure the source zone for the rule. For more information, refer to "Configuring the Source Zone" (Page 218).

7. Configure the destination zone for the rule. For more information, refer to "Configuring the Destination Zone" (Page 218).
8. Commit the changes.

### 6.10.15.3 Configuring the Source Zone

A firewall rule can be applied to a single source zone, select source zones, or all source zones.

To configure the source zone(s) for a firewall rule, do the following:

1. Navigate to the **Rule** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.

#### NOTICE

It is recommended to select a specific zone, rather than all zones. Corresponding iptables rules between each active zone to all other zones will be created for each rule whose source zone and destination zone are both set to **all**, which may affect system performance and configuration commit times.

2. Select a rule, and then select one of the following options:

Option	Description
<b>A Predefined Zone</b>	Select an available predefined zone.
<b>Other</b>	Enter a comma-separated list of available zones.
<b>All</b>	Select to apply the firewall policy to all zones.

3. Commit the change.

### 6.10.15.4 Configuring the Destination Zone

A firewall rule can be applied to a single destination zone, select destination zones, or all destination zones.

To configure the destination zone for a firewall rule, do the following:

1. Navigate to the **Rule** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.

#### NOTICE

It is recommended to select a specific zone, rather than all zones. Corresponding iptables rules between each active zone to all other zones will be created for each rule whose source zone and destination zone are both set to **all**, which may affect system performance and configuration commit times.

2. Select a rule, and then select one of the following options:

Option	Description
<b>A Predefined Zone</b>	Select an available predefined zone.
<b>Other</b>	Enter a comma-separated list of available zones.
<b>All</b>	Select to apply the firewall policy to all zones.

3. Commit the change.

### 6.10.15.5 Deleting a Rule

To delete a rule, do the following:

1. Navigate to the **Rule** tab under **Firewall » { firewall }**, where { firewall } is the name of the firewall.
2. Select the rule to be deleted, and then click **Delete Entry**.
3. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
4. Commit the change.

### 6.10.16 Validating a Firewall Configuration

To validate a firewall configuration, do the following:

1. Navigate to the **Parameters - { configuration }** tab under **Firewall » { firewall }**, where { configuration } is the name of the configuration and { firewall } is the name of the firewall.
2. Under **Specify work configuration**, select the firewall configuration from the list.
3. Commit the change.

### 6.10.17 Enabling/Disabling a Firewall

To enable or disable the firewall, do the following:

#### NOTICE

Enabling or disabling the firewall will reset – but not disable – the BFA protection mechanism, if previously enabled. Any hosts that were previously blocked will be allowed to log in again. If multiple hosts are actively attacking at the time, this could result in reduced system performance.

1. Navigate to the **Parameters - { configuration }** tab under **Firewall » { firewall }**, where { configuration } is the name of the configuration and { firewall } is the name of the firewall.

2. Under **Specify active configuration**, select the firewall configuration from the list to enable.
3. Select the **Enabled** check box to enable the firewall or clear the check box to disable the firewall.
4. Commit the change.

## 6.11 Restricting Management Access to Specific Interfaces

RUGGEDCOM ROX II can be configured to restrict CLI, WebUI, SNMP and NETCONF management access to specific VLANs and/or source IP addresses.

The following examples describe how to configure RUGGEDCOM ROX II to restrict management access via IP address and firewall configuration.

### Specifying Listen IP Interfaces

In Layer 3 routing, RUGGEDCOM ROX II must have an IP address on each of the interfaces it is routing traffic between. However, administrative services do not need to be offered for each IP address.

In this configuration, a Listen IP address is configured for each of the available services, rather than being available on all configured interface addresses as per default.

#### NOTICE

##### Accessibility hazard – risk of access disruption

The following configuration can prevent administration of the device if the specified IP address becomes unreachable. Make sure serial console access is available during configuration.

#### Note

By default, ports are reachable over IPv6 addresses and their associated ports. To restrict access, make sure no extra IP port is configured for each service. For more information about configuring extra IP ports for available services, refer to "Security" (Page 127).

```
admin
cli
listen-ip    192.168.0.20
!
sftp
listen-ip    192.168.0.20
!
webui
listen-ip    192.168.0.20
no ssl-redirect-enabled
!
netconf
listen-ip    192.168.0.20
!
```

```
snmp
listen-ip 192.168.0.20
!
!
```

For more information about configuring the Listen IP for available services, refer to "Security" (Page 127).

For more information about configuring the Listen IP for available services, refer to "Restricting Management Access to Specific Interfaces" (Page 220).

## Excluding the Management VLAN from the Network

In Layer 3 routing, each VLAN must have an IP address. However, VLANs handled by the device only as a Layer 2 switch do not need an IP address. As such, the device is not accessible through the network via IP address, and is therefore not exposed to directed IP-based traffic.

In this example, RUGGEDCOM ROX II exists on VLAN1 and VLAN3, and can route traffic between them, but does not exist on the VLAN2 network. It will only send Layer2 traffic between devices on VLAN2 switch ports. Administration is via the interface on VLAN3. The address on VLAN1 can be pinged, but no web or CLI interfaces exist on it.

```
ip switch.0001
no bandwidth
ipv4
address 192.168.15.1/24
no peer
!
!
!
ip switch.0002
no bandwidth
!
ip switch.0003
no bandwidth
ipv4
address 192.168.0.20/24
no peer
!
!
!
```

For more information about configuring IP addresses, refer to "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).

## Using a Firewall to Restrict Source IP Addresses

A firewall can be configured to restrict source IP addresses.

This configuration allows any source device to ping the RUGGEDCOM ROX II interfaces, but only devices with a specific IP address are granted admin access for a single administrator PC. All other connections are refused.

```
security
firewall
fwconfig asbestos
fwzone fw
```



## 6.11 Restricting Management Access to Specific Interfaces

```
type firewall
description "The DUT itself"
!
fwzone Loc
description "The rest of the world"
!
fwinterface switch+
zone Loc
description "All traffic on all switch ports"
!
fwpolicy fwprotect
source-zone all
destination-zone fw
description "Reject all input to DUT except as allowed in fwrules"
!
fwpolicy pass
source-zone all
destination-zone all
policy accept
description "Allow all other traffic (passing or leaving DUT)"
!
fwrule pingme
action accept
source-zone all
destination-zone fw
protocol icmp
destination-ports 8
description "Allow everyone to ping the DUT"
!
fwrule adm
action accept
source-zone all
source-zone-hosts 192.168.0.100
destination-zone fw
description "Allow admin workstation to connect to DUT"
!
!
!
```

For more information about configuring a firewall, refer to "Adding a Firewall" (Page 198).

## IP Address Assignment

This chapter describes features related to the assignment of IP addresses, such as DHCP and DNS.

### 7.1 Managing IP Addresses for Routable Interfaces

This section describes how to manage IP address for routable interfaces.

#### 7.1.1 Configuring Costing for Routable Interfaces

To configure the costing for a routable interface, do the following:

1. Navigate to the **Interface - { interface }** tab under **Interface » IP Interfaces**, where { interface } is the name of the routable interface.

---

#### Note

The **VRF Forwarding** list is not available for the *dummy* interface.

---

2. Configure the following parameter(s) as required:

Parameter	Description
Auto-Cost Bandwidth (kps)	<p><b>Synopsis:</b> An integer between 1 and 10000000000</p> <p><b>Default:</b> 10000</p> <p>This value is used in auto-cost calculations for this routable logical interface in kbps.</p>

3. Commit the change.

#### 7.1.2 Viewing Statistics for Routable Interfaces

To view basic statistics for all routable interfaces, navigate to the **Interface Status - { interface }** tab under **Interface » IP Interfaces**, where { interface } is the name of the routable interface.

The table displays the following information:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 15 characters long The name of the interface.
Admin State	<b>Synopsis:</b> [ not set   up   down   testing   unknown   dormant   notPresent   lowerLayerDown ] The port's administrative status.
State	<b>Synopsis:</b> [ not set   up   down   testing   unknown   dormant   notPresent   lowerLayerDown ] Shows whether the link is up or down.
Point to Point	<b>Synopsis:</b> [ true   false ] The point-to-point link.

To view statistics for a specific routable interface, do the following:

1. Navigate to the **Interface Status** tab under **Interface » IP Interfaces**.
2. Select an interface, and then select **Statistics Data**.

The following information is displayed:

Parameter	Description
Bytes	<b>Synopsis:</b> An integer The number of bytes received.
Packets	<b>Synopsis:</b> An integer The number of packets received.
Errors	<b>Synopsis:</b> An integer The number of error packets received.
Dropped	<b>Synopsis:</b> An integer The number of packets dropped by the receiving device.
Bytes	<b>Synopsis:</b> An integer The number of bytes transmitted.
Packets	<b>Synopsis:</b> An integer The number of packets transmitted.
Errors	<b>Synopsis:</b> An integer The number of error packets transmitted.
Dropped	<b>Synopsis:</b> An integer The number of packets dropped by the transmitting device.

Parameter	Description
Collisions	<b>Synopsis:</b> An integer The number of collisions detected on the port.

## 7.1.3 Managing IPv4 Addresses

This section describes how to manage IPv4 addresses for a routable interface.

### 7.1.3.1 Viewing a List of IPv4 Addresses

- To view a list of static IPv4 addresses for a routable interface, navigate to the **Interface** tab under **Interface » IP Interfaces**.
- Select an interface, and then select the **IPv4** tab. If addresses have been configured, a list appears.

If no addresses have been configured, add addresses as needed. For more information, refer to "Adding an IPv4 Address" (Page 225).

### 7.1.3.2 Adding an IPv4 Address

To add an IPv4 address to a routable interface, do the following:

- Navigate to the **Interface** tab under **Interface » IP Interfaces**.
- Select a routable interface, and then select the **IPv4** tab.
- Click **Add Entry**.
- Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string between 9 and 18 characters long The IPv4/Prefix (xxx.xxx.xxx.xxx/xx).

- Click **OK** to create the new address.
- Configure the following parameter(s) as required:

Parameter	Description
Peer	<b>Synopsis:</b> A string between 7 and 15 characters long The peer IPv4 Address (xxx.xxx.xxx.xxx, PPP, MLPPP, FrameRelay link only).

- Commit the changes.

### 7.1.3.3 Deleting an IPv4 Address

To delete an IPv4 address for a routable interface, do the following:

1. Navigate to the **Interface** tab under **Interface » IP Interfaces**, and then select a routable interface.
2. Select the **IPv4** tab.
3. Select the address to be deleted, and then click **Delete Entry**.
4. Commit the changes.

## 7.1.4 Managing IPv6 Addresses

This section describes how to manage IPv6 addresses for a routable interface.

### 7.1.4.1 Viewing a List of IPv6 Addresses

1. To view a list of IPv6 addresses for a routable interface, navigate to the **Interface** tab under **Interface » IP Interfaces**.
2. Select an interface, and then select the **IPv6** tab. If addresses have been configured, a list appears.

If no addresses have been configured, add addresses as needed. For more information, refer to "Adding an IPv6 Address" (Page 226).

### 7.1.4.2 Adding an IPv6 Address

To add an IPv6 address to a routable interface, do the following:

1. Navigate to the **Interface** tab under **Interface » IP Interfaces**.
2. Select a routable interface, and then select the **IPv6** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string between 4 and 43 characters long The IPv6 address/prefix of this interface.

5. Click **OK** to create the new address.
6. Commit the changes.

### 7.1.4.3 Deleting an IPv6 Address

To delete an IPv6 address for a routable interface, do the following:

1. Navigate to the **Interface** tab under **Interface » IP Interfaces**.
2. Select a routable interface, and then select the **IPv6** tab.
3. Select the address to be deleted, and then click **Delete Entry**.
4. Commit the changes.

### 7.1.5 Configuring IPv6 Neighbor Discovery

The Neighbor Discovery (ND) protocol in IPv6 is a replacement for IPv4 ARP messages. The protocol uses ICMPv6 messages for various purposes including:

- Finding a link-layer address of a neighbor
- Discovering neighbor routers
- Determining any change in the link-layer address
- Determining when a neighbor is down
- Sending network information from routers to hosts, which includes hop limit, MTU size, determining the network prefix used on a link, address auto configuration, and the default route information

The Neighbor Discovery protocol uses five types of ICMPv6 messages:

- **Router Solicitation (ICMPv6 type 133)**

This message is sent by hosts to routers as a request to router advertisement message. It uses a destination multicast address (i.e. FF02:2).

- **Router Advertisement Messages (ICMPv6 type 134)**

This message is used by routers to announce its presence in a network. The message includes network information related to IPv6 prefixes, default route, MTU size, hop limit and auto configuration flag. It uses a destination multicast address (i.e. FF02:1).

- **Neighbor Solicitation Messages (ICMPv6 type 135)**

This message is sent by hosts to determine the existence of another host on the same link. The goal is to find the link-layer of neighboring nodes.

- **Neighbor Advertisement Messages (ICMPv6 type 136)**

This message is sent by hosts to indicate the existence of the host and it provides information about its own link-layer address.

- **Redirect Messages (ICMPv6 type 137)**

This message is sent by a router to inform a host about a better router to reach a particular destination address.

Neighbor Discovery should be configured on all Ethernet interfaces enabled for IPv6.

To enable and configure settings for IPv6 Neighbor Discovery, do the following:

1. Navigate to the **IPv6** tab under **Interface » IP Interfaces**, and then click **IPv6 - Neighbor Discovery**.
2. Under **Router Advertisement Interval** form, configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 3 and 1800 The interval value.
Unit	<b>Synopsis:</b> [ sec   msec ] The interval unit.

3. Under **Neighbor Discovery** form, configure the following parameter(s) as required:

Parameter	Description
Enable Route Advertisement	Enable to send router advertisement messages.
Set Advertisement Interval Option	Includes an Advertisement Interval option which indicates to hosts the maximum time in milliseconds, between successive unsolicited router advertisements.
Set Home Agent Configuration Flag	Sets/unsets the flag in IPv6 router advertisements which indicates to hosts that the router acts as a home agent and includes a home agent option.
Home Agent Lifetime	<b>Synopsis:</b> An integer between 0 and 65520 <b>Default:</b> 1800 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent lifetime to hosts. A value of 0 means to place a router lifetime value.
Home Agent Preference	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 0 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent preference to hosts.
Set Managed Address Configuration Flag	The flag in IPv6 router advertisements, which indicates to hosts that they should use the managed (stateful) protocol for addresses autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.
Set Other Stateful Configuration Flag	The flag in IPv6 router advertisements, which indicates to hosts that they should use the administered (stateful) protocol to obtain autoconfiguration information other than addresses.

Parameter	Description
Router Lifetime	<p><b>Synopsis:</b> An integer between 0 and 9000</p> <p><b>Default:</b> 1800</p> <p>The value (in seconds) to be placed in the Router Lifetime field of router advertisements sent from the interface. Indicates the usefulness of the router as a default router on this interface. Setting the value to zero indicates that the router should not be considered a default router on this interface. It must be either zero or between the value specified with the IPv6 nd ra-interval (or default) and 9000 seconds.</p>
Reachable Time (Milliseconds)	<p><b>Synopsis:</b> An integer between 0 and 3600000</p> <p><b>Default:</b> 0</p> <p>The value (in milliseconds) to be placed in the Reachable Time field in the router advertisement messages sent by the router. The configured time enables the router to detect unavailable neighbors. The value zero means unspecified (by this router).</p>

- If required, add IPv6 network prefixes to the device can be advertised its neighbor. For more information on IPv6 network prefixes, refer to "Managing IPv6 Network Prefixes" (Page 229).
- Commit the changes.

## 7.1.6 Managing IPv6 Network Prefixes

An IPv6-capable interface can use Neighbor Discovery to advertise IPv6 network prefixes to its neighbor on the same link.

### 7.1.6.1 Adding an IPv6 Network Prefix

To add a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

- Navigate to the **IPv6** tab under **Interface » IP Interfaces**, and then click **IPv6 - Neighbor Discovery**.
- Under **Prefix**, click **Add Entry**.
- Configure the following parameter(s) as required:

Parameter	Description
IPv6 Prefix	<p><b>Synopsis:</b> A string between 4 and 43 characters long</p> <p>The IPv6 network/prefix.</p>

- Click **OK** to add the network prefix.
- Configure the following parameter(s) as required:



Parameter	Description
Valid Lifetime	<b>Synopsis:</b> An integer between 0 and 4294967295 or [ infinite ] The length of time in seconds during which time the prefix is valid for the purpose of on-link determination.
Preferred Lifetime	<b>Synopsis:</b> An integer between 0 and 4294967295 or [ infinite ] The length of time in seconds during which addresses generated from the prefix remain preferred.
Off Link	Indicates that advertisement makes no statement about on-link or off-link properties of the prefix.
No Autoconfig	Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
Set Router Address Flag	Indicates to hosts on the local link that the specified prefix contains a complete IP address by setting the R flag.

6. Commit the changes.

### 7.1.6.2 Deleting an IPv6 Network Prefix

To delete a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

1. Navigate to the **IPv6** tab under **Interface » IP Interfaces**, and then click **IPv6 - Neighbor Discovery**.
2. Under **Prefix**, select the network prefix to be deleted then click **Delete Entry**.
3. Commit the changes.

## 7.2 Managing the DHCP Relay Agent

A DHCP Relay Agent is a device that forwards DHCP packets between clients and servers when they are not on the same physical LAN segment or IP subnet. The feature is enabled if the DHCP server IP address and a set of access ports are configured.

DHCP Option 82 provides a mechanism for assigning an IP Address based on the location of the client device in the network. Information about the client's location can be sent along with the DHCP request to the server. Based on this information, the DHCP server makes a decision about an IP Address to be assigned.

DHCP Relay Agent takes the broadcast DHCP requests from clients received on the configured access port and inserts the relay agent information option (Option 82) into the packet. Option 82 contains the VLAN ID (2 bytes) and the port number of the access port (2 bytes: the circuit ID sub-option) and the switch's MAC address (the remote ID sub-option). This information uniquely defines the access port's position in

the network. For example, in RUGGEDCOM ROX II, the Circuit ID for VLAN 2 on Line Module (LM) 4 Port 15 is 00:00:00:02:04:0F.

The DHCP Server supporting DHCP Option 82 sends a unicast reply and echoes Option 82. The DHCP Relay Agent removes the Option 82 field and broadcasts the packet to the port from which the original request was received.

The DHCP Relay Agent communicates to the server on a management interface. The agent's IP address is the address configured for the management interface.

RUGGEDCOM ROX II can be configured to act as a DHCP Relay Agent that forwards DHCP and BOOTP requests from clients on one Layer 2 network to one or more configured DHCP servers on other networks. This allows the implementation of some measure of isolation between DHCP clients and servers.

The DHCP Relay Agent is configured to listen for DHCP and BOOTP requests on particular Ethernet and VLAN network interfaces, and to relay to a list of one or more DHCP servers. When a request is received from a client, RUGGEDCOM ROX II forwards the request to each of the configured DHCP servers. When a reply is received from a server, RUGGEDCOM ROX II forwards the reply back to the originating client.

---

**Note**

While DHCP Relay and DHCP Server may both be configured to run concurrently, they may not be configured to run on the same network interface.

---

## 7.2.1 Configuring the DHCP Relay Agent

To configure the DHCP relay agent, do the following:

1. Assign an IP address to the DHCP Server where DHCP queries are to be forwarded. For more information, refer to "Assigning a DHCP Server Address" (Page 231).

---

**Note**

If client ports do not reside on the same subnet, make sure to assign the client ports to different VLANs.

---

2. Add client ports. For more information, refer to "Adding a DHCP Client Port" (Page 232).
3. Commit the change.

## 7.2.2 Assigning a DHCP Server Address

To assign a DHCP server address to the DHCP relay agent, do the following:

1. Navigate to **Layer 3 » DHCP Relay Agent**.
2. Under **DHCP Server Address**, configure the following parameter(s) as required:

Parameter	Description
DHCP Server Address	<b>Synopsis:</b> A string  The IP address of the DHCP server to which DHCP queries will be forwarded from this relay agent.

3. Commit the change.

### 7.2.3 Viewing a List of DHCP Client Ports

To view a list of DHCP relay agent client ports, navigate to **Layer 3 » DHCP Relay Agent**. If client ports have been configured, a list appears.

If no client ports have been configured, add client ports as needed. For more information, refer to "Adding a DHCP Client Port" (Page 232).

### 7.2.4 Adding a DHCP Client Port

To add a client port for the DHCP relay agent, do the following:

1. Navigate to **Layer 3 » DHCP Relay Agent**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Slot	The slot and port (or list of ports, if aggregated in a port trunk) to be used as the client port.

4. Click **OK** to add the client port.
5. Commit the change.

### 7.2.5 Deleting a DHCP Client Port

To delete a client port for the DHCP relay agent, do the following:

1. Navigate to **Layer 3 » DHCP Relay Agent**.
2. Select the client port to be deleted then click **Delete Entry**.
3. Commit the change.

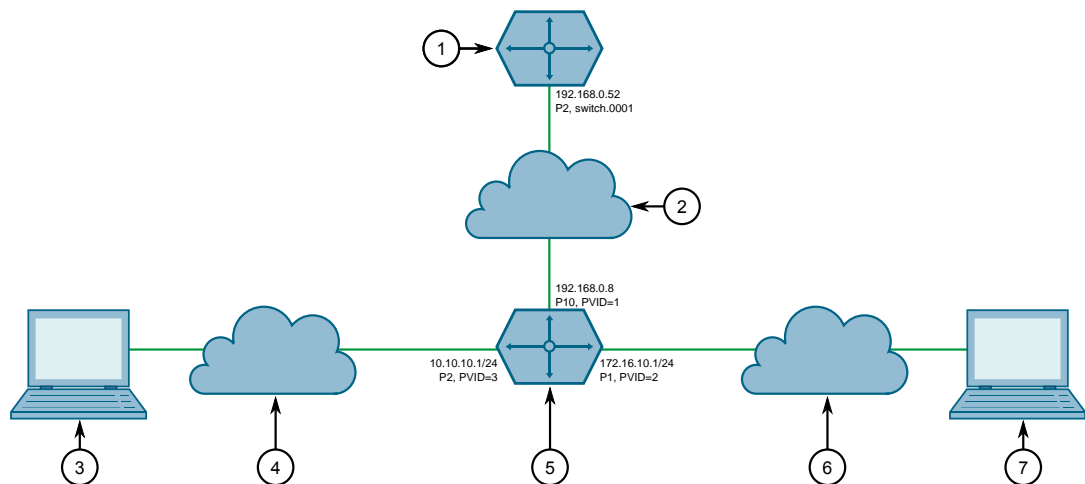
### 7.2.6 Example: Configuring the Device as a Relay Agent

This example demonstrates how to configure the device as a DHCP relay agent.

The following topology depicts a scenario where two clients on separate LANs require IP addresses on different subnets from a DHCP server. Each client connects to the DHCP relay agent using different VLANs. The DHCP relay agent manages the requests and responses between the clients and the DHCP server.

**NOTICE**

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① DHCP Server
- ② LAN A
- ③ Client 2
- ④ LAN B
- ⑤ DHCP Relay Agent (RUGGEDCOM ROX II Device)
- ⑥ LAN C
- ⑦ Client 1

Figure 7.1 Topology – Device as a Relay Agent

To configure the device as a DHCP relay agent per the topology, do the following:

1. Configure the device as a DHCP relay agent:
  - a. Add VLAN 2 and VLAN 3. For more information, refer to "Adding a Static VLAN" (Page 321).
  - b. Assign IP address *192.168.0.8* to VLAN 1. For more information, refer to "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).
  - c. Change the PVID of port 1 to PVID 2, and change the PVID of port 2 to PVID 3. Refer to "Configuring a Switched Ethernet Port" (Page 276) for more information.
2. Configure a separate device as the DHCP Server. If the DHCP server being used is a RUGGEDCOM ROX II device, refer to "Example: Configuring the Device as a DHCP Server to Support a Relay Agent" (Page 267) for more information.

### Final Configuration Example

The following configuration reflects the topology:

```
# show running-config switch dhcp-relay-agent
dhcp-server-address 192.168.0.52
dhcp-client-ports lm4 1
!
dhcp-client-ports lm4 2
!
```

## 7.3 Managing the DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a method for centrally and consistently managing IP addresses and settings for clients, offering a variety of assignment methods. IP addresses can be assigned based on the Ethernet MAC address of a client either sequentially or by using port identification provided by a DHCP relay agent device.

The information that is assigned to addresses in DHCP is organized to deal with clients at the interface, subnet, pool, shared network, host-group and host levels.

RUGGEDCOM ROX II supports both IPv4 and IPv6 address assignments.

### 7.3.1 Viewing a List of Active Leases

RUGGEDCOM ROX II can generate a list of active leases. The list includes the start and end times, hardware Ethernet address, and client host name for each lease.

To view a list of active leases, do the following:

- Navigate to:
  - **For IPv4**  
the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv6**

If active leases have been configured, a list appears under **Active Leases**.

### 7.3.2 Configuring the DHCP Server

To configure the DHCP server, do the following:

---

#### Note

This procedure outlines the basic steps required to configure the device as a DHCP server. For a configuration example that includes a DHCP relay agent, refer to "Example: Configuring the Device as a DHCP Server to Support a Relay Agent" (Page 267).

---

1. [Optional] Configure a separate device as a DHCP relay agent. The relay agent may be a RUGGEDCOM ROX II device, a RUGGEDCOM ROS device, or a third party device with relay agent capabilities.  
If the relay agent being used is a RUGGEDCOM ROX II device, refer to "Example: Configuring the Device as a Relay Agent" (Page 232) for more information.
2. Enable the DHCP server. For more information, refer to "Enabling/Disabling the DHCP Server" (Page 235).
3. Add a DHCP listen interface. For more information, refer to "Adding a DHCP Listen Interface" (Page 242).
4. Assign an IP address to the listen interface. For more information, refer to "Adding a Subnet" (Page 246).
5. Create a shared network and enable Option82. For more information, refer to "Adding a Shared Network" (Page 244) and "Configuring Shared Network Options" (Page 244).
6. Create a subnet for each LAN that has DHCP clients. For more information about creating subnets, refer to "Adding a Subnet" (Page 246).
7. [Optional] If a dynamic IP address is needed for the relay agent, create a subnet for the DHCP relay agent. For more information about creating subnets, refer to "Adding a Subnet" (Page 246).
8. For each client subnet (excluding the subnet for the DHCP relay agent, if used), do the following:
  - a. Create one or more IP address pools to define a range of IP addresses for each client.  
For more information about IP address pools, refer to "Adding an Address Pool (IPv4)" (Page 255) or "Adding an Address Pool (IPv6)" (Page 257).  
For more information about IP ranges, refer to "Adding an IP Range (IPv4)" (Page 259) or "Adding an IP Range (IPv6)" (Page 260).
  - b. [Optional] Configure the option82 class on the relay agent, if used. For more information, refer to "Adding an Option 82 Class to an Address Pool" (Page 266).
9. [Optional] Add and configure hosts and host-groups. For more information, refer to "Adding a Host" (Page 252).

### 7.3.3 Enabling/Disabling the DHCP Server

To enable or disable the DHCP server, do the following:

1. Navigate to:
  - **For IPv4**  
the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv6**

- Configure the following parameter(s) as required:

- For IPv4, under DHCP Server:**

Parameter	Description
DHCP Server	Enables and disables the the DHCP server.

- For IPv6, under DHCPv6 Server:**

Parameter	Description
DHCPv6 Server	Enables and disables the DHCPv6 server.

- Commit the change.

### 7.3.4 Configuring DHCP Server Options

To configure options for the DHCP server, do the following:


#### Note

Options set at the subnet level override options set at the DHCP server level.

- Navigate to:
  - For IPv4**  
the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv4**
  - For IPv6**  
the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv6**
- Configure the following parameters as required:

Parameter	Description
Leased Configuration Default	<p><b>Synopsis:</b> An integer <b>Default:</b> 600</p> <p>The minimum leased time in seconds that the server offers to the clients.</p>
Leased Configuration Maximum	<p><b>Synopsis:</b> An integer <b>Default:</b> 7200</p> <p>The maximum leased time in seconds that the server offers to the clients.</p>

- Configure the following parameters as required:

 <b>NOTICE</b>
<p><b>For IPv4 only:</b></p> <p>If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the DHCP server. Because the DHCP</p>

server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK (negative acknowledgement or not acknowledged) message to disallow the lease. Enabling Option 82 disables the NAK message so the renewal request sent from the DHCP relay agent (which the DHCP server accepts, since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

Option 82 support should only be enabled if the DHCP server and clients are on the same subnet.

The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

DHCP relay support can also be enabled on individual subnets. For more information, refer to "Configuring Subnet Options" (Page 247).

Parameter	Description
Unknown Client	<b>Synopsis:</b> [ allow   deny   ignore ] The action to take for previously unregistered clients
Authorize Server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.
Option 82	Enables/disables the NAK of option 82 clients for this subnet.

4. [Optional] Configure additional client configuration options. For more information, refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 237) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 239).
5. Commit the changes.

## 7.3.5 Managing DHCP Client Configuration Options

Standard and custom options can be configured globally at the DHCP server level, or for specific shared networks, subnets, host groups or hosts. Options set at an individual level override options set at the global level.

### 7.3.5.1 Configuring Standard DHCP Client Configuration Options (IPv4)

Configuration options for DHCP clients can be configured globally or for an individual shared network, subnet, host group or host.



**Note**

Options set for individual shared networks, subnets, host groups or hosts override the options set at the global level.

To configure client options, do the following:

1. Navigate to **Layer 3 » DHCP Server » IPv4 » { path }**, where *path* is the path to and name of the desired shared network, subnet, host group or host.  
Select an entry, and then click the **Parameters** tab.
2. Alternatively, to access options at the global level, navigate to the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv4**.
3. Click **Client**.
4. Configure the following parameters as required:

Parameter	Description
Host Name	<b>Synopsis:</b> A string between 1 and 32 characters long The unique name to refer to the host within a DHCP configuration.
Subnet Mask	<b>Synopsis:</b> A string between 7 and 15 characters long Subnet mask
Default Route	<b>Synopsis:</b> A string between 7 and 15 characters long The default route that the server offers to the client when it issues the lease to the client.
Broadcast	<b>Synopsis:</b> A string between 7 and 15 characters long The broadcast address that the server offers to the client when it issues the lease to the client.
Domain	<b>Synopsis:</b> A string between 1 and 253 characters long The domain name that the server offers to the client when it issues the lease to the client.
DNS Server	<b>Synopsis:</b> A string between 7 and 31 characters long The domain name server that the server offers to the client when it issues the lease to the client.
Static Route	<b>Synopsis:</b> A string between 7 and 15 characters long The static route that the DHCP server offers to the client when it issues the lease to the client.
NIS Server	<b>Synopsis:</b> A string between 7 and 15 characters long The NIS server address that the DHCP server offers to the client when it issues the lease to the client.

Parameter	Description
NIS Domain	<b>Synopsis:</b> A string between 1 and 253 characters long The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.
NetBios Scope	<b>Synopsis:</b> A string between 1 and 256 characters long <b>Default:</b> netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
NetBios Server	<b>Synopsis:</b> A string between 1 and 256 characters long <b>Default:</b> 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

- [Optional] Add custom options. For more information, refer to "Adding a Custom DHCP Client Configuration Option" (Page 241).
- Commit the changes.

### 7.3.5.2 Configuring Standard DHCP Client Configuration Options (IPv6)

Configuration options for DHCP clients can be configured globally or for an individual shared network, subnet, host group or host.

#### Note

Options set for individual shared networks, subnets, host groups or hosts override the options set at the global level.

To configure client options, do the following:

- Navigate to **Layer 3 » DHCP Server » IPv6 » { path }**, where *path* is the path to and name of the desired shared network, subnet, host group or host.  
Select an entry, and then click the **Parameters** tab.
- Alternatively, to access options at the global level, navigate to the **Server Parameters** tab under **Layer 3 » DHCP Server » IPv6**.
- Click **Client**.
- Configure the following parameters as required:

Parameter	Description
Domain	<b>Synopsis:</b> A string between 1 and 253 characters long The domain name that the server offers to the client when it issues the lease to the client.

Parameter	Description
DNS Server	<b>Synopsis:</b> A string between 6 and 87 characters long  The domain name server that the server offers to the client when it issues the lease to the client.
Domain Search List	<b>Synopsis:</b> A string up to 773 characters long  The domain search list that the server offers to the client when it issues the lease to the client.
NIS Server	<b>Synopsis:</b> A string between 6 and 40 characters long  The NIS server address that the DHCPv6 server offers to the client when it issues the lease to the client.
NIS Domain	<b>Synopsis:</b> A string between 1 and 253 characters long  The NIS domain name that the DHCPv6 server offers to the client when it issues the lease to the client.

5. [Optional] Add custom options. For more information, refer to "Adding a Custom DHCP Client Configuration Option" (Page 241).
6. Commit the changes.

### 7.3.5.3 Viewing a List of Custom DHCP Client Configuration Options

1. To view a list of custom DHCP client configuration options set at the global level or for a specific shared network, subnet, host group or host, navigate to:
  - **For IPv4**  
*Layer 3 » DHCP Server » IPv4 » { path }*, where *path* is the path to and name of the desired shared network, subnet, host group or host.  
Select an entry, and then click the **Parameters** tab.
  - **For IPv6**  
*Layer 3 » DHCP Server » IPv6 » { path }*, where *path* is the path to and name of the desired shared network, subnet, host group or host.  
Select an entry, and then click the **Parameters** tab.

---

#### Note

Custom options at the **{ path }** level are only available for IPv4.

---

2. Alternatively, to view custom options at the global level, navigate to the **Server Parameters** tab under *Layer 3 » DHCP Server » [ IPv4 | IPv6 ]*.
3. Click **Custom**. If custom options have been configured, a list appears.

If custom configurations have not been configured, add custom configurations as needed. For more information, refer to "Adding a Custom DHCP Client Configuration Option" (Page 241).

### 7.3.5.4 Adding a Custom DHCP Client Configuration Option

To add a custom client option, do the following:

---

#### Note

The number of the option (defined by the Internet Assigned Numbers Authority or IANA) and its allowed value must be known before a custom option can be configured. For more information about available DHCP options, refer to [RFC 2132](http://tools.ietf.org/html/rfc2132) [<http://tools.ietf.org/html/rfc2132>].

---

1. Navigate to:
  - **For IPv4**  
*Layer 3 » DHCP Server » IPv4 » { path }*, where *path* is the path to and name of the desired shared network, subnet, host group or host.  
 Select an entry, and then click the **Custom** tab.
  - **For IPv6**  
*Layer 3 » DHCP Server » IPv6 » { path }*, where *path* is the path to and name of the desired shared network, subnet, host group or host.  
 Select an entry, and then click the **Custom** tab.

---

#### Note

Custom options at the **{ path }** level are only available for IPv4.

---

2. Alternatively, to view custom options at the global level, navigate to the **Server Parameters** tab under *Layer 3 » DHCP Server » [IPv4 | IPv6]*.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Number	<b>Synopsis:</b> An integer
Value	<b>Synopsis:</b> An integer The value of the custom option.

5. Click **OK** to add the custom option.
6. Commit the changes.

### 7.3.5.5 Deleting a Custom DHCP Client Configuration Option

To delete a custom client option, do the following:

1. Navigate to:
  - **For IPv4**  
*Layer 3 » DHCP Server » IPv4 » { path }*, where *path* is the path to and name of the desired shared network, subnet, host group or host.

Select an entry, and then click the **Custom** tab.

- **For IPv6**  
**Layer 3 » DHCP Server » IPv6 » { path }**, where *path* is the path to and name of the desired shared network, subnet, host group or host.

Select an entry, and then click the **Custom** tab.

---

**Note**

Custom options at the **{ path }** level are only available for IPv4.

---

2. Alternatively, to view custom options at the global level, navigate to the **Server Parameters** tab under **Layer 3 » DHCP Server » [IPv4 | IPv6]**.
3. Select the custom option to be deleted, and then click **Delete Entry**.
4. Commit the changes.

## 7.3.6 Managing DHCP Listen Interfaces

DHCP listen interfaces specify the IP interface to which the client sends a request.

### 7.3.6.1 Viewing a List of DHCP Listen Interfaces

To view a list of DHCP listen interfaces, navigate to:

- **For IPv4**  
the **Interface** tab under **Layer 3 » DHCP Server » IPv4**
- **For IPv6**  
the **Interface** tab under **Layer 3 » DHCP Server » IPv6**

If DHCP listen interfaces have been configured, a list appears.

If no DHCP listen interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a DHCP Listen Interface" (Page 242).

### 7.3.6.2 Adding a DHCP Listen Interface

To add a DHCP listen interface, do the following:

1. Navigate to:
  - **For IPv4**  
the **Interface** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Interface** tab under **Layer 3 » DHCP Server » IPv6**
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string

4. Click **OK** to create the new DHCP listen interface.
5. Commit the change.

### 7.3.6.3 Deleting a DHCP Listen Interface

To delete a DHCP listen interface, do the following:

1. Navigate to:
  - **For IPv4**  
the **Interface** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Interface** tab under **Layer 3 » DHCP Server » IPv6**
2. Select the DHCP listen interface to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 7.3.7 Managing Shared Networks

Shared networks are used when multiple subnets should be served by a single physical port. This applies both when using a DHCP relay agent connected to the port with additional subnets behind the relay agent, or when multiple virtual networks exist on one physical interface. Each subnet then gets its own subnet definition inside the shared network rather than at the top level. Shared networks contain subnets, groups and hosts.

### 7.3.7.1 Viewing a List of Shared Networks

To view a list of shared networks, navigate to:

- **For IPv4**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv4**
- **For IPv6**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv6**

If shared networks have been configured, a list appears.

If no shared networks have been configured, add shared networks as needed. For more information, refer to "Adding a Shared Network" (Page 244).

### 7.3.7.2 Adding a Shared Network

To add a shared network to the DHCP server, do the following:

1. Navigate to:
  - **For IPv4**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv6**
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The unique name to refer to the host within a DHCP configuration.</p>

4. Click **OK** to create the new shared network.
5. Configure options for the shared network. For more information, refer to "Configuring Shared Network Options" (Page 244).
6. Commit the change.

### 7.3.7.3 Configuring Shared Network Options

To configure options for a shared network on the DHCP server, do the following:

#### Note

Options set at the shared network level override options set at the DHCP server level.

1. Navigate to:
  - **For IPv4**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv6**
2. Select an entry, and then click the **Parameters** tab.
3. Configure the following parameters as required:

#### NOTICE

##### For IPv4 only:

If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the DHCP server. Because the DHCP server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK

(negative acknowledgment or not acknowledged) message to disallow the lease. Enabling Option 82 disables the NAK message so the renewal request sent from the DHCP relay agent (which the DHCP server accepts, since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

Option 82 support should only be enabled if the DHCP server and clients are on the same subnet.

The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

DHCP relay support can also be enabled on individual subnets. For more information, refer to "Configuring Subnet Options" (Page 247).

Parameter	Description
Leased Configuration Default	<b>Synopsis:</b> An integer <b>Default:</b> 600  The minimum leased time in seconds that the server offers to the clients.
Leased Configuration Maximum	<b>Synopsis:</b> An integer <b>Default:</b> 7200  The maximum leased time in seconds that the server offers to the clients.
Unknown Client	<b>Synopsis:</b> [ allow   deny   ignore ]  The action to take for previously unregistered clients
Authorize Server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.
Option 82	Enables/disables the NAK of option 82 clients for this subnet.

4. [Optional] Configure configuration options for DHCP clients at the shared network level. For more information, refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 237) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 239).
5. Commit the changes.

#### 7.3.7.4 Deleting a Shared Network

To delete a shared network, do the following:

1. Navigate to:
  - **For IPv4**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv4**



- **For IPv6**  
the **Shared Network List** tab under **Layer 3 » DHCP Server » IPv6**
2. Select a shared network then click **Delete Entry**.
  3. Commit the change.

## 7.3.8 Managing Subnets

Subnets control settings for each subnet that DHCP serves. A subnet can include a range of IP addresses to give clients. Subnets contain groups, pools and hosts. Only one subnet can contain dynamic IP address ranges without any access restrictions on any given physical port, since DHCP doesn't know which subnet a client should belong to when the request is received.

### 7.3.8.1 Viewing a List of Subnets

To view a list of subnets, navigate to:

- **For IPv4**  
the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**
- **For IPv6**  
the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv6**

If subnets have been configured, a list appears.

If no subnets have been configured, add subnets as needed. For more information, refer to "Adding a Subnet" (Page 246).

### 7.3.8.2 Adding a Subnet

To add a subnet to the DHCP server, do the following:

---

#### Note

At least one shared network must be available if two or more subnets are configured for the same interface. For information about configuring a shared network, refer to "Adding a Shared Network" (Page 244).

---

1. Navigate to:
  - **For IPv4**  
the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv6**
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 32 characters long  The unique name to refer to the host within a DHCP configuration.

4. Click **OK** to create the new subnet.
5. Configure the following parameter(s) as required:

Parameter	Description
Network IP	<b>Synopsis:</b> A string between 9 and 18 characters long  The network IP address for this subnet.
Shared Network	<b>Synopsis:</b> A string between 1 and 32 characters long  The shared-network that this host belongs to.
Network IP	<b>Synopsis:</b> A string between 4 and 43 characters long  The network IPv6 address for this subnet.
Shared Network	<b>Synopsis:</b> A string between 1 and 32 characters long  The shared-network that this host belongs to.

6. Configure the options for the subnet. For more information, refer to "Configuring Subnet Options" (Page 247).
7. Commit the change.

### 7.3.8.3 Configuring Subnet Options

To configure options for a subnet, do the following:

---

#### Note

Options set at the subnet level override options set at the DHCP server level.

---

1. Navigate to:
  - **For IPv4**  
the **Subnet Name List** tab under *Layer 3 » DHCP Server » IPv4*
  - **For IPv6**  
the **Subnet Name List** tab under *Layer 3 » DHCP Server » IPv6*
2. Select an entry, and then click the **Parameters** tab.
3. Configure the following parameters as required:

**⚠ NOTICE****For IPv4 only:**

If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the DHCP server. Because the DHCP server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK (negative acknowledgment or not acknowledged) message to disallow the lease. Enabling Option 82 disables the NAK message so the renewal request sent from the DHCP relay agent (which the DHCP server accepts, since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

Option 82 support should only be enabled if the DHCP server and clients are on the same subnet.

The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

DHCP relay support can also be enabled on individual subnets.

Parameter	Description
Leased Configuration Default	<b>Synopsis:</b> An integer <b>Default:</b> 600  The minimum leased time in seconds that the server offers to the clients.
Leased Configuration Maximum	<b>Synopsis:</b> An integer <b>Default:</b> 7200  The maximum leased time in seconds that the server offers to the clients.
Unknown Client	<b>Synopsis:</b> [ allow   deny   ignore ]  The action to take for previously unregistered clients
Option 82	Enables/disables the NAK of option 82 clients for this subnet.
Authorize Server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.

4. [Optional] Configure configuration options for DHCP clients at the subnet level. For more information, refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 237) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 239).

5. Configure one or more address pools to the subnet. For more information, refer to "Adding an Address Pool (IPv4)" (Page 255) or "Adding an Address Pool (IPv6)" (Page 257).
6. Configure one or more IP ranges to the subnet. For more information, refer to "Adding an IP Range (IPv4)" (Page 259) or "Adding an IP Range (IPv6)" (Page 260).
7. Commit the change.

#### 7.3.8.4 Deleting a Subnet

To delete a subnet, do the following:

1. Navigate to:
  - **For IPv4**  
the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv6**
2. Select the subnet to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 7.3.9 Managing Host Groups

Host-groups allow identical settings to be created for a group of hosts, making it easier to manage changes to the settings for all the hosts contained within the group. Host-groups contain hosts.

#### 7.3.9.1 Viewing a List of Host Groups

To view a list of host groups, navigate to:

- **For IPv4**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv4**
- **For IPv6**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv6**

If host groups have been configured, a list appears.

If no host groups have been configured, add host groups as needed. For more information, refer to "Adding a Host Group" (Page 250).

### 7.3.9.2 Adding a Host Group

To add a host group to the DHCP server, do the following:

1. Navigate to:
  - **For IPv4**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv6**
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 32 characters long The description of the host groups.

4. Click **OK** to create the new host group.
5. Configure the options for the host group. For more information, refer to "Configuring Host Group Options" (Page 250).
6. Commit the change.

### 7.3.9.3 Configuring Host Group Options

To configure options for a host group on the DHCP server, do the following:

---

#### Note

Options set at the host group level override options set at the DHCP server level.

---

1. Navigate to:
  - **For IPv4**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv6**
2. Select an entry, and then click the **Parameters** tab.
3. Configure the following parameters as required:

Parameter	Description
Leased Configuration Default	<b>Synopsis:</b> An integer <b>Default:</b> 600 The minimum leased time in seconds that the server offers to the clients.

Parameter	Description
Leased Configuration Maximum	<p><b>Synopsis:</b> An integer <b>Default:</b> 7200</p> <p>The maximum leased time in seconds that the server offers to the clients.</p>
Unknown Client	<p><b>Synopsis:</b> [ allow   deny   ignore ]</p> <p>The action to take for previously unregistered clients</p>
Shared Network	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The shared-network that this host belongs to.</p>
Subnet	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The subnet that this host belongs to.</p>

- **For IPv6**

Parameter	Description
Leased Configuration Default	<p><b>Synopsis:</b> An integer <b>Default:</b> 600</p> <p>The minimum leased time in seconds that the server offers to the clients.</p>
Leased Configuration Maximum	<p><b>Synopsis:</b> An integer <b>Default:</b> 7200</p> <p>The maximum leased time in seconds that the server offers to the clients.</p>
Unknown Client	<p><b>Synopsis:</b> [ allow   deny   ignore ]</p> <p>The action to take for previously unregistered clients</p>
Shared Network	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The shared-network that this host belongs to.</p>
Subnet6	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The subnet that this host belongs to.</p>

4. [Optional] Configure configuration options for DHCP clients at the host group level. For more information, refer to refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 237) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 239).
5. Commit the change.

#### 7.3.9.4 Deleting a Host Group

To delete a host group, do the following:

1. Navigate to:
  - **For IPv4**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Host Groups List** tab under **Layer 3 » DHCP Server » IPv6**
2. Select the host group to be deleted, and then click **Delete Entry**.
3. Commit the change.

#### 7.3.10 Managing DHCP Hosts

Host entries assign settings to a specific client based on its Ethernet MAC address.

##### 7.3.10.1 Viewing a List of Hosts

To view a list of hosts on the DHCP server, navigate to:

- **For IPv4**  
the **Hosts List** tab under **Layer 3 » DHCP Server » IPv4**
- **For IPv6**  
the **Hosts List** tab under **Layer 3 » DHCP Server » IPv6**

If hosts have been configured, a list appears.

If no hosts have been configured, add hosts as needed. For more information, refer to "Adding a Host" (Page 252).

##### 7.3.10.2 Adding a Host

To add a host to the DHCP server, do the following:

1. Navigate to:
  - **For IPv4**  
the **Hosts List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Hosts List** tab under **Layer 3 » DHCP Server » IPv6**
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The unique name to refer to the host within a DHCP configuration.</p>

4. Click **OK** to create the new host.
5. Configure options for the host. For more information, refer to "Configuring Host Options" (Page 253).
6. Commit the change.

### 7.3.10.3 Configuring Host Options

To configure options for a host on the DHCP server, do the following:

---

#### Note

Options set at the host level override options set at the DHCP server level.

---

1. Navigate to:
  - **For IPv4**  
the **Hosts List** tab under *Layer 3 » DHCP Server » IPv4*
  - **For IPv6**  
the **Hosts List** tab under *Layer 3 » DHCP Server » IPv6*
2. Select an entry, and then click the **Parameters** tab.
3. Configure the following parameters as required:

Parameter	Description
Type	<p><b>Synopsis:</b> [ fddi   token-ring   ethernet ]</p> <p><b>Default:</b> ethernet</p> <p>The type of network hardware used by the client, associated with the host entry.</p>
MAC	<p><b>Synopsis:</b> A string up to 17 characters long</p> <p>The physical network address of the client. Note that this corresponds to the hardware type; for example, the MAC address for the ethernet.</p>
Leased Configuration Default	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 600</p> <p>The minimum leased time in seconds that the server offers to the clients.</p>



Parameter	Description
Leased Configuration Maximum	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 7200</p> <p>The maximum leased time in seconds that the server offers to the clients.</p>

- **For IPv4**

Parameter	Description
Fixed IP	<p><b>Synopsis:</b> A string between 7 and 15 characters long</p> <p>The IP address that the server assigns to the matching client.</p>
Unknown Client	<p><b>Synopsis:</b> [ allow   deny   ignore ]</p> <p>The action to take for previously unregistered clients</p>
Shared Network	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The shared-network that this host belongs to.</p>
Subnet	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The subnet that this host belongs to.</p>
Host Groups	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The host groups that this host belongs to.</p>

- **For IPv6**

Parameter	Description
Fixed IPv6	<p><b>Synopsis:</b> A string between 6 and 40 characters long</p> <p>The IPv6 address that the server assigns to the matching client.</p>
Fixed Prefix	<p><b>Synopsis:</b> A string between 4 and 43 characters long</p> <p>The IPv6 prefix delegation that the server assigns to the matching client.</p>
Unknown Client	<p><b>Synopsis:</b> [ allow   deny   ignore ]</p> <p>The action to take for previously unregistered clients</p>
Shared network	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The shared-network that this host belongs to.</p>
Subnet6	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The subnet that this host belongs to.</p>
Host Groups	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The host groups that this host belongs to.</p>

4. [Optional] Configure configuration options for DHCP clients at the host level. For more information, refer to refer to "Configuring Standard DHCP Client

Configuration Options (IPv4)" (Page 237) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 239).

5. Commit the changes.

#### 7.3.10.4 Deleting Hosts

To delete a host, do the following:

1. Navigate to:
  - **For IPv4**  
the **Hosts List** tab under **Layer 3 » DHCP Server » IPv4**
  - **For IPv6**  
the **Hosts List** tab under **Layer 3 » DHCP Server » IPv6**
2. Select the host to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 7.3.11 Managing Address Pools (IPv4)

Address pools define a range of IP addresses that can be assigned to DHCP clients belonging to the same subnet.

#### 7.3.11.1 Viewing a List of Address Pools (IPv4)

1. To view a list of address pools configured for a DHCP subnet, navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
2. Select an entry, and then click the **IP Pool** tab.

If pools have been configured, a list appears.

If no IP pools have been configured, add pools as needed. For more information, refer to "Adding an Address Pool (IPv4)" (Page 255).

#### 7.3.11.2 Adding an Address Pool (IPv4)

To add an address pool to a DHCP subnet, do the following:

1. Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
2. Select an entry, and then click the **IP Pool** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string up to 32 characters long Describes the IP pool.

- Click **OK** to create the IP pool.
- Click **Pool Parameters**, and then configure the following parameter(s) as required:

Parameter	Description
Leased Configuration Default	<b>Synopsis:</b> An integer <b>Default:</b> 600 The minimum leased time in seconds that the server offers to the clients.
Leased Configuration Maximum	<b>Synopsis:</b> An integer <b>Default:</b> 7200 The maximum leased time in seconds that the server offers to the clients.
Unknown Client	<b>Synopsis:</b> [ allow   deny   ignore ] The action to take for previously unregistered clients
Failover Peer	<b>Synopsis:</b> A string between 7 and 15 characters long The IP address of a DHCP peer server if a failover pool is created.

- Add one or more IP ranges to the pool. For more information, refer to "Adding an IP Range (IPv4)" (Page 259).
- Add one or more Option82 classes to the pool. For more information, refer to "Adding an Option 82 Class to an Address Pool" (Page 266).
- Commit the changes.

### 7.3.11.3 Deleting an Address Pool (IPv4)

To delete an address pool, do the following:

- Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
- Select an entry, and then click the **IP Pool** tab.
- Select the pool to be deleted, and then click **Delete Entry**.
- Commit the change.

## 7.3.12 Managing Address Pools (IPv6)

Address pools define a range of IP addresses that can be assigned to DHCP clients belonging to the same subnet.

### 7.3.12.1 Viewing a List of Address Pools (IPv6)

1. To view a list of address pools configured for a DHCP subnet, navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**.
2. Select an entry, and then click the **IP Pool6** tab.

If pools have been configured, a list appears.

If no IP pools have been configured, add pools as needed. For more information, refer to "Adding an Address Pool (IPv6)" (Page 257).

### 7.3.12.2 Adding an Address Pool (IPv6)

To add an address pool to a DHCP subnet, do the following:

1. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**.
2. Select an entry, and then click the **IP Pool6** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string between 1 and 32 characters long Describes the IPv6 pool.

5. Click **OK** to create the IP pool.
6. Click **Pool Parameters**, and then configure the following parameter(s) as required:

Parameter	Description
Leased Configuration default	<b>Synopsis:</b> An integer <b>Default:</b> 600 The minimum leased time in seconds that the server offers to the clients.
Leased Configuration Maximum	<b>Synopsis:</b> An integer <b>Default:</b> 7200 The maximum leased time in seconds that the server offers to the clients.

Parameter	Description
Unknown Client	<p><b>Synopsis:</b> [ allow   deny   ignore ]</p> <p>The action to take for previously unregistered clients</p>

7. [Optional] Add one or more IP ranges to the pool. For more information, refer to "Adding an IP Range (IPv6)" (Page 260).
8. [Optional] Add one or more subnets to the pool. For more information, refer to "Adding a IPv6 Subnet" (Page 265).
9. [Optional] Add one or more temporary subnets to the pool. For more information, refer to "Adding a Temporary Subnet" (Page 263).
10. [Optional] Add one or more prefixes to the pool. For more information, refer to "Adding an IPv6 Prefix" (Page 262).
11. Commit the changes.

### 7.3.12.3 Deleting an Address Pool (IPv6)

To delete an address pool, do the following:

1. Navigate to the **Subnet6 Name List** tab under *Layer 3 » DHCP Server » IPv6*.
2. Select an entry, and then click the **IP Pool6** tab.
3. Select the pool to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 7.3.13 Managing IP Ranges (IPv4)

An IP range represents the range of IP addresses the DHCP server can assign to clients. IP addresses outside the set range are reserved for statically addressed clients.

An IP range can be configured for a DHCP subnet and/or its associated address pool(s).

### 7.3.13.1 Viewing a List of IP Ranges (IPv4)

To view a list of IP ranges configured for a DHCP subnet or one of its associated address pools, do the following:

1. Make sure a DHCP subnet or one of its associated address pools have been configured.
2. Navigate to the **Subnet Name List** tab under *Layer 3 » DHCP Server » IPv4*.
3. Select the **IP Range** tab.
  - For a DHCP subnet, click the **Parameters** tab, and then click **IP Range**.

- For an address pool, click the **IP Pool** tab, then **Pool Parameters**, and then click **IP Range**.

If no IP ranges have been configured, add ranges as needed. For more information, refer to "Adding an IP Range (IPv4)" (Page 259) or "Adding an IP Range (IPv6)" (Page 260).

### 7.3.13.2 Adding an IP Range (IPv4)

To add an IP range to a DHCP subnet or one of its associated address pools, do the following:

1. Make sure a DHCP subnet or one of its associated address pools have been configured.
2. Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
3. Select the desired DHCP subnet or address pool.
4. Select the **IP Range** tab.
  - For a DHCP subnet, click the **Parameters** tab, and then click **IP Range**.
  - For an address pool, click the **IP Pool** tab, then **Pool Parameters**, and then click **IP Range**.
5. Click **Add Entry**.
6. Configure the following parameter(s) as required:

Parameter	Description
Start	<b>Synopsis:</b> A string between 7 and 15 characters long The starting IP address pool that the server uses to offer to the client.

7. Click **OK** to create the IP range.
8. Configure the following parameter(s) as required:

Parameter	Description
End	<b>Synopsis:</b> A string between 7 and 15 characters long The ending IP address pool that the server uses to offer to the client.

9. Commit the changes.

### 7.3.13.3 Deleting an IP Range (IPv4)

To delete an IP range from a DHCP subnet or one of its associated address pools, do the following:

1. Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.

2. Select the desired DHCP subnet or address pool.
3. For a DHCP subnet, click the **Parameters** tab, and then click **IP Range**.
4. For an address pool, click the **IP Pool** tab, then **Pool Parameters**, and then click **IP Range**.
5. Select the IP range to be deleted, and then click **Delete Entry**.
6. Commit the change.

### 7.3.14 Managing IP Ranges (IPv6)

An IP range represents the range of IP addresses the DHCP server can assign to clients. IP addresses outside the set range are reserved for statically addressed clients.

An IP range can be configured for a DHCP subnet and/or its associated address pool(s).

#### 7.3.14.1 Viewing a List of IP Ranges (IPv6)

To view a list of IP ranges configured for a DHCP subnet or one of its associated address pools, do the following:

1. Make sure a DHCP subnet or one of its associated address pools have been configured.
2. Navigate to the **Subnet6 Name List** tab under *Layer 3 » DHCP Server » IPv6*.
3. Select the **IP Range6** tab.
  - For a DHCP subnet, click the **Parameters** tab, and then click **IP Range6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **IP Range6**.

If no IP ranges have been configured, add ranges as needed. For more information, refer to "Adding an IP Range (IPv6)" (Page 260).

#### 7.3.14.2 Adding an IP Range (IPv6)

To add an IP range to a DHCP subnet or one of its associated address pools, do the following:

1. Make sure a DHCP subnet or one of its associated address pools have been configured.
2. Navigate to the **Subnet6 Name List** tab under *Layer 3 » DHCP Server » IPv6*.
3. Select the desired DHCP subnet or address pool.
4. Select the **IP Range6** tab.
  - For a DHCP subnet, click the **Parameters** tab, and then click **IP Range6**.

- For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **IP Range6**.
5. Click **Add Entry**.
  6. Configure the following parameter(s) as required:

Parameter	Description
Start	<b>Synopsis:</b> A string between 6 and 40 characters long The starting IPv6 address pool that the server uses to offer to the client.

7. Click **OK** to create the IP range.
8. Configure the following parameter(s) as required:

Parameter	Description
End	<b>Synopsis:</b> A string between 6 and 40 characters long The ending IPv6 address pool that the server uses to offer to the client.

9. Commit the changes.

### 7.3.14.3 Deleting an IP Range (IPv6)

To delete an IP range from a DHCP subnet or one of its associated address pools, do the following:

1. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**.
2. Select the desired DHCP subnet or address pool.
3. Select the **IP Range6** tab.
  - For a DHCP subnet, click the **Parameters** tab, and then click **IP Range6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **IP Range6**.
4. Select the IP range to be deleted, and then click **Delete Entry**.
5. Commit the change.

## 7.3.15 Managing IPv6 Prefixes

One or more optional IPv6 prefix can be defined for the server to offer to the client.

A *prefix6* delegation includes the IPv6 subnetwork, along with the prefix length in bits. The subnetwork value used should be within the subnetwork value of the enclosing subnet6 declaration.



### 7.3.15.1 Viewing a List of IPv6 Prefixes

To view a list of prefixes, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Prefix6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Prefix6**.

If no prefixes have been configured, add ranges as needed. For more information, refer to "Adding an IPv6 Prefix" (Page 262).

### 7.3.15.2 Adding an IPv6 Prefix

To add a prefix, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Prefix6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Prefix6**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Start	<b>Synopsis:</b> A string between 6 and 40 characters long The starting IPv6 prefix delegation that the server uses to offer to the client.

5. Click **OK** to create the prefix.
6. Configure the following parameter(s) as required:

Parameter	Description
End	<b>Synopsis:</b> A string between 6 and 40 characters long The ending IPv6 prefix delegation that the server uses to offer to the client.
Bits	<b>Synopsis:</b> An integer between 1 and 64 Prefix delegations of bits length that are offered to the client.

7. Commit the changes.

### 7.3.15.3 Deleting an IPv6 Prefix

To delete a prefix, do the following:

1. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Prefix6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Prefix6**.
2. Select the prefix to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 7.3.16 Managing Temporary Subnets

One or more optional IPv6 subnets with temporary addresses can be defined for the server to offer to the client.

### 7.3.16.1 Viewing a List of Temporary Subnets

To view a list of temporary subnets, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Temporary Subnet6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Temporary Subnet6**.

If no prefixes have been configured, add ranges as needed. For more information, refer to "Adding an IPv6 Prefix" (Page 262).

### 7.3.16.2 Adding a Temporary Subnet

To add a temporary subnet, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Temporary Subnet6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Temporary Subnet6**.
3. Click **Add Entry**.

4. Configure the following parameter(s) as required:

Parameter	Description
Subnet Number	<p><b>Synopsis:</b> A string between 4 and 43 characters long</p> <p>The IPv6 subnet with temporary addresses that the server uses to offer to the client.</p>

5. Click **OK** to create the temporary subnet.
6. Commit the change.

### 7.3.16.3 Deleting a Temporary Subnet

To delete a prefix, do the following:

1. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Temporary Subnet6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Temporary Subnet6**.
2. Select the temporary subnet to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 7.3.17 Managing IPv6 Subnets

One or more optional IPv6 subnets can be defined for the server to offer to the client.

### 7.3.17.1 Viewing a List of IPv6 Subnets

To view a list of IPv6 subnets, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Subnet6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Subnet6**.

If no prefixes have been configured, add ranges as needed. For more information, refer to "Adding an IPv6 Prefix" (Page 262).

### 7.3.17.2 Adding a IPv6 Subnet

To add a IPv6 subnet, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Subnet6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Subnet6**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Subnet Number	<b>Synopsis:</b> A string between 4 and 43 characters long The IPv6 subnet that the server uses to offer to the client.

5. Click **OK** to create the IPv6 subnet.
6. Commit the change.

### 7.3.17.3 Deleting an IPv6 Subnet

To delete an IPv6 subnet, do the following:

1. Make sure a DHCP subnet has been configured.
2. Navigate to the **Subnet6 Name List** tab under **Layer 3 » DHCP Server » IPv6**, and then select a subnet.
  - For a DHCP subnet, click the **Parameters** tab, and then click **Subnet6**.
  - For an address pool, click the **IP Pool6** tab, then **Pool Parameters**, and then click **Subnet6**.
3. Select the prefix to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 7.3.18 Managing Option 82 Classes for Address Pools

Option 82, or the DHCP relay agent information option, helps protect the DHCP server from IP address spoofing and DHCP IP starvation attacks by providing information about the network source of IP address requests. When a DHCP client issues an IP address request, a DHCP relay agent adds Option 82 information to the packet header for the request. The relay agent then forwards the request to the DHCP server for consideration. If the DHCP server determines the request came from an untrusted source, the request is rejected.

The DHCP server must be configured to accept Option 82 information if it is to determine the trustworthiness of the network interface used by a DHCP client. This can be done at the global level or for individual subnets.

---

#### Note

For more information about enabling the DHCP server to accept Option 82 information, refer to either "Configuring DHCP Server Options" (Page 236) or "Configuring Subnet Options" (Page 247).

---

Once Option 82 is enabled, sub-option components (or classes) must be defined for each address pool that includes DHCP clients that will send Option 82 information. This section describes how to manage the sub-option components for address pools.

### 7.3.18.1 Viewing a List of Option 82 Classes for Address Pools

To view a list of Option 82 classes configured for an address pool, do the following:

1. Make sure an address pools has been configured.
2. Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
3. Click the **IP Pool** tab, then **Pool Parameters**, and then click **Option 82**.

If no Option 82 classes have been configured, add classes as needed. For more information, refer to "Adding an Option 82 Class to an Address Pool" (Page 266).

### 7.3.18.2 Adding an Option 82 Class to an Address Pool

To add an Option 82 class to an address pool, do the following:

1. Make sure an address pools has been configured.
2. Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
3. Select the desired address pool.
4. Click the **IP Pool** tab, then **Pool Parameters**, and then click **Option 82**.
5. Click **Add Entry**.
6. Configure the following parameter(s) as required:

Parameter	Description
Class Name	<b>Synopsis:</b> A string up to 32 characters long The class name of option 82.

7. Click **OK** to create the class.
8. Configure the following parameter(s) as required:

## 7.3.19 Example: Configuring the Device as a DHCP Server to Support a Relay Agent

**Note**

The format for the **Circuit ID** value is `00:00:00:{vlan}:{slot}:{port}`. If the remote host is connected to LM3/1 on VLAN 1, the ID would be `00:00:00:01:03:01`. The Circuit ID uses hexadecimal values.

Parameter	Description
Remote ID	<b>Synopsis:</b> A string up to 17 characters long Specifies the information relating to the remote host end of the circuit.
Circuit ID	<b>Synopsis:</b> A string up to 17 characters long Specifies the local information to which circuit the request came in on (ie. 00:02:03:02)

9. Commit the changes.

### 7.3.18.3 Deleting an Option 82 Class From an Address Pool

To delete an Option 82 class from an address pool, do the following:

1. Navigate to the **Subnet Name List** tab under **Layer 3 » DHCP Server » IPv4**.
2. Select the desired address pool.
3. Click the **IP Pool** tab, then **Pool Parameters**, and then click **Option 82**.
4. Select the class to be deleted, and then click **Delete Entry**.
5. Commit the change.

### 7.3.19 Example: Configuring the Device as a DHCP Server to Support a Relay Agent

This example demonstrates how to configure the device as a DHCP server, with a relay agent, without hosts or host groups.

The following topology depicts a scenario where two clients on separate LANs require IP addresses on different subnets from a DHCP server. Each client connects to the DHCP relay agent using different VLANs. The DHCP relay agent manages the requests and responses between the clients and the DHCP server.

 **NOTICE**

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

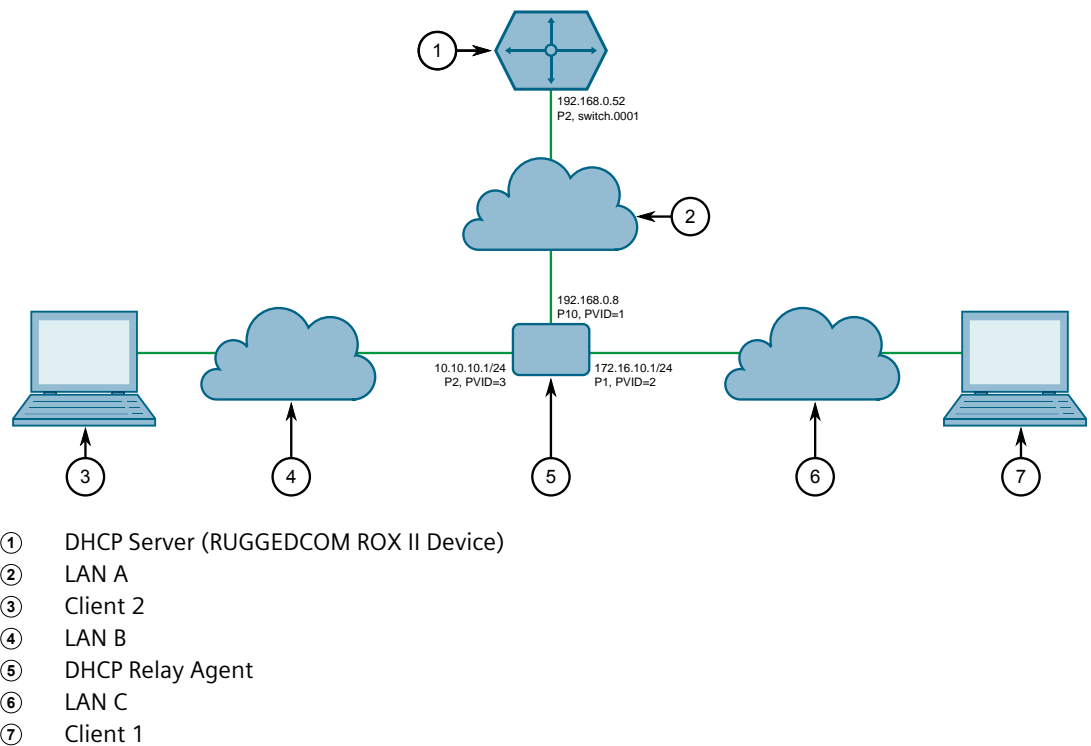


Figure 7.2 Topology – Device as a DHCP Server

To configure the device per the topology, do the following:

1. Configure a separate device as the DHCP relay agent:

---

**Note**

The relay agent may be a RUGGEDCOM ROX II device, a RUGGEDCOM ROS device, or a third party device with relay agent capabilities.

---

- a. Add and configure VLAN 2 and VLAN 3.
- b. Assign IP address *192.168.0.8* to VLAN 1.
- c. Change the PVID of port 1 to PVID 2.
- d. Change the PVID of port 2 to PVID 3.

If the relay agent being used is a RUGGEDCOM ROX II device, refer to "Example: Configuring the Device as a Relay Agent" (Page 232) for more information.

2. Enable the DHCP server. For more information, refer to "Enabling/Disabling the DHCP Server" (Page 235).
3. Add the management interface (switch.0001) as a DHCP listen interface. For more information, refer to "Adding a DHCP Listen Interface" (Page 242).
4. Assign IP address *192.168.0.52* to switch.0001 on the DHCP server. For more information, refer to "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).

## 7.3.19 Example: Configuring the Device as a DHCP Server to Support a Relay Agent

5. Create a shared network named *LAN.10-LAN.172* and enable Option82. For more information, refer to "Configuring Shared Network Options" (Page 244).
6. Under the subnet for the DHCP Client, create the following 3 subnets:

Name	Network IP	Shared Network
MainSub	192.168.0.0/24	LAN.10-LAN.172
LAN_A-172	172.16.10.0/24	LAN.10-LAN.172
LAN_B-10	10.10.10.0/24	LAN.10-LAN.172

For more information about creating subnets, refer to "Adding a Subnet" (Page 246).

7. [Optional] For the LAN A-172 subnet, configure *172.16.10.1* as a default route for clients. For more information, refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 237).
8. Create an address pool for the LAN A-172 subnet and configure the IP range for the address pool with the following parameters:

Pool Name	Starting Address	Ending Address
LAN-A_VLAN2	172.16.10.10	172.16.10.200

For more information, refer to "Adding an Address Pool (IPv4)" (Page 255) or "Adding an Address Pool (IPv6)" (Page 257).

9. Configure the following option82 class for the LAN-A\_VLAN2 pool:

Class Name	Remote ID	Circuit ID
LAN-A_Option	00:0a:dc:00:00:00	00:02:00:01

The Remote ID represents the MAC address of the DHCP relay agent. In the Circuit ID, *00:02* denotes the VLAN ID and *00:01* represents the line module (if applicable) and the port number of the DHCP relay agent where Client 1 is connected.

For more information, refer to "Adding an Option 82 Class to an Address Pool" (Page 266).

10. [Optional] For the LAN B-10 subnet, configure *10.10.10.1* as a default route for clients. For more information, refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 237).
11. Create an address pool for the LAN B-10 subnet and configure the IP range for the address pool with the following parameters:

Pool Name	Starting Address	Ending Address
LAN-B_VLAN3	10.10.10.10	10.10.10.200

For more information, refer to "Adding an Address Pool (IPv4)" (Page 255) or "Adding an Address Pool (IPv6)" (Page 257).

12. Configure the following option82 class for LAN-B\_VLAN3 pool:

Class Name	Remote ID	Circuit ID
LAN-B_Option	00:0a:dc:00:00:00	00:03:00:02



The Remote ID represents the MAC address of the DHCP relay agent, *00:03* denotes the VLAN ID and *00:02* represents the line module (if applicable) and the port number of the DHCP relay agent where Client 2 is connected.

For more information, refer to "Adding an Option 82 Class to an Address Pool" (Page 266).

### Final Configuration Example

The following configuration reflects the topology:

```
#show running-config services dhcpserver
enabled
interface switch.0001
!
options
  client
    no hostname
    no subnetmask
no default-route
no broadcast
no domain
no dns-server
no static-route
no nis server
no nis domain
!
!
shared-network LAN.10-LAN.172
options option82
options client
  no hostname
  no subnetmask
  no default-route
  no broadcast
  no domain
  no dns-server
  no static-route
  no nis server
  no nis domain
!
!
subnet-name "LAN A-172"
network-ip 172.16.10.0/24
shared-network LAN.10-LAN.172
options
  no unknown-client
  ippool LAN-A_VLAN2
  no unknown-client
  iprange 172.16.10.10
  end 172.16.10.200
!
  option82 LAN-A_Option
    remote-id 00:0a:dc:00:00:00
    circuit-id 00:02:00:01
!
!
client
  no hostname`
  no subnetmask
  default-route 172.16.10.1
  no broadcast
no domain
  no dns-server
```

```
no static-route
no nis server
no nis domain
!
!
!
subnet-name "LAN B-10"
network-ip 10.10.10.0/24
shared-network LAN.10-LAN.172
options
no unknown-client
ippool LAN-B_VLAN3
no unknown-client
iprange 10.10.10.10
end 10.10.10.200
!
option82 LAN-B_Option
remote-id 00:0a:dc:00:00:00
circuit-id 00:03:00:02
!
!
client
no hostname
no subnetmask
default-route 10.10.10.1
no broadcast
no domain
no dns-server
no static-route
no nis server
no nis domain
!
!
!
subnet-name mainSub
network-ip 192.168.0.0/24
shared-network LAN.10-LAN.172
options
no unknown-client
client
no hostname
no subnetmask
no default-route
no broadcast
no domain
no dns-server
no static-route
no nis server
no nis domain
```

## 7.4 Managing Static DNS

This section describes how to reserve a static or fixed IP address for the device. While it is more common to obtain a random address from a *dynamic* DNS server, obtaining a fixed address from a static DNS server may be required to connect to Virtual Private Networks (VPNs) or other remote access services that only trust specific IP addresses.

## 7.4.1 Managing Domain Names

The DNS service can be configured to use one or more domain names when querying a domain name server. The list of domain names can include the domain in which the router is a member of, and other domains that may be used to search for an unqualified host name (i.e. as though it were local).

### 7.4.1.1 Viewing a List of Domain Names

To view a list of domain names, navigate to the **DNS** tab under **Administration » DNS**, and then click **Search**. If domain names have been configured, a list appears.

If no domain names have been configured, add names as needed. For more information, refer to "Adding a Domain Name" (Page 272).

### 7.4.1.2 Adding a Domain Name

To add a domain name, do the following:

1. Navigate to the **DNS** tab under **Administration » DNS**, and then click **Search**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Domain	<b>Synopsis:</b> A string between 1 and 253 characters long

4. Click **OK** to create the domain name.
5. Commit the change.

### 7.4.1.3 Deleting a Domain Name

To delete a domain name, do the following:

1. Navigate to the **DNS** tab under **Administration » DNS**, and then click **Search**.
2. Select the domain name to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 7.4.2 Managing Domain Name Servers

A hierarchical list of domain name servers can be configured for the DNS service. RUGGEDCOM ROX II will contact each server in the order they are listed when domain names require resolution.

### 7.4.2.1 Viewing a List of Domain Name Servers

To view a list of domain name servers, navigate to the **DNS** tab under **Administration » DNS**, and then click **Server**. If domain name servers have been configured, a list appears.

If no domain name servers have been configured, add servers as needed. For more information, refer to "Adding a Domain Name Server" (Page 273).

### 7.4.2.2 Adding a Domain Name Server

To add a domain name server, do the following:

1. Navigate to the **DNS** tab under **Administration » DNS**, and then click **Server**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Address	<b>Synopsis:</b> A string

4. Click **OK** to create the domain name server.
5. Commit the change.

### 7.4.2.3 Deleting a Domain Name Server

To delete a domain name server, do the following:

1. Navigate to the **DNS** tab under **Administration » DNS**, and then click **Server**.
2. Select the domain name server to be deleted and then click **Delete Entry**.
3. Commit the change.



## Layer 2

This chapter describes the Layer 2, or Data Link Layer (DLL), features of RUGGEDCOM ROX II.

### 8.1 Configuring Link Detection

Link detection provides protection against faulty end devices that are generating an improper link integrity signal. When a faulty end device or mismatched fiber port is connected to the unit, a large number of continuous link state changes could be reported over a short period of time. The high number of bogus link state changes could render the system unresponsive as most, if not all, of the system resources are used to process the link state changes. This could in turn cause a serious network problem that prevents the Rapid Spanning Tree Protocol (RSTP) process from running, and thus allowing a network loop to form.

To configure link detection, do the following:

1. Navigate to the **Link Detection** tab under **Layer 2**.
2. Configure the following parameters as needed:

Parameter	Description
Fast Link Detection	<p><b>Synopsis:</b> [ on   off   portguard ]</p> <p><b>Default:</b> portguard</p> <p>The state of fast link detection.</p> <p>Options include:</p> <ul style="list-style-type: none"> <li>• <b>portguard</b> (recommended): Enables fast link detection with Port Guard. In this mode, an extended period (~2 minutes) of excessive link state changes reported by a port will prompt the Port Guard feature to disable fast link detection on that port and raise an alarm. By disabling fast link detection on the port, excessive link state changes can no longer consume a substantial amount of system resources. However, if fast link detection is disabled, the port will require more time to detect a link failure. This may result in a longer network recovery time of up to 2 seconds. After Port Guard disables fast link detection on a particular port, fast link detection can be reenabled by clearing the alarm.</li> <li>• <b>on:</b> Enables fast link detection without Port Guard. In certain special cases, where prolonged excessive link state changes constitute a legitimate link operation, using this setting can prevent Port Guard from disabling fast link detection on the port in question. If excessive link state changes persist for more than 2 minutes, an alarm will be</li> </ul>

Parameter	Description
	<p>generated to warn the user about the observed bouncing link. If the condition of the excessive link state changes is resolved later on, the alarm will be cleared automatically. Since this option does not disable fast link detection, a persistent bouncing link could continue to affect the system in terms of response time. This setting should be used with caution.</p> <ul style="list-style-type: none"> <li><b>off:</b> Disables fast link detection. The switch will need a longer time to detect a link failure. This will result in longer network recovery times of up to 2 seconds.</li> </ul>
Link Detection Time (ms)	<p><b>Synopsis:</b> An integer between 100 and 1000 <b>Default:</b> 100</p> <p>The time that the link has to continuously stay up before the 'link up' decision is made by the device. The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing event, e.g. when a cable is shaking while being plugged-in or unplugged.</p>

3. Commit the changes.

## 8.2 Managing Switched Ethernet Ports

This section describes how to configure and manage switched Ethernet ports.

### 8.2.1 Viewing a List of Switched Ethernet Ports

To view a list of switched Ethernet ports configured on the device, navigate to the **Port Parameters** tab under **Interface » Switch Ports**.

### 8.2.2 Configuring a Switched Ethernet Port

To configure a switched Ethernet port, do the following:

1. Configure the port parameters:
  - a. Navigate to the **Port Parameters** tab under **Interface » Switch Ports**.

---

#### Note

For information about configuring port rate limiting, refer to "Configuring Port Rate Limiting" (Page 760).

---

#### Note

For information about configuring RMON threshold alerts, refer to "Configuring RMON Threshold Alerts" (Page 281).

---

- b. Select a switched Ethernet port.
- c. Configure the following parameter(s) as required:

**⚠ NOTICE**

**Security hazard – risk of unauthorized access and/or exploitation**

Switched Ethernet ports are enabled by default. It is recommended that ports that are not in use be disabled. Unused ports, if not configured properly, could potentially be used to gain access to the network behind the device.

**⚠ NOTICE**

**Configuration hazard – risk of data corruption**

Changing a switched Ethernet port from switchport mode to dedicated routing mode will automatically change any configuration elements that depended on it and potentially invalidate parts of the device configuration. For example, if a switched Ethernet port is a trunk port, changing it to dedicated routing mode will automatically remove it from the trunk and, therefore, make the trunk invalid. A trunk must consist of two trunk ports.

**Note**

Switched Ethernet ports in dedicated routing port mode cannot be trunk ports.

**Note**

The configuration for a switched Ethernet port in switchport mode can be restored when it is removed from a trunk. However, the configuration cannot be restored if the port is in dedicated routing mode.

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Provides the option to enable or disable this interface. When unchecked(i.e disabled), the interface will prevent all frames from being sent and received on that interface.</p>
AutoN	<p><b>Synopsis:</b> [ on   off ]</p> <p>Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results.</p>
Speed	<p><b>Synopsis:</b> [ auto   1.5M   2.4M   10M   100M   1G   10G   1.776M   3.072M   7.2M   1.2K   2.4K   9.6K   19.2K   38.4K   57.6K   115.2K   230.4K   4.8K   76.8K ]</p> <p>Speed (in megabits-per-second or gigabits-per-second). If auto-negotiation is enabled, this is the speed capability</p>



Parameter	Description
	advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes.
Duplex	<b>Synopsis:</b> [ auto   half   full ]  If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes.
Link Alarms	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true  Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
Switchport	<b>Synopsis:</b> [ true   false ]  Sets the physical port into either switched mode or a dedicated routing mode.
Flow Control	Flow control is useful for preventing frame loss during times of severe network traffic
On Demand	Bring up this interface on-demand only
IP Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static  Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
IPv6 Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static  Whether the IPv6 address is static or dynamically assigned via DHCPv6. Option DYNAMIC is a common case of a dynamically assigned IPv6 address. This must be static for non-management interfaces.
Proxy ARP	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
MTU	<b>Synopsis:</b> An integer between 68 and 9216 <b>Default:</b> 1500  Maximum transmission unit (largest packet size allowed for this interface).

Parameter	Description
Alias	<b>Synopsis:</b> A string up to 64 characters long The SNMP alias name of the interface

2. Configure the LLDP parameters:
  - a. Navigate to the **Interface LLDP Parameters** tab under **Layer 2 » Net Discovery**, and then click **Switchport LLDP Parameters**.
  - b. Select a switched Ethernet port.
  - c. Configure the following parameter(s) as required:

Parameter	Description
Admin Status	<b>Synopsis:</b> [ tx-only   rx-only   rx-tx   no-lldp ] <b>Default:</b> rx-tx <ul style="list-style-type: none"> <li>• no-lldp : The local LLDP agent can neither transmit nor receive LLDP frames.</li> <li>• rxTx : The local LLDP agent can both transmit and receive LLDP frames through the port.</li> <li>• txOnly : The local LLDP agent can only transmit LLDP frames.</li> <li>• rxOnly : The local LLDP agent can only receive LLDP frames.</li> </ul>
Notify	Disabling notifications will prevent sending notifications and generating alarms for a particular interface from the LLDP agent.

3. Configure the multicast filtering parameters:
  - a. Navigate to the **GMRP Parameters** tab under **Layer 2 » Multicast Filtering**, and then click **Ports**.
  - b. Select a switched Ethernet port.
  - c. Configure the following parameter(s) as required:

Parameter	Description
GMRP	<b>Synopsis:</b> [ advertise_only   learn_advertise ] GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: <ul style="list-style-type: none"> <li>• DISABLED : the port is not capable of any GMRP processing.</li> <li>• ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.</li> <li>• ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.</li> </ul>

4. Configure the CoS parameters:

- a. Navigate to the **CoS Parameters** tab under **Layer 2 » CoS Mapping**, and then click **Ports**.
- b. Select a switched Ethernet port.
- c. Configure the following parameter(s) as required:

Parameter	Description
Default Priority	<p><b>Synopsis:</b> An integer between 0 and 7</p> <p><b>Default:</b> 0</p> <p>The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. the priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).</p>
Inspect ToS	<p>Enables or disables parsing of the Type-of-Service (ToS) field in the IP header of the received frames to determine what Class of Service (CoS) they should be assigned. When ToS parsing is enabled the switch will use the differentiated services bits in the TOS field.</p>

5. Configure the VLAN parameters:
  - a. Navigate to the **Port Parameters** tab under **Layer 2 » VLANs**, and then click **Ports**.
  - b. Select a switched Ethernet port.
  - c. Configure the following parameter(s) as required:

Parameter	Description
PVID	<p><b>Synopsis:</b> An integer between 1 and 4094</p> <p>The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.</p>
Type	<p><b>Synopsis:</b> [ edge   trunk   pvlanedge ]</p> <p><b>Default:</b> edge</p> <p>How the port determines its membership in VLANs. There are a few types of ports:</p> <ul style="list-style-type: none"> <li>• <b>EDGE</b> : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter).</li> <li>• <b>PVLAN Edge</b> : the port does not forward traffic to other PVLAN edge ports within the same VLAN.</li> <li>• <b>TRUNK</b> : the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration.</li> </ul>

Parameter	Description
Format	<p><b>Synopsis:</b> [ untagged   tagged ]</p> <p><b>Default:</b> untagged</p> <p>Whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.</p>
GVRP Mode	<p><b>Synopsis:</b> [ advertise_only   learn_advertise ]</p> <p>GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes:</p> <ul style="list-style-type: none"> <li>• DISABLED : the port is not capable of any GVRP processing.</li> <li>• ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.</li> <li>• ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.</li> </ul>

**Note**

Once a VLAN ID has been assigned to a switched Ethernet port, a VLAN is created and can be configured in **switch » vlans » all-vlans**.

6. If the port is in switchport mode, configure the VLAN for the port. For more information, refer to "Configuring VLANs for Switched Ethernet Ports" (Page 320).
7. Configure the port security settings. For more information, refer to "Configuring Port Security" (Page 139).
8. Configure the spanning tree settings. For more information, refer to "Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces" (Page 667).
9. Commit the changes.

### 8.2.3 Configuring RMON Threshold Alerts

RUGGEDCOM ROX II allows users to configure thresholds related to the performance and operation of physical Ethernet ports. When the rate of occurrence of a specified event is exceeded on the configured port, a log entry is recorded, an alarm is raised and an SNMP trap is generated.

An alarm and SNMP trap are only sent once when the threshold is crossed. If the current throughput value remains above the threshold value, additional alarms and traps are not sent at each interval. Once the current throughput value has dropped below the threshold value, its alarm state is reset and monitoring continues as normal. An alarm and trap are generated if the threshold is crossed again.

To configure RMON threshold alerts, do the following:

1. Navigate to the **RMON Parameters** tab under **Layer 2 » RMON Probing**.
2. Select an Ethernet port.
3. Configure the following parameter(s) as required:

---

#### Note

RMON may generate false alarms or SNMP traps under the following conditions:

- **The interval is low and the traffic throughput is 95% (but below 100%)**

In this scenario, do one of the following to eliminate the false alarms/traps:

- Reset **interval** to its default value (60 seconds)
  - If **monitor-type** is set to absolute or delta, increase the value of **threshold-value** by 5%
  - If **monitor-type** is set to percentage, increase the value of **threshold-percentage** by 5%
- **CPU usage is high and the traffic throughput is 90% (but below 100%)**
- In this scenario, do one of the following to eliminate the false alarms/traps:
- Reset **interval** to its default value (60 seconds)
  - If **monitor-type** is set to absolute or delta, increase the value of **threshold-value** by 10%
  - If **monitor-type** is set to percentage, increase the value of **threshold-percentage** by 10%

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables RMON threshold probing. When enabled, RMON probing will generate alarms and SNMP traps for that interface when threshold values are exceeded. RMON threshold alarms may also be controlled for the whole system under admin/alarm-cfg</p>
Direction	<p><b>Synopsis:</b> [ ingress   egress   both ]</p> <p><b>Default:</b> both</p> <p>The direction of traffic to be monitored. Possible values include:</p> <ul style="list-style-type: none"> <li>• Ingress - Monitors only the received bytes.</li> <li>• Egress - Monitors only the transmitted bytes.</li> <li>• Both - Monitors both the received and transmitted bytes.</li> </ul>
Monitoring Type	<p><b>Synopsis:</b> [ absolute   delta   percentage ]</p> <p><b>Default:</b> absolute</p> <p>The type of monitoring to perform on the threshold value. Possible values include:</p>

Parameter	Description
	<ul style="list-style-type: none"> <li>Absolute - The current absolute value of the monitored value is compared with the threshold value.</li> <li>Delta - The difference between the current value and the last recorded value (previous interval) of the monitored variable is compared with the threshold value.</li> <li>Percentage - The percentage of the total port bandwidth being utilized.</li> </ul>
Threshold Value	<p><b>Synopsis:</b> An integer between 1 and 18446744073709551615</p> <p><b>Default:</b> 1000</p> <p>The value of data throughput (in bytes per interval period) to be compared.</p>
Threshold Percentage	<p><b>Synopsis:</b> An integer between 1 and 100</p> <p><b>Default:</b> 80</p> <p>The percentage of total data throughput to check for bandwidth threshold.</p>
Threshold Checking Interval	<p><b>Synopsis:</b> An integer between 10 and 65535</p> <p><b>Default:</b> 60</p> <p>The number of seconds over which the data is sampled and compared with the threshold</p>

- Commit the changes.

## 8.2.4 Viewing Switched Ethernet Port Statistics

To view statistics collected for a specific switched Ethernet port, navigate to the **Port Statistics** tab under **Interface » Switch Ports**, and then select a switched Ethernet port.

The following information is provided:

Parameter	Description
InOctets	<p><b>Synopsis:</b> An integer</p> <p>The number of octets in received good packets. (Unicast+Multicast +Broadcast) and dropped packets.</p>
OutOctets	<p><b>Synopsis:</b> An integer</p> <p>The number of octets in transmitted good packets.</p>
InPkts	<p><b>Synopsis:</b> An integer</p> <p>The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.</p>
OutPkts	<p><b>Synopsis:</b> An integer</p> <p>The number of transmitted good packets.</p>

Parameter	Description
ErrorPkts	<b>Synopsis:</b> An integer The number of any type of erroneous packets.

## 8.2.5 Viewing the Status of a Switched Ethernet Port

To view the current status of a switched Ethernet port, navigate to the **Port Status** tab under **Interface » Switch Ports**, and then select a switched Ethernet port.

The following information is provided:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 10 characters long A descriptive name that may be used to identify the device connected on that port.
State	<b>Synopsis:</b> [ not set   up   down   testing   unknown   dormant   notPresent   lowerLayerDown ] The port's link status.
Media	<b>Synopsis:</b> A string up to 31 characters long The type of port media { 100TX, 10FL, 100FX, 1000X, 1000T, 802.11g, EoVDSL, 100TX }. It provides the user with a description of the installed media type on the port for modular products. Please note that fiber media may be either Single Mode(SM), Multi Mode(MM), and may be Short Distance, Long Distance or Very Long Distance with connectors like LC, SC, ST, MTRJ etc. For the modules with SFP/GBICs, the media description is displayed per the SFF-8472 specification, if the transceiver is plugged into the module. E.g. 10/100/1000TX RJ45, 100FX SM SC, 10FX MM ST, 1000SX SFP LC S SL M5.
Speed	<b>Synopsis:</b> [ auto   1.5M   2.4M   10M   100M   1G   10G   1.776M   3.072M   7.2M   1.2K   2.4K   9.6K   19.2K   38.4K   57.6K   115.2K   230.4K   4.8K   76.8K ] Speed (in Megabits-per-second or Gigabits-per-second)
Duplex	<b>Synopsis:</b> [ auto   half   full ] Duplex Setting: { Auto, Half, Full }
MTU	<b>Synopsis:</b> An integer The Maximum Transmission Unit of frame (in bytes) permitted on the interface.
MAC	<b>Synopsis:</b> A string up to 17 characters long The MAC Address of this specific port.

## 8.2.6 Viewing RMON Port Statistics

To view Remote Network Monitoring (RMON) statistics collected for a specific switched Ethernet port, navigate to the **RMON Statistics** tab under **Layer 2 » RMON Probing**, and then select a switched Ethernet port.

The following information is provided:

Parameter	Description
InOctets	<b>Synopsis:</b> An integer The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
InPkts	<b>Synopsis:</b> An integer The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
InBcastPkts	<b>Synopsis:</b> An integer The number of good broadcast packets received.
InMcastPkts	<b>Synopsis:</b> An integer The number of good multicast packets received.
TotalInOctets	<b>Synopsis:</b> An integer The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
TotalInPkts	<b>Synopsis:</b> An integer The number of received packets. This includes rejected, dropped and local packets, as well as packets which are not forwarded to the switching core for transmission. It should reflect all packets received on the line.
OutOctets	<b>Synopsis:</b> An integer The number of octets in transmitted good packets.
OutPkts	<b>Synopsis:</b> An integer The number of transmitted good packets.
Drop Events	<b>Synopsis:</b> An integer The number of received packets that are dropped due to lack of receive buffers.
OutBcastPkts	<b>Synopsis:</b> An integer The number of transmitted broadcast packets.
OutMcastPkts	<b>Synopsis:</b> An integer The number of transmitted multicast packets. This does not include broadcast packets.



Parameter	Description
CRCAAlignErrors	<b>Synopsis:</b> An integer  The number of packets received which meet all the following conditions: 1. The packet data length is between 64 and 1536 octets inclusive. 2. The packet has invalid CRC. 3. A Collision Event has not been detected. 4. A Late Collision Event has not been detected.
UndersizePkts	<b>Synopsis:</b> An integer  The number of received packets which meet all the following conditions: 1. The packet data length is less than 64 octets. 2. A Collision Event has not been detected. 3. A Late Collision Event has not been detected. 4. The packet has valid CRC.
OversizePkts	<b>Synopsis:</b> An integer  The number of packets received with data length greater than 1536 octets and valid CRC.
Fragments	<b>Synopsis:</b> An integer  The number of packets received which meet all the following conditions: 1. The packet data length is less than 64 octets, or it is a packet without SFD and is less than 64 octets in length. 2. A Collision Event has not been detected. 3. A Late Collision Event has not been detected. 4. The packet has invalid CRC.
Jabbers	<b>Synopsis:</b> An integer  The number of packets which meet all the following conditions: 1. The packet data length is greater than 1536 octets. 2. The packet has invalid CRC.
Collisions	<b>Synopsis:</b> An integer  The number of received packets for which a Collision Event has been detected.
Late Collision	<b>Synopsis:</b> An integer  The number of received packets for which a Late Collision Event has been detected.
Pkts64Octets	<b>Synopsis:</b> An integer  The number of received and transmitted packets with a size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkts65to127Octets	<b>Synopsis:</b> An integer  The number of received and transmitted packets with a size of 65 to 127 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets
Pkts128to255Octets	<b>Synopsis:</b> An integer  The number of received and transmitted packets with a size of 128 to 257 octets. This includes received and transmitted packets as

Parameter	Description
	well as dropped and local received packets. This does not include rejected received packets
Pkts256to511Octets	<b>Synopsis:</b> An integer  The number of received and transmitted packets with size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkts512to1023Octets	<b>Synopsis:</b> An integer  The number of received and transmitted packets with size of 512 to 1023 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets
Pkts1024to1518Octets	<b>Synopsis:</b> An integer  The number of received and transmitted packets with a size of 1024 to 1536 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.

## 8.2.7 Clearing Switched Ethernet Port Statistics

The following describes how to clear the statistics collected for switched ethernet ports. All of the statistics or only those for a specific switchport can be cleared.

### Clearing All Switched Ethernet Port Statistics

To clear all statistics collected for switched Ethernet ports, do the following:

1. Navigate to the **Port Statistics** tab under **Interface » Switch Ports**.
2. Under **Clear All Switch Statistics**, click **Perform**.

### Clearing Statistics for a Specific Switched Ethernet Port

To clear the statistics collected for a specific switched Ethernet port, do the following:

1. Navigate to the **Port Statistics** tab under **Interface » Switch Ports**.
2. In the **Port Statistics** column of the table, click the **Clear** button for the selected entry.

## 8.2.8 Resetting a Switched Ethernet Port

The following describes how to reset a specific Ethernet port, or all Ethernet ports.

### Resetting All Switched Ethernet Ports

To reset all switched Ethernet ports, do the following:

1. Navigate to the **Port Status** tab under **Interface » Switch Ports**.
2. Under **Reset All Switch Ports**, click **Perform**.

### Resetting a Specific Switched Ethernet Port

To reset a specific switched Ethernet port, do the following:


1. Navigate to the **Port Status** tab under **Interface » Switch Ports**, and then select a switched Ethernet port.
2. In the **Ethernet Port** column of the table, click the **Reset** button for the selected entry.

## 8.2.9 Testing Switched Ethernet Port Cables

Diagnostics can be performed on switched Ethernet port cables to assess their overall quality.

### 8.2.9.1 Running a Cable Diagnostic Test

To run a cable diagnostic test on a specific port, do the following:

 <b>NOTICE</b>
When cable diagnostics are performed on a port, any established network link on the port will be dropped and normal network traffic will not be able to pass through either the Port Under Test (PUT) or the Partner Port. When the cable diagnostic test is done, the original network port settings for both the PUT and the Partner Port are restored along with any established link.

1. Navigate to the **Diagnostics** tab under **Interface » Switch Ports**.
2. In the **Diagnostic** column of the table, click the **Start** button for the desired switch port. A dialog box appears.
3. Configure the following parameter(s) as required:

Parameter	Description
Runs	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 10
Calibration	<b>Synopsis:</b> A string <b>Default:</b> 0.0

4. Read and follow the instructions in the dialog box, and then click **OK** to start the test.

For information about how to view the test results, refer to "Viewing Cable Diagnostic Statistics" (Page 289).

### 8.2.9.2 Viewing Cable Diagnostic Statistics

Navigate to the **Diagnostics** tab under **Interface » Switch Ports**.

The following information is provided:

Parameter	Description
Running	<b>Synopsis:</b> [ true   false ] Whether or not a cable test is currently running on this port
Good Termination	<b>Synopsis:</b> An integer The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
Open	<b>Synopsis:</b> An integer The number of times OPEN is detected on the cable pairs of the selected port.
Short	<b>Synopsis:</b> An integer The number of times SHORT is detected on the cable pairs of the selected port.
Impedance Mismatch	<b>Synopsis:</b> An integer The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
Pass/Fail Total	<b>Synopsis:</b> A string between 1 and 19 characters long This field summarizes the results of the cable diagnostics performed so far. <ul style="list-style-type: none"> <li>• Pass : the number of times cable diagnostics were successfully completed on the selected port.</li> <li>• Fail : the number of times cable diagnostics failed to complete on the selected port.</li> <li>• Total : the total number of times cable diagnostics have been attempted on the selected port.</li> </ul>
Run Count	<b>Synopsis:</b> An integer Run Count : The total number of iterations
Pass Count	<b>Synopsis:</b> An integer Pass Count
Failure Count	<b>Synopsis:</b> An integer Failure Count

### 8.2.9.3 Clearing Cable Diagnostic Statistics

The following describes how to clear the statistics collected when cable diagnostic tests are performed. All of the statistics or only those for a specific switchport can be cleared.

#### Clearing All Cable Diagnostic Statistics

To clear the statistics, do the following:

1. Navigate to the **Diagnostics** tab under **Interface » Switch Ports**.
2. Under **Clear all Cable Diagnostics Results**, click **Perform**.

#### Clearing Cable Diagnostic Statistics for a Specific Switchport

To clear only the statistics for a specific switchport, do the following:

1. Navigate to the **Diagnostics** tab under **Interface » Switch Ports**.
2. In the **Diagnostics Result** column of the table, click the **Clear** button for the selected entry.

## 8.3 Managing Ethernet Trunk Interfaces

This section describes how to configure and manage Ethernet trunk interfaces.

### 8.3.1 Viewing a List of Ethernet Trunk Interfaces

To view a list of Ethernet trunk interfaces, navigate to **Interface » Trunks**. If trunks have been configured, a list appears.

If no Ethernet trunk interfaces have been configured, add trunks as needed. For more information, refer to "Adding an Ethernet Trunk Interface" (Page 290).

### 8.3.2 Adding an Ethernet Trunk Interface

To add an Ethernet trunk interface, do the following:

1. Navigate to **Interface » Trunks**, and then click **Add Entry**. A dialog box appears.
2. Configure the following parameter(s) as required:

Parameter	Description
Trunk ID	<b>Synopsis:</b> An integer between 1 and 15  The trunk number. It doesn't affect port trunk operation in any way and is only used for identification.

3. Click **OK** to create the new trunk.

4. Select the trunk, and then configure the following parameter(s) as required:

Parameter	Description
Switch Port	<b>Synopsis:</b> [ true   false ] The physical port into either Switched mode or a dedicated Routing mode.
On Demand	Bring up this interface on-demand only
IP Address Source	<b>Synopsis:</b> [ static   dynamic ] Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
IPv6 Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IP address is static or dynamically assigned via DHCP. Option DYNAMIC is a common case of a dynamically assigned IP address. This must be static for non-management interfaces.
Proxy ARP	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
MTU	<b>Synopsis:</b> An integer between 68 and 9216 <b>Default:</b> 1500 Maximum transmission unit (largest packet size allowed for this interface).
Alias	<b>Synopsis:</b> A string up to 64 characters long The SNMP alias name of the interface
Trunk Ports	<b>Synopsis:</b> An integer between 1 and 16 List of ports aggregated into the trunk.

5. Configure the multicast filtering parameters:
- Navigate to the **GMRP Parameters** tab under **Layer 2 » Multicast Filtering**, and then click **Trunks**.
  - Select a trunk.
  - Configure the following parameter(s) as required:

Parameter	Description
GMRP	<b>Synopsis:</b> [ advertise_only   learn_advertise ] GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: <ul style="list-style-type: none"> <li><b>DISABLED</b> : the port is not capable of any GMRP processing.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.</li> <li>ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.</li> </ul>

6. Configure the CoS parameters:
  - a. Navigate to the **CoS Parameters** tab under **Layer 2 » CoS Mapping**, and then click **Trunks**.
  - b. Select a trunk.
  - c. Configure the following parameter(s) as required:

Parameter	Description
Default Priority	<p><b>Synopsis:</b> An integer between 0 and 7</p> <p><b>Default:</b> 0</p> <p>The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).</p>
Inspect ToS	<p>Enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing is enabled the switch will use the Differentiated Services bits in the TOS field.</p>

7. Configure the VLAN parameters:
  - a. Navigate to the **Port Parameters** tab under **Layer 2 » VLANs**, and then click **Trunks**.
  - b. Select a trunk.
  - c. Configure the following parameter(s) as required:

Parameter	Description
PVID	<p><b>Synopsis:</b> An integer between 1 and 4094</p> <p>The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.</p>
Type	<p><b>Synopsis:</b> [ edge   trunk   pvlanedge ]</p> <p><b>Default:</b> edge</p> <p>How the port determines its membership in VLANs. There are the following port types:</p> <ul style="list-style-type: none"> <li>EDGE : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter).</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN.</li> <li>TRUNK : the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration.</li> </ul>
Format	<p><b>Synopsis:</b> [ untagged   tagged ]</p> <p><b>Default:</b> untagged</p> <p>Whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.</p>
GVRP Mode	<p><b>Synopsis:</b> [ advertise_only   learn_advertise ]</p> <p>GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes:</p> <ul style="list-style-type: none"> <li>DISABLED : the port is not capable of any GVRP processing.</li> <li>ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.</li> <li>ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.</li> </ul>

8. Commit the changes.

### 8.3.3 Deleting an Ethernet Trunk Interface

To delete an Ethernet trunk interface, do the following:

1. Navigate to **Interface » Trunks**.
2. Select the trunk to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 8.3.4 Managing Ethernet Trunk Ports

This section describes how to manage Ethernet trunk port assignments.

#### 8.3.4.1 Viewing a List of Ethernet Trunk Ports

To view a list of Ethernet trunk ports, navigate to **Interface » Trunks**. If trunk ports have been configured, the a list appears.



If no Ethernet trunk ports have been configured, add ports as needed. For more information, refer to "Adding an Ethernet Trunk Port" (Page 294).

#### 8.3.4.2 Adding an Ethernet Trunk Port

To add an Ethernet trunk port, do the following:

1. Navigate to **Interface » Trunks**.
2. Under **Trunk Ports**, select the trunk port to be added from the drop down list, and then click **OK**.

---

**Note**

Routable Ethernet ports cannot be configured as trunk ports.

---

3. Commit the change.

#### 8.3.4.3 Deleting an Ethernet Trunk Port

To delete an Ethernet trunk port, do the following:

1. Navigate to **Interface » Trunks**.
2. Under **Trunk Ports**, deselect the trunk port to be deleted from the drop down list, and then click **OK**.
3. Commit the change.

## 8.4 Managing MAC Addresses

As part of the Layer 2 functionality, RUGGEDCOM ROX II maintains a Media Access Control (MAC) address table, a list of unique MAC addresses for network interfaces that can communicate with the device at the data link layer. The MAC address table can be populated manually by defining specific MAC addresses and/or dynamically. When populated dynamically, RUGGEDCOM ROX II automatically adds the MAC addresses of network interfaces it detects on the network. It will also remove those addresses if the address ages out or there is a link failure.

### 8.4.1 Viewing a Dynamic List of MAC Addresses

To view a dynamic list of learned and statically configured MAC addresses, navigate to the **View Mac Table** tab under **Layer 2 » Mac Table**. If MAC addresses have been learned, a list appears.

The following information is provided:

Parameter	Description
Slot	<p><b>Synopsis:</b> [ sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport ]</p> <p>The slot containing the module including the port.</p>
Port	<p><b>Synopsis:</b> An integer between 1 and 16</p> <p>The port on which the MAC address has been learned.</p>
Type	<p><b>Synopsis:</b> [ static   dynamic ]</p> <p>How the MAC address has been learned by the switch:</p> <ul style="list-style-type: none"> <li>• <b>STATIC:</b> The address has been learned as a result of static MAC address table configuration or some other management activity and cannot be automatically unlearned or relearned by the switch.</li> <li>• <b>DYNAMIC:</b> The address has been automatically learned by the switch and can be automatically unlearned.</li> </ul>
CoS	<p><b>Synopsis:</b> [ N/A   normal   medium   high   crit ]</p> <p>The Class Of Service (CoS) that is assigned to frames carrying this address as a source or destination address.</p>

If a MAC address is not listed, do the following:

- Configure the MAC address learning options to dynamically detect the MAC addresses of other devices on the network. For more information, refer to "Configuring MAC Address Learning Options" (Page 295).
- Configure the address on the device as a static MAC address. For more information, refer to "Adding a Static MAC Address" (Page 296).

## 8.4.2 Purging the Dynamic MAC Address List

To purge the dynamic MAC address list of all entries, do the following:

1. Navigate to the **View Mac Table** tab under **Layer 2 » Mac Table**.
2. Under **Purge MAC Address Table**, click the **Perform** button.

## 8.4.3 Configuring MAC Address Learning Options

The MAC address learning options control how and when MAC addresses are removed automatically from the MAC address table. Individual addresses are removed when the aging timer is exceeded. Addresses can also be removed when a link failure or topology change occurs.

To configure the MAC address learning options, do the following:

1. Navigate to the **General** tab under **Layer 2 » Mac Table**.
2. Configure the following parameter(s) as required:

Parameter	Description
MAC Aging Time (s)	<p><b>Synopsis:</b> An integer between 15 and 800</p> <p><b>Default:</b> 300</p> <p>The time a learned MAC address is held before being aged out.</p>
MAC Aging on Loss	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>When link failure (and potentially a topology change) occurs, the switch may have some MAC addresses previously learned on the failed port. As long as those addresses are not aged-out, the switch will still be forwarding traffic to that port, thus preventing that traffic from reaching its destination via the new network topology. This parameter allows the aging-out of all MAC addresses learned on a failed port immediately upon link failure detection.</p>

3. Commit the changes.

## 8.4.4 Managing Static MAC Addresses

Static MAC addresses must be configured when destination devices are only able to receive frames, not transmit them. They may also need to be configured if port security (if supported) must be enforced.

Prioritized MAC addresses are configured when traffic to or from a specific device on a LAN segment is to be assigned a higher CoS priority than other devices on that LAN segment.

### 8.4.4.1 Viewing a List of Static MAC Addresses

To view a list of static MAC addresses configured on the device, navigate to the **Static MAC Table** tab under **Layer 2 » Mac Table**. If static MAC addresses have been configured, a list appears.

If no static MAC addresses have been configured, add addresses as needed. For more information, refer to "Adding a Static MAC Address" (Page 296).

### 8.4.4.2 Adding a Static MAC Address

To add a static MAC address, do the following:

1. Navigate to the **Static MAC Table** tab under **Layer 2 » Mac Table**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

**Note**

Letters in MAC addresses must be lowercase.

Parameter	Description
MAC Address	<b>Synopsis:</b> A string up to 17 characters long  A unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094  The VLAN identifier of the VLAN upon which the MAC address operates.

- Click **OK** to add the static MAC address.
- Configure the following parameter(s) as required:

Parameter	Description
Learned	If set, the system will auto-learn the port upon which the device with this address is located.
Slot	<b>Synopsis:</b> [ sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport ]  The name of the module location provided on the silkscreen across the top of the device.
Port	<b>Synopsis:</b> An integer between 1 and 16  The selected ports on the module installed in the indicated slot.
CoS	<b>Synopsis:</b> [ N/A   normal   medium   high   crit ] <b>Default:</b> normal  The priority of traffic for a specified address.

- Commit the changes.

### 8.4.4.3 Deleting a Static MAC Address

To delete a static MAC address, do the following:

- Navigate to the **Static MAC Table** tab under **Layer 2 » Mac Table**.
- Select the static MAC address to be deleted, and then click **Delete Entry**.
- Commit the change.

## 8.5 Managing Multicast Filtering

Multicast traffic can be filtered using either static multicast groups, IGMP (Internet Group Management Protocol) snooping, or GMRP (GARP Multicast Registration Protocol).

### 8.5.1 Multicast Filtering Concepts

This section describes some of the concepts important to the implementation of multicast filtering in RUGGEDCOM ROX II.

#### 8.5.1.1 IGMP

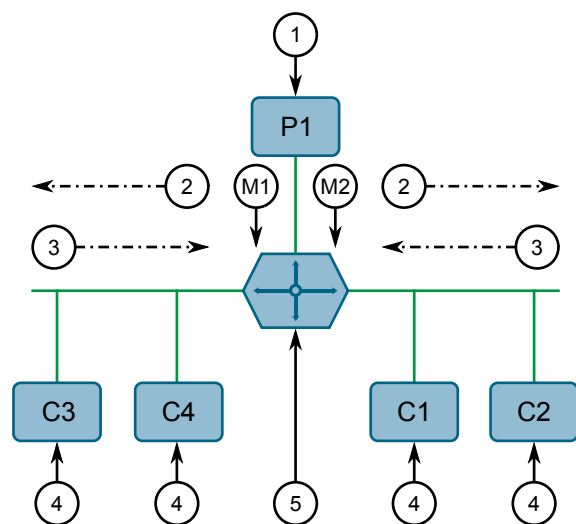
IGMP is used by IP hosts to report their host group memberships with multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host.

The IGMP protocol operates between multicast routers and IP hosts. When an unmanaged switch is placed between multicast routers and their hosts, the multicast streams will be distributed to all ports. This may introduce significant traffic onto ports that do not require it and receive no benefit from it.

IGMP Snooping, when enabled, will act on IGMP messages sent from the router and the host, restricting traffic streams to the appropriate LAN segments.

#### Example: IGMP In Operation

The following network diagram provides a simple example of the use of IGMP.



- ① Producer
- ② Membership Queries
- ③ Membership Reports

- ④ Host
- ⑤ Multicast Router

Figure 8.1 Example – IGMP In Operation

One *producer* IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential *consumers* of these streams, C1 through C4. The multicast router discovers which host wishes to subscribe to which stream by sending general membership queries to each segment.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (or *join*) indicating the desire to subscribe to stream M2. The router will forward the M2 stream to the C1-C2 segment. In a similar fashion, the router discovers that it must forward stream M1 to segment C3-C4.

A *consumer* may join any number of multicast groups, issuing a membership report for each group. When a host issues a membership report, other hosts on the same network segment that also require membership to the same group suppress their own requests, since they would be redundant. In this way, the IGMP protocol guarantees the segment will issue only one membership report for each group.

The router periodically queries each of its segments in order to determine whether at least one consumer still subscribes to a given stream. If it receives no responses within a given time period (usually two query intervals), the router will prune the multicast stream from the given segment.

A more common method of pruning occurs when consumers wishing to unsubscribe issue an IGMP *leave group* message. The router will immediately issue a group-specific membership query to determine whether there are any remaining subscribers of that group on the segment. After the last consumer of a group has unsubscribed, the router will prune the multicast stream from the given segment.

## Switch IGMP Operation

The IGMP Snooping feature provides a means for switches to snoop (i.e. watch) the operation of routers, respond with joins/leaves on the behalf of consumer ports, and prune multicast streams accordingly. There are two modes of IGMP the switch can be configured to assume: active and passive.

- **Active Mode**

IGMP supports a *routerless* mode of operation.

When such a switch is used without a multicast router, it is able to function as if it is a multicast router sending IGMP general queries.

- **Passive Mode**

When such a switch is used in a network with a multicast router, it can be configured to run Passive IGMP. This mode prevents the switch from sending the queries that can confuse the router causing it to stop issuing IGMP queries.

**Note**

A switch running in passive mode requires the presence of a multicast router or it will be unable to forward multicast streams at all if no multicast routers are present.

---

**Note**

Without a multicast router, at least one IGMP Snooping switch must be in active mode to make IGMP functional.

---

## IGMP Snooping Rules

IGMP Snooping adheres to the following rules:

- When a multicast source starts multicasting, the traffic stream will be immediately blocked on segments from which joins have not been received.
- Unless configured otherwise, the switch will forward all multicast traffic to the ports where multicast routers are attached.
- Packets with a destination IP multicast address in the 224.0.0.X range that are not IGMP are always forwarded to all ports. This behavior is based on the fact that many systems do not send membership reports for IP multicast addresses in this range while still listening to such packets.
- The switch implements *proxy-reporting* (i.e. membership reports received from downstream are summarized and used by the switch to issue its own reports).
- The switch will only send IGMP membership reports out of those ports where multicast routers are attached, as sending membership reports to hosts could result in unintentionally preventing a host from joining a specific group.
- Multicast routers use IGMP to elect a master router known as the *querier*. The *querier* is the router with the lowest IP address. All other routers become non-queriers, participating only in forwarding multicast traffic. Switches running in active mode participate in the querier election the same as multicast routers.
- When the querier election process is complete, the switch simply relays IGMP queries received from the querier.
- When sending IGMP packets, the switch uses its own IP address, if it has one, for the VLAN on which packets are sent, or an address of 0.0.0.0, if it does not have an assigned IP address.

**Note**

IGMP Snooping switches perform multicast pruning using a multicast frame's destination MAC multicast address, which depends on the group IP multicast address. IP address W.X.Y.Z corresponds to MAC address 01-00-5E-XX-YY-ZZ where XX is the lower 7 bits of X, and YY and ZZ are simply Y and Z coded in hexadecimal.

One can note that IP multicast addresses, such as 224.1.1.1 and 225.1.1.1, will both map onto the same MAC address 01-00-5E-01-01-01. This is a problem for which the

IETF Network Working Group currently has offered no solution. Users are advised to be aware of and avoid this problem.

## IGMP and RSTP

An RSTP change of topology can render the routes selected to carry multicast traffic as incorrect. This results in lost multicast traffic.

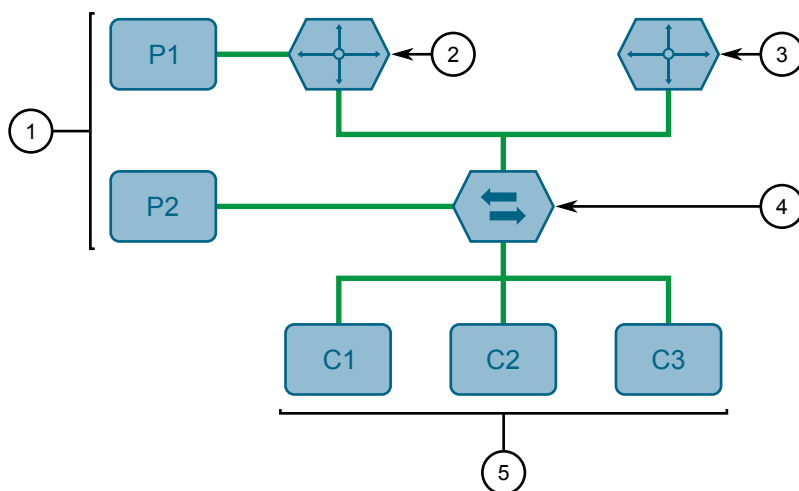
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- The switch will immediately issue IGMP queries (if in IGMP Active mode) to obtain potential new group membership information.
- The switch can be configured to flood multicast streams temporarily out of all ports that are not RSTP Edge Ports.

## Combined Router and Switch IGMP Operation

The following example illustrates the challenges faced with multiple routers, VLAN support and switching.

Producer P1 resides on VLAN 2 while P2 resides on VLAN 3. Consumer C1 resides on both VLANs whereas C2 and C3 reside on VLANs 3 and 2, respectively. Router 2 resides on VLAN 2, presumably to forward multicast traffic to a remote network or act as a source of multicast traffic itself.



- ① Producer
- ② Multicast Router 1
- ③ Multicast Router 2
- ④ Switch
- ⑤ Host

Figure 8.2 Example – Combined Router and Switch IGMP In Operation

In this example:



- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

- **Processing Joins**

If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.

- **Processing Leaves**

When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

### 8.5.1.2 GMRP (GARP Multicast Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.

**Note**

GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.

---

**Joining a Multicast Group**

In order to join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

**Leaving a Multicast Group**

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

**Notes About GMRP**

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

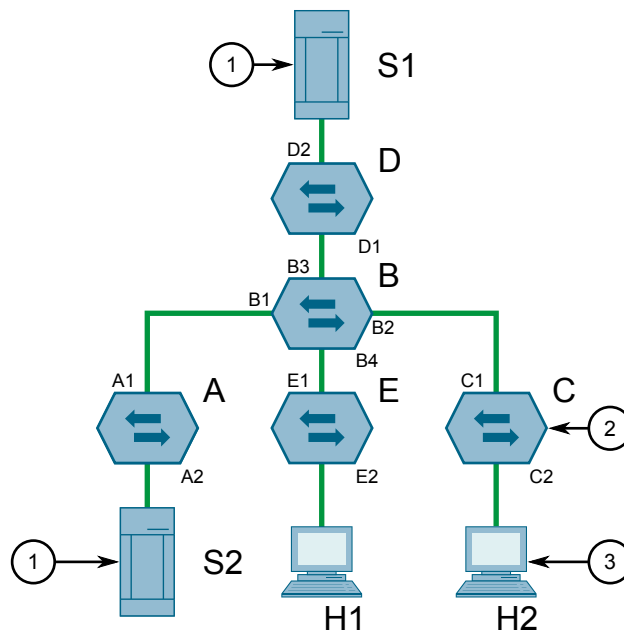
- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled on the RUGGEDCOM RX5000, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the RUGGEDCOM RX5000, and not forwarded.

**Example: Establishing Membership with GMRP**

The following example illustrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

In this scenario, there are two multicast sources, S1 and S2, multicasting to Multicast Groups 1 and 2, respectively. A network of five switches, including one core switch (B), connects the sources to two hosts, H1 and H2, which receive the multicast streams from S1 and S2, respectively.



- ① Multicast Source
- ② Switch
- ③ Multicast Host

Figure 8.3 Example – Establishing Membership with GMRP

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

1. Host H1 is GMRP unaware, but needs to see traffic for Multicast Group 1. Therefore, Port E2 on Switch E is statically configured to forward traffic for Multicast Group 1.
2. Switch E advertises membership in Multicast Group 1 to the network through Port E1, making Port B4 on Switch B a member of Multicast Group 1.
3. Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
4. Host H2 is GMRP-aware and sends a *join* request for Multicast Group 2 to Port C2, which thereby becomes a member of Multicast Group 2.
5. Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.
- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.
- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.
- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

## 8.5.2 Enabling and Configuring GMRP

To enable and configure GMRP (GARP Multicast Registration Protocol), do the following:

1. Navigate to the **Global GMRP Parameters** tab under **Layer 2 » Multicast Filtering**.
2. Configure the following parameter(s) as required:

Parameter	Description
GMRP	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>GMRP Enable</p>
RSTP Flooding	Determines whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.
Leave Timer (ms)	<p><b>Synopsis:</b> An integer between 600 and 300000</p> <p><b>Default:</b> 4000</p> <p>The time in milliseconds to wait after issuing Leave or LeaveAll before removing registered multicast groups. If Join messages for specific addresses are received before this timer expires, the addresses will be kept registered.</p>

3. Enable GMRP on one or more switched Ethernet ports. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276).
4. Commit the changes.

### 8.5.3 Managing IGMP Snooping

This sections describes how to configure IGMP snooping and manage ports monitored by the service.

#### 8.5.3.1 Configuring IGMP Snooping

To configure IGMP snooping, do the following:

1. Navigate to the **IGMP Snooping** tab under **Layer 2 » Multicast Filtering**.
2. Configure the following parameter(s) as required:

Parameter	Description
IGMP Mode	<p><b>Synopsis:</b> [ active   passive ]</p> <p><b>Default:</b> passive</p> <p>Specifies the IGMP mode:</p> <ul style="list-style-type: none"> <li>• PASSIVE : The switch passively snoops IGMP traffic and never sends IGMP queries.</li> <li>• ACTIVE : The switch generates IGMP queries, if no queries from a better candidate for the querier are detected for a while.</li> </ul>
IGMP Query Internal (s)	<p><b>Synopsis:</b> An integer between 10 and 3600</p> <p><b>Default:</b> 60</p> <p>The time interval between IGMP queries generated by the switch. NOTE: This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in PASSIVE mode.</p>
IGMP Version	<p><b>Synopsis:</b> [ v2   v3 ]</p> <p><b>Default:</b> v2</p> <p>The version of IGMP. Options include:</p> <ul style="list-style-type: none"> <li>• v2: IGMP version 2.</li> <li>• v3: IGMP version 3. Backwards compatible with v2.</li> </ul>
Router Forwarding	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Whether or not multicast streams will always be forwarded to multicast routers.</p>
RSTP Flooding	<p>Whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.</p>

3. Assign one or more ports for IGMP to use when sending Membership Reports. For more information, refer to "Adding a Router Port" (Page 307).

4. Enable IGMP snooping for the required static VLAN(s). For more information, refer to "Adding a Static VLAN" (Page 321).
5. Commit the changes.

### 8.5.3.2 Viewing a List of Router Ports

To view a list of router ports used for IGMP snooping, navigate to the **IGMP Snooping** tab under **Layer 2 » Multicast Filtering**. If router ports have been configured, a list appears under **Router Ports**.

If no router ports have been configured, add ports as needed. For more information, refer to "Adding a Router Port" (Page 307).

### 8.5.3.3 Adding a Router Port

To add a router port for IGMP snooping, do the following:

1. Navigate to the **IGMP Snooping** tab under **Layer 2 » Multicast Filtering**.
2. Under **Router Ports**, select the port to be added from the drop down list.
3. Commit the change.

### 8.5.3.4 Deleting a Router Port

To delete a router port for IGMP snooping, do the following:

1. Navigate to the **IGMP Snooping** tab under **Layer 2 » Multicast Filtering**.
2. Under **Router Ports**, click the **X** beside the port to be deleted.
3. Commit the change.

## 8.5.4 Managing the Static Multicast Group Table

This section describes how to manage entries in the Static Multicast Group table.

### 8.5.4.1 Viewing a List of Static Multicast Group Entries

To view a list of entries for known static multicast groups on other devices, navigate to the **Static Multicast Table** tab under **Layer 2 » Multicast Filtering**. If entries have been configured, a list appears.

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Static Multicast Group Entry" (Page 308).

### 8.5.4.2 Adding a Static Multicast Group Entry

To list a static multicast group from another device in the Static Multicast Summary table, do the following:

1. Navigate to the **Static Multicast Table** tab under **Layer 2 » Multicast Filtering**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094  The VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	<b>Synopsis:</b> A string up to 17 characters long  The multicast group MAC address in the form 01:xx:xx:xx:xx:xx.

4. Click OK to add the static multicast group.
5. Configure the following parameter(s) as required:

---

#### Note

Letters in MAC addresses must be lowercase.

---

Parameter	Description
CoS	<b>Synopsis:</b> [ N/A   normal   medium   high   crit ] <b>Default:</b> normal  The Class Of Service that is assigned to the multicast group frames.

6. Add one or more egress ports. For more information, refer to "Adding an Egress Port" (Page 309).
7. Click **Add** to create the table entry.
8. Commit the changes.

### 8.5.4.3 Deleting a Static Multicast Group Entry

To delete a static multicast group from the Static Multicast Summary table, do the following:

1. Navigate to the **Static Multicast Table** tab under **Layer 2 » Multicast Filtering**.
2. Select the table entry to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 8.5.5 Managing Egress Ports for Multicast Groups

This section describes how to configure and manage egress ports for a multicast group.

### 8.5.5.1 Viewing a List of Egress Ports

To view a list of egress ports for a static multicast group defined in the Static Multicast Group Summary table, navigate to the **Static Multicast Table** tab under **Layer 2 » Multicast Filtering**. If egress ports have been configured, they appear in the **Egress Ports** column.

If no egress ports have been configured, add egress ports as needed. For more information, refer to "Adding an Egress Port" (Page 309).

### 8.5.5.2 Adding an Egress Port

To add an egress port to a static multicast group defined in the Static Multicast Group Summary table, do the following:

1. Navigate to the **Static Multicast Table** tab under **Layer 2 » Multicast Filtering**.
2. Select a static multicast group.
3. Under **Egress Ports**, select the port to be added from the drop down list, and then click **OK**.
4. Commit the change.

### 8.5.5.3 Deleting an Egress Port

To delete an egress port for a static multicast group defined in the Static Multicast Group Summary table, do the following:

1. Navigate to the **Static Multicast Table** tab under **Layer 2 » Multicast Filtering**.
2. Under **Egress Ports**, deselect the port to be deleted from the drop down list, and then click **OK**.
3. Commit the change.

## 8.5.6 Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, navigate to the **Multicast Group Summary** tab under **Layer 2 » Multicast Filtering**. If multicast groups have been configured, a list appears.

The following information is provided:



Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer The VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	<b>Synopsis:</b> A string up to 17 characters long The multicast group MAC address.
Static Ports	<b>Synopsis:</b> An integer between 1 and 16 The ports that joined this group statically through static configuration in the Static MAC Table and to which the multicast group traffic is forwarded.
GMRP Dynamic Ports	<b>Synopsis:</b> An integer between 1 and 16 The ports that joined this group dynamically through GMRP application and to which the multicast group traffic is forwarded.

## 8.5.7 Viewing a List of IP Multicast Groups

To view a list of all IP multicast groups, navigate to the **IP Multicast Summary** tab under **Layer 2 » Multicast Filtering**. If IP multicast groups have been configured, a list appears.

The following information is provided:

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer The VLAN Identifier of the VLAN upon which the multicast group operates.
IP Address	<b>Synopsis:</b> A string The multicast group IP address.
MAC Address	<b>Synopsis:</b> A string up to 17 characters long The multicast MAC address corresponding to the group multicast IP address.
Joined Ports	<b>Synopsis:</b> An integer between 1 and 16 The selected ports on the module installed in the indicated slot.
Router Ports	<b>Synopsis:</b> An integer between 1 and 16 The selected ports on the module installed in the indicated slot.

## 8.6 Managing VLANs

A Virtual Local Area Network (VLAN) is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. VLANs are extremely flexible because they are based on logical connections, rather than physical connections.

When VLANs are introduced, all traffic in the network must belong to one VLAN or another. Traffic on one VLAN cannot pass to another, except through an inter-network router or Layer 3 switch.

VLANs are created in three ways:

- **Explicitly**  
Static VLANs can be created in the switch. For more information about static VLANs, refer to "Managing Static VLANs" (Page 321).
- **Implicitly**  
When a VLAN ID (VID) is set for a Port VLAN (PVLAN), static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.
- **Dynamically**  
VLANs can be learned through GVRP. For more information about GVRP, refer to "GARP VLAN Registration Protocol (GVRP)" (Page 313)

### 8.6.1 VLAN Concepts

This section describes some of the concepts important to the implementation of VLANs in RUGGEDCOM ROX II.

#### 8.6.1.1 Tagged vs. Untagged Frames

VLAN tags identify frames as part of a VLAN network. When a switch receives a frame with a VLAN (or 802.1Q) tag, the VLAN identifier (VID) is extracted and the frame is forwarded to other ports on the same VLAN.

When a frame does not contain a VLAN tag, or contains an 802.1p (prioritization) tag that only has prioritization information and a VID of 0, it is considered an untagged frame.

#### 8.6.1.2 Native VLAN

Each port is assigned a native VLAN number, the Port VLAN ID (PVID). When an untagged frame ingresses a port, it is associated with the port's native VLAN.

By default, when a switch transmits a frame on the native VLAN, it sends the frame untagged. The switch can be configured to transmit tagged frames on the native VLAN.

### 8.6.1.3 Edge and Trunk Port Types

Each port can be configured as an edge or trunk port.

An edge port attaches to a single end device, such as a PC or Intelligent Electronic Device (IED). An edge port carries traffic on the native VLAN.

Trunk ports are part of the network and carry traffic for all VLANs between switches. Trunk ports are automatically members of all VLANs configured in the switch.

The switch can 'pass through' traffic, forwarding frames received on one trunk port out of another trunk port. The trunk ports must be members of all VLANs that the 'pass through' traffic is part of, even if none of those VLANs are used on edge ports.

Frames transmitted out of the port on all VLANs other than the port's native VLAN are always sent tagged.

---

#### Note

It may be desirable to manually restrict the traffic on the trunk to a specific group of VLANs. For example, when the trunk connects to a device, such as a Layer 3 router, that supports a subset of the available LANs. To prevent the trunk port from being a member of the VLAN, include it in the VLAN's Forbidden Ports list.

For more information about the Forbidden Ports list, refer to "Forbidden Ports List" (Page 313).

Port Type	VLANs Supported	PVID Format	Usage
Edge	1 (Native) Configured	Untagged	<i>VLAN Unaware Networks:</i> All frames are sent and received without the need for VLAN tags.
		Tagged	<i>VLAN Aware Networks:</i> VLAN traffic domains are enforced on a single VLAN.
Trunk	All Configured	Tagged or Untagged	<p><i>switch-to-Switch Connections:</i> VLANs must be manually created and administered, or can be dynamically learned through GVRP.</p> <p><i>Multiple-VLAN End Devices:</i> Implement connections to end devices that support multiple VLANs at the same time.</p>

### 8.6.1.4 Ingress Filtering

Ingress filtering is a method of verifying that inbound packets arriving at a network originate from the source they are expected to be from, before entry (or ingress) is granted.

When ingress filtering is enabled, the switch verifies any tagged frame arriving at a port. When the port is not a member of the VLAN with which the frame is associated, the frame is dropped. When ingress filtering is disabled, frames from VLANs configured to the switch are not dropped. For more information about enabling or disabling ingress filtering, refer to "Enabling/Disabling Ingress Filtering" (Page 319).

### 8.6.1.5 Forbidden Ports List

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more about configuring a list of forbidden ports, refer to "Managing Forbidden Ports" (Page 322).

### 8.6.1.6 VLAN-Aware Mode of Operation

The native operation mode for an IEEE 802.1Q compliant switch is VLAN-aware. Even if a specific network architecture does not use VLANs, RUGGEDCOM ROX II's default VLAN settings allow the switch to still operate in a VLAN-aware mode, while providing functionality required for almost any network application. However, the IEEE 802.1Q standard defines a set of rules that must be followed by all VLAN-aware switches:

- Valid VIDs are within the range of 1 to 4094. VID's equal to 0 or 4095 are invalid.
- Each frame ingressing a VLAN-aware switch is associated with a valid VID.
- Each frame egressing a VLAN-aware switch is either untagged or tagged with a valid VID. Priority-tagged frames with an invalid VID will never be sent out by a VLAN-aware switch.

---

#### Note

Some applications have requirements conflicting with IEEE 802.Q native mode of operation. For example, some applications explicitly require priority-tagged frames to be received by end devices.

---

### 8.6.1.7 GARP VLAN Registration Protocol (GVRP)

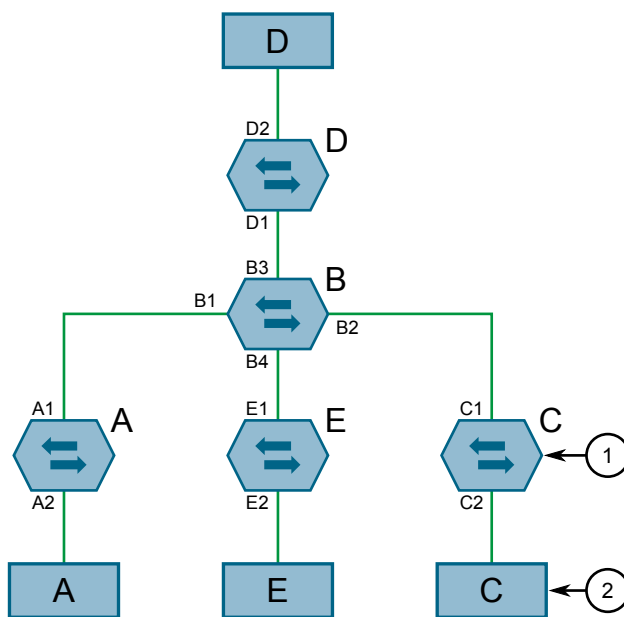
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere in the network are learned through GVRP. A GVRP-aware end station (i.e. PC or Intelligent Electronic Device) configured for a particular VID can be connected to a trunk on a GVRP-aware switch and automatically become part of the desired VLAN.

When a switch sends GVRP bridge protocol data units (BPDUs) out of all GVRP-enabled ports, GVRP BPDUs advertise all the VLANs known to that switch (configured manually or learned dynamically through GVRP) to the rest of the network.

When a GVRP-enabled switch receives a GVRP BPDU advertising a set of VLANs, the receiving port becomes a member of those advertised VLANs and the switch begins advertising those VLANs through all the GVRP-enabled ports (other than the port on which the VLANs were learned).

To improve network security using VLANs, GVRP-enabled ports may be configured to prohibit the learning of any new dynamic VLANs but at the same time be allowed to advertise the VLANs configured on the switch.

The following is an example of how to use GVRP:



- ① Switch
- ② End Node

Figure 8.4 Using GVRP

- Switch B is the core switch, all others are edge switches
- Ports A1, B1 to B4, C1, D1, D2 and E1 are GVRP aware
- Ports B1 to B4, D1 and D2 are set to advertise and learn
- Ports A1, C1 and E1 are set to advertise only
- Ports A2, C2 and E2 are edge ports
- End node D is GVRP aware
- End nodes A, E and C are GVRP unaware
- Ports A2 and C2 are configured with PVID 7
- Port E2 is configured with PVID 20
- End node D is interested in VLAN 20, hence VLAN 20 is advertised by it towards switch B
- D2 becomes a member of VLAN 20
- Ports A1 and C1 advertise VID 7
- Ports B1 and B2 become members of VLAN 7
- Ports D1 and B1 advertise VID 20
- Ports B3, B4 and D1 become members of VLAN 20

### 8.6.1.8 PVLAN Edge

Protected VLAN (PVLAN) Edge refers to a feature of the switch that isolates multiple VLAN Edge ports from each other on a single device. All VLAN Edge ports in a switch that are configured as *protected* in this way are prohibited from sending frames to one another, but are still permitted to send frames to other, non-protected ports within the same VLAN. This protection extends to all traffic on the VLAN, including unicast, multicast and broadcast traffic.

---

#### Note

This feature is strictly local to the switch. PVLAN Edge ports are not prevented from communicating with ports outside of the switch, whether protected (remotely) or not.

---

Ports belonging to a specific PVID and a VLAN type of PVLAN Edge are part of one PVLAN Edge group. A PVLAN Edge group should include a minimum of two ports. There can be multiple PVLAN Edge groups on a switch.

It is not possible to combine a Gbit port with a 10/100 Mbit port as part of the same PVLAN Edge group.

Possible combinations of a PVLAN Edge group are listed below:

- A PVLAN Edge group with 10/100 Mbit ports from any line modules, with the exception of 2-port 100Base-FX line modules
- A PVLAN Edge group with Gbit ports from any line modules
- A PVLAN Edge group with 10/10 Mbit ports from 2-port 100Base-FX and Gbit ports from any line modules

### 8.6.1.9 Restricted VLANs

RUGGEDCOM ROX II allows users to configure 802.1X ports in **Guest VLAN** or **Quarantine VLAN** mode, to limit services to clients when IEEE 802.1x or 802.1x/ MAC-Auth authentication fails. For example, an administrator may choose to restrict access to only printers, Internet, or specific downloads for unauthenticated users.

When a client fails to authenticate after a specified number of attempts, the configured port will switch automatically to either the Quarantine VLAN or the Guest VLAN, depending on the port security mode and the client's security setup:

- If a connected device supports 802.1x security but has failed authentication, the port will switch to the Quarantine VID.
- If a connected device is 802.1X incompatible and port security is set to 802.1X, the port will become a member of the Guest VLAN after the authentication times out.

When a port is a member of the Quarantine VLAN, RUGGEDCOM ROX II will attempt to re-authenticate the client at configured intervals. Clients who fail to authenticate remain in the Quarantine VLAN until successfully re-authenticated, or until the

physical link goes down. If re-authentication fails, the port remains a member of the Quarantine VLAN.

There are no re-authentication attempts for clients in Guest VLANs. When an EAPOL Start frame is received from the client, the port will revert to the unauthenticated state, removing the client's access from the Guest VLAN to continue with the authentication process.

The following table outlines Quarantine vs Guest port placement behavior following authentication failure:

Port Security Mode	Client Security	Placement Following Authentication Failure
802.1x	802.1x Capable	Quarantine VLAN
	802.1x Not Capable	Guest VLAN
802.1x/MAC-Auth	802.1x Capable	Quarantine VLAN
	802.1x Not Capable	Quarantine VLAN

For more information about configuring a Guest/Quarantine VLAN, refer to "Configuring Port Security" (Page 139).

#### 8.6.1.10 VLAN Advantages

The following are a few of the advantages offered by VLANs.

##### Traffic Domain Isolation

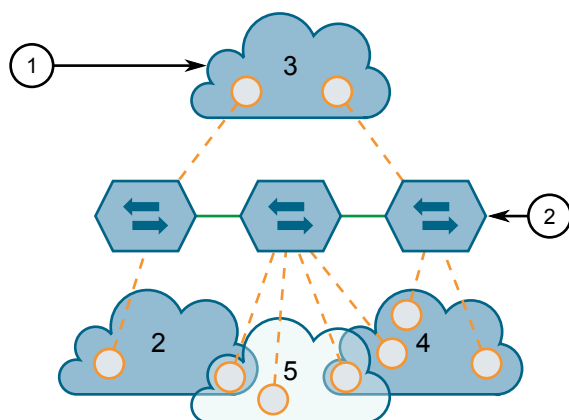
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

Unnecessary broadcast traffic can be restricted to the VLAN that requires it. Broadcast storms in one VLAN need not affect users in other VLANs.

Hosts on one VLAN can be prevented from accidentally or deliberately assuming the IP address of a host on another VLAN.

The use of creative bridge filtering and multiple VLANs can carve seemingly unified IP subnets into multiple regions policed by different security/access policies.

Multi-VLAN hosts can assign different traffic types to different VLANs.



- ① VLAN
- ② Switch

Figure 8.5 Multiple Overlapping VLANs

### Administrative Convenience

VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

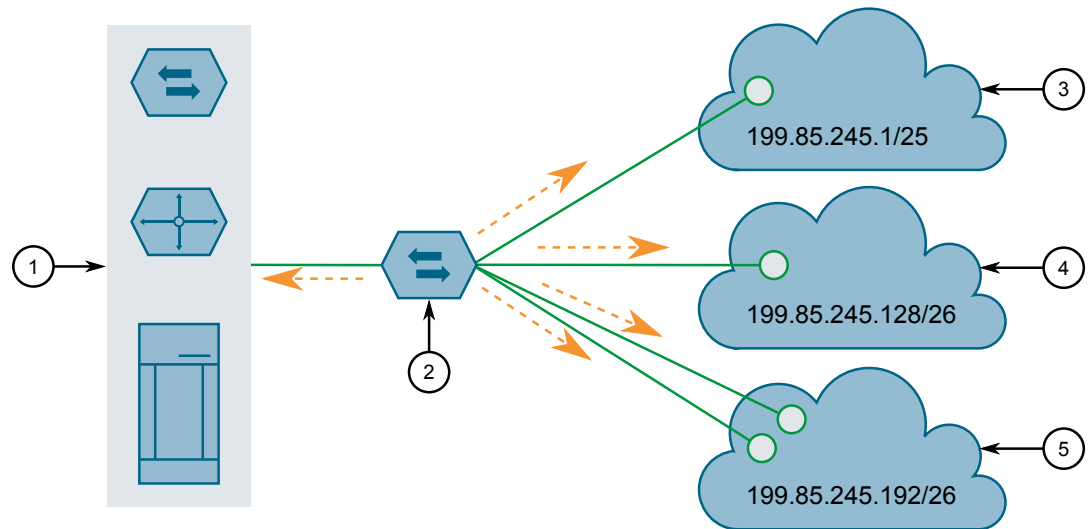
### Reduced Hardware

Without VLANs, traffic domain isolation requires the use of separate bridges for separate networks. VLANs eliminate the need for separate bridges.

The number of network hosts may often be reduced. Often, a server is assigned to provide services for independent networks. These hosts may be replaced by a single, multi-horned host supporting each network on its own VLAN. This host can perform routing between VLANs.

Multi-VLAN hosts can assign different traffic types to different VLANs.





- ① Server, Router or Layer 3 Switch
- ② Switch
- ③ VLAN 2
- ④ VLAN 3
- ⑤ VLAN 4

Figure 8.6 Inter-VLAN Communications

## 8.6.2 Configuring the Internal VLAN Range

RUGGEDCOM ROX II creates and utilizes internal VLANs for internal functions. To provide RUGGEDCOM ROX II with a pool of VLAN IDs to pull from when creating internal VLANs, a range of VLAN IDs must be reserved.

### ⚠ NOTICE

#### Configuration hazard – risk of data loss

If the range-start or range-end values are changed in a way that invalidates any configured internal VLANs, the configurations defined for the affected VLANs will be lost upon repositioning.

#### Note

VLAN IDs reserved for internal VLANs should not be used by the network.

#### Note

Changing the **End of Range** value repositions the matching serial VLAN. However, the matching serial VLAN is not affected when the **Start of Range** value is changed.

**Note**

If no internal VLANs are available when a switched Ethernet or trunk port is configured, the range is automatically extended so a unique value can be assigned.

**Note**

Routable Ethernet ports and trunks cannot be configured if internal VLANs are not enabled.

To configure the internal VLAN range, do the following:

1. Navigate to the **General** tab under **Layer 2 » VLANs**.
2. Under Internal VLAN Range, configure the following parameters:

**Note**

By default, internal VLAN ranges are enabled whenever a serial module is detected, and are disabled otherwise.

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables the Internal VLAN Range settings.</p>
Start of Range	<p><b>Synopsis:</b> An integer between 2 and 4094</p> <p><b>Default:</b> 4094</p> <p>Defines the lower end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.</p>
End of Range	<p><b>Synopsis:</b> An integer between 2 and 4094</p> <p><b>Default:</b> 4094</p> <p>Defines the higher end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.</p>

3. Commit the changes.

### 8.6.3 Enabling/Disabling Ingress Filtering

When ingress filtering is enabled, any tagged packet arriving at a port, which is not a member of a VLAN with which that packet is associated, is dropped. When disabled, packets are not dropped.

To enable or disable ingress filtering, do the following:

1. Navigate to the **General** tab under **Layer 2 » VLANs**.
2. Under **Ingress-Filtering**, click **Enabled** to enable ingress filtering, or clear **Enabled** to disable ingress filtering.

3. Commit the change.

## 8.6.4 Managing VLANs for Switched Ethernet Ports

This section describes how to configure and manage VLANs assigned to switched Ethernet ports.

### 8.6.4.1 Viewing VLAN Assignments for Switched Ethernet Ports

To determine which VLANs are assigned to each switched Ethernet port, navigate to the **VLAN Summary** page under **Layer 2 » VLANs**. A list appears.

The VLANs listed are based on the PVIDs assigned to the switched Ethernet ports. For more information about assigning PVIDs to switched Ethernet Ports, refer to "Configuring a Switched Ethernet Port" (Page 276).

### 8.6.4.2 Configuring VLANs for Switched Ethernet Ports

When a VLAN ID is assigned to a switched Ethernet port, the VLAN appears in the All-VLANs Table where it can be further configured.

To configure a VLAN for a switched Ethernet port, do the following:

1. Navigate to **Interface » VLAN Interfaces**.
2. Select a VLAN ID, and then configure the following parameter(s) as required:

Parameter	Description
IP Address Source	<p><b>Synopsis:</b> [ static   dynamic ]</p> <p>Whether the IP address is static or dynamically assigned via Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP). The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.</p>
IPv6 Address Source	<p><b>Synopsis:</b> [ static   dynamic ]</p> <p><b>Default:</b> static</p> <p>Whether the IPv6 address is static or dynamically assigned via Dynamic Host Configuration Protocol (DHCP). This must be static for non-management interfaces.</p>
Proxy ARP	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself.
On Demand	Brings up this interface on demand only.

Parameter	Description
MTU	<p><b>Synopsis:</b> An integer between 68 and 9216</p> <p><b>Default:</b> 1500</p> <p>Maximum transmission unit (largest packet size allowed for this interface).</p>

3. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to "Adding a QoS Map" (Page 743).
4. Commit the changes.

## 8.6.5 Managing Static VLANs

This section describes how to configure and manage static VLANs.

### 8.6.5.1 Viewing a List of Static VLANs

To view a list of static VLANs, navigate to the **Static VLAN** page under **Layer 2 » VLANs**. If static VLANs have been configured, a list appears.

If no static VLANs have been configured, add static VLANs as needed. For more information, refer to "Adding a Static VLAN" (Page 321).

### 8.6.5.2 Adding a Static VLAN

To add a static VLAN for either a routable Ethernet port or virtual switch, do the following:

1. Navigate to the **Static VLAN** page under **Layer 2 » VLANs**.
2. Click **Add Entry**, and then configure the following parameter(s) as required:

#### Note

The VLAN ID must be outside the internal VLAN range. For more information about configuring the internal VLAN range, refer to "Configuring the Internal VLAN Range" (Page 318).

Parameter	Description
VLAN ID	<p><b>Synopsis:</b> An integer between 1 and 4094</p> <p>The VLAN identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.</p>

3. Click **OK** to create the new static VLAN. A dialog box appears.
4. Configure the following parameter(s) as required:

**Note**

If **IGMP Snooping** is not enabled for the VLAN, both IGMP messages and multicast streams will be forwarded directly to all members of the VLAN. If any one member of the VLAN joins a multicast group, then all members of the VLAN will receive the multicast traffic.

Parameter	Description
IGMP Snooping	Enables or disables IGMP Snooping on the VLAN.
MSTI	<p><b>Synopsis:</b> [ cst ] or An integer between 1 and 16</p> <p><b>Default:</b> cst</p> <p>Only valid for Multiple Spanning Tree Protocol (MSTP) and has no effect, if MSTP is not used. The parameter specifies the Multiple Spanning Tree Instance (MSTI) the VLAN should be mapped to.</p>

5. If needed, configure a forbidden ports list. For more information, refer to "Adding a Forbidden Port" (Page 323).
6. Configure the VLAN. For more information, refer to "Configuring VLANs for Switched Ethernet Ports" (Page 320).
7. Commit the changes.

### 8.6.5.3 Deleting a Static VLAN

To delete a static VLAN for either a routable Ethernet port or virtual switch, do the following:

1. Navigate to the **Static VLAN** page under **Layer 2 » VLANs**.
2. Select the static VLAN to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 8.6.6 Managing Forbidden Ports

Static VLANs can be configured to exclude ports from membership in the VLAN using the forbidden ports list.

### 8.6.6.1 Viewing a List of Forbidden Ports

To view a list of forbidden ports, navigate to the **Static VLAN** page under **Layer 2 » VLANs**. If ports have been forbidden, a list appears.

If no ports have been forbidden, add forbidden ports as needed. For more information, refer to "Adding a Forbidden Port" (Page 323).

### 8.6.6.2 Adding a Forbidden Port

To add a forbidden port, do the following:

1. Navigate to the **Static VLAN** page under **Layer 2 » VLANs**.
2. Select a static VLAN, and then select a forbidden port from the drop down list under **Forbidden Ports**.
3. Commit the changes.

### 8.6.6.3 Deleting a Forbidden Port

To delete a forbidden port, do the following:

1. Navigate to the **Static VLAN** page under **Layer 2 » VLANs**.
2. Select the forbidden port to be deleted from the drop down list under **Forbidden Ports**, and then click the **X**.
3. Commit the changes.

## 8.6.7 Managing VLANs for Interfaces and Tunnels

The following sections describes how to view, add and delete tunnels for specific interfaces and tunnels.

- "Managing VLANs for Virtual Switches" (Page 376)
- "Managing VLANs for L2TPv3 Tunnels" (Page 390)
- "Managing VLANs for Routable Ethernet Ports" (Page 102)



## Layer 3

This chapter describes the Layer 3, or Network layer, features of RUGGEDCOM ROX II. For information about specific protocols that operate on this network layer, such as RIP, refer to "Unicast and Multicast Routing" (Page 445).

### 9.1 Layer 3 Switching Concepts

This section describes some of the concepts important to the implementation of Layer 3 switching in RUGGEDCOM ROX II.

#### 9.1.1 Layer 3 Switch Forwarding Table

To route a packet with a specific destination IP address, a router needs the following information:

- **Egress interface (subnet):** this information is stored in the router's Routing Table.

---

**Note**

In a Layer 2 switched network segment, a VLAN constitutes an IP subnet.

---

- **Next-hop gateway Media Access Control (MAC) address:** this information is stored in the router's ARP Table.

---

**Note**

If the next hop is the destination subnet itself, then the destination host MAC address is required.

---

A Layer 3 Switch uses the routing information listed above and translates it into Layer 3 switching rules. These rules are known as the *Layer 3 Switch Forwarding Information Base (FIB)* or the *Layer 3 Switch Forwarding Table*. A Layer 3 switching rule is actually a set of parameters identifying a traffic flow to be switched and determining how to perform the switching.

Layer 3 switching Application-Specific Integrated Circuits (ASICs) store Layer 3 switching rules in a Ternary Content Addressable Memory (TCAM) table. Layer 3 switching rules can be statically configured or dynamically learned (also known as *auto-learned*).



## 9.1.2 Static Layer 3 Switching Rules

When creating a static route through switch management, hardware acceleration can be explicitly configured. If hardware acceleration is selected, an appropriate Layer 3 switching rule is installed in the ASIC's TCAM and never ages out.

---

**Note**

All layer 3 protocol traffic flows will be accelerated by the IP/Layer 3 switch fabric.

---

## 9.1.3 Dynamic Learning of Layer 3 Switching Rules

For static routes without hardware acceleration or for dynamic routes, Layer 3 switching rules can be dynamically learned based on software-based router and firewall decisions. For example, the Layer 3 switch can automatically decide to offload some flows from the router into the Layer 3 Forwarding Table.

---

**Note**

Only TCP, UDP, and IPsec traffic flows are accelerated by the IP/Layer switch fabric.

---

After a certain amount of traffic for the same flow is successfully routed, the Layer 3 switching ASIC begins switching the rest of the packets belonging to the same flow. A flow is unidirectional traffic between two hosts. For example, traffic flowing between ports from one host to another is considered a flow. Traffic flowing in the opposite direction between the same ports is considered a different flow.

---

**Note**

For 8G or 88G SM, the maximum number of Layer 3 switching rules is 1000 or 3000 respectively.

---

Different auto-learning methods may be used:

- **Flow-oriented learning** is when the switch uses the following information to identify a traffic flow:
  - Source IP address
  - Destination IP address
  - Protocol
  - Source TCP/UDP port
  - Destination TCP/UDP port

This learning method is more granular and requires more ASIC resources, but it provides more flexibility in firewall configuration as the rule takes the protocol and TCP/UDP port into consideration to make forwarding decisions.

- **Host-oriented learning** is when the switch uses the following information to identify a traffic flow:
  - Source IP address

- Destination IP address

This learning method provides less flexibility in firewall configuration, as the user can allow or disallow traffic between two hosts.

For unicast traffic, each flow constitutes one rule. For multicast routing, one multicast route may constitute several rules.

The Layer 3 switch continuously monitors activity (i.e the presence of traffic) for dynamically learned rules. Dynamically learned rules may be removed after a configurable time due to inactivity.

#### 9.1.4 Layer 3 Switch ARP Table

A router needs to know the destination host or next-hop gateway MAC address for it to forward a packet on the other subnet. Therefore, software maintains an Address Resolution Protocol (ARP) table that maps IP addresses to MAC addresses. The same information is also needed by the Layer 3 switching ASIC when it switches IP packets between subnets.

The destination or gateway MAC address is usually obtained through ARP. However, ARP entries can also be statically configured in the Layer 3 Switch so that they do not time out. When configuring a static ARP entry, if no value is entered for the MAC Address parameter, the address is automatically resolved through ARP and then saved statically. This is preserved across reboots of the device.

For a static Layer 3 switching rule, the destination MAC address for the rule is always resolved, and is also saved statically.

#### 9.1.5 Multicast Cross-VLAN Layer 2 Switching

Some RUGGEDCOM Layer 3 Switch models do not have full multicast Layer 3 switching capability and only support multicast cross-VLAN Layer 2 switching. Multicast cross-VLAN Layer 2 switching differs from the normal multicast Layer 3 switching in the following ways:

- Packet modification is not done. Specifically, the source MAC address and Time-To-Live (TTL) values in forwarded packets do not change.
- Separate TCAM table entries are required for each VLAN in the multicast switching rule. For example, a multicast stream ingressing VLAN 1 and egressing VLAN 2 and VLAN 3 requires three TCAM table entries.
- Supported bandwidth depends on the rule. Multicast traffic potentially has multiple egress VLANs, and the total utilized ASIC bandwidth is the ingress bandwidth multiplied by the number of ingress and egress VLANs. For example, a 256 Mbps multicast stream ingressing VLAN 1 and egressing VLANs 2 and 3 requires 768 Mbps (256 Mbps × 3) of ASIC bandwidth.

- If a multicast packet should be forwarded to multiple egress VLANs, it egresses those VLANs sequentially rather than concurrently. This means the packet will experience different latency for each egress VLAN.

### 9.1.6 Size of the Layer 3 Switch Forwarding Table

The routing table in a software router is limited only by the amount of available memory; its size can be virtually unlimited. However, the size of the TCAM in Layer 3 switching ASICs is significantly limited and may not be sufficient to accommodate all Layer 3 switching rules. If the TCAM is full and a new static rule is created, the new rule replaces some dynamically learned rule. If all of the rules in the TCAM are static, then the new static rule is rejected.

### 9.1.7 Interaction with the Firewall

If security is a concern and you use a firewall in a Layer 3 Switch, it is important to understand how the Layer 3 switch interacts with the firewall.

A software router always works in agreement with a firewall so that firewall rules are always applied. However, in a Layer 3 Switch, if a switching rule is set in the switching ASIC (for example, due to a statically configured route), the ASIC switches all the traffic matching the rule before the firewall inspects the traffic.

Layer 3 switch ASICs are somewhat limited in how switching rules can be defined. These limitations do not allow configuring arbitrary firewall rules directly in the Layer 3 switch hardware. For sophisticated firewall rules, the firewall has to be implemented in software and the Layer 3 Switch must not switch traffic that is subject to firewall processing.

Whenever a change is made to the firewall configuration, some of the dynamically learned Layer 3 switching rules might conflict with the new firewall configuration. To resolve potential conflicts, dynamically learned Layer 3 switching rules are flushed upon any changes to the firewall configuration. The dynamically learned Layer 3 switching rules then have to be re-learned while the new firewall rules are applied.

For statically configured Layer 3 switching rules, take care to avoid conflicts between Layer 3 switching and the firewall. It should be understood that static Layer 3 switching rules always take precedence. Therefore, you must thoroughly examine the switch configuration for potential conflicts with the firewall. For more information about firewalls, refer to "Managing Firewalls" (Page 195)

### 9.1.8 Layer 3 Switching Summary

The following tables summarize the Layer 3 switching configuration-based behavior in RUGGEDCOM ROX II.

For more information about configuring hardware acceleration for a specific application, refer to the following:

- For static VRF routes, refer to "Adding a Static VRF Route" (Page 575)
- For static IPv4 routes, refer to "Adding an IPv4 Static Route" (Page 585)
- For static multicast groups, refer to "Adding a Static Multicast Group" (Page 592)

## Static Routing

Auto		Static		Disabled
No HW Acceleration	HW Acceleration	No HW Acceleration	HW Acceleration	
Layer 3 switching rules are dynamically learned from software-based router and firewall decisions.	Layer 3 switching rules are added to the Layer 3 switch forwarding table. The ARP table is pre-populated. For information about verifying rules, refer to "Viewing a Static and Dynamic ARP Table Summary" (Page 333).	Packets are not hardware accelerated. No entries are found in either the Layer 3 switch forwarding or ARP tables.	An appropriate Layer 3 switching rule is installed in the ASIC's TCAM, and never ages out. ARP adjacency is also built/resolved.	Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which is not supported by the Layer 3 switching ASIC and would require software processing.

## Dynamic Routing

Auto	Static	Disabled
Layer 3 switching rules are dynamically learned from software-based router and firewall decisions. Both the L3 forwarding and ARP summary tables are built dynamically.	Packets are not hardware accelerated. No entries are found in either the Layer 3 switch forwarding or ARP tables.	Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which is not supported by the Layer 3 switching ASIC and would require software processing.

## 9.2 Configuring Layer 3 Switching

To configure Layer 3 switching, do the following:

### Note

When hardware acceleration is used, and learning mode is set to *flow-oriented*, any fragmented packets received by RUGGEDCOM ROX II will not be hardware accelerated but instead will be software routed.

If it is known there will be a significant amount of fragmented packets that require hardware acceleration, and the network setup allows it, set the learning-mode to *host-oriented*.

1. Navigate to the **Switching Parameters** tab under **Layer 3 » Switching**.
2. Configure the following parameter(s) as required:

Parameter	Description
Unicast Mode	<p><b>Synopsis:</b> [ disabled   auto   static ]</p> <p><b>Default:</b> auto</p> <ul style="list-style-type: none"> <li>• Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing.</li> <li>• Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering.</li> <li>• Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.</li> </ul>
Multicast Mode	<p><b>Synopsis:</b> [ disabled   auto   static ]</p> <p><b>Default:</b> auto</p> <ul style="list-style-type: none"> <li>• Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing.</li> <li>• Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering.</li> <li>• Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.</li> </ul>
Learn Mode	<p><b>Synopsis:</b> [ flow-oriented   host-oriented ]</p> <p><b>Default:</b> flow-oriented</p> <p>Defines how dynamically learned traffic flows are identified:</p> <ul style="list-style-type: none"> <li>• Flow-oriented: Traffic flows are identified by a 5-tuple signature:</li> </ul> <pre style="background-color: #f0f0f0; padding: 5px;"> Src IP address Dst IP address Protocol Src TCP/UDP port Dst TCP/UDP port </pre>

Parameter	Description
	<p>This mode should be used, if fine-granularity firewall filtering is configured in the device (i.e. some flows between two hosts should be forwarded, while other flows between the same two hosts should be filtered). However, this mode utilizes more Layer 3 switching ASIC resources and is not recommended if fine-granularity firewall filtering is not required.</p> <ul style="list-style-type: none"> <li>Host-oriented: Traffic flows are identified by a 2-tuple signature: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>Src IP address Dst IP address</pre> </div> </li> </ul> <p>All traffic between two IP hosts is hardware-accelerated regardless of the protocol and TCP/UDP ports. This mode potentially controls multiple flows with a single rule and hence is more efficient in utilizing Layer3 switching ASIC resources.</p>
Aging Time (sec)	<p><b>Synopsis:</b> An integer between 16 and 600</p> <p><b>Default:</b> 32</p> <p>This parameter configures the time a dynamically learned rule for a traffic flow, which has become inactive, is held before being removed from the Layer 3 switch forwarding table.</p>

3. Commit the changes.

## 9.3 Enabling/Disabling IPsec Hardware Acceleration

RUGGEDCOM ROX II supports hardware acceleration for IPsec traffic.

When enabled, the device monitors ingress traffic for any IPsec packets. After the 31st packet, any subsequent IPsec traffic is then hardware accelerated.

To enable or disable IPsec hardware acceleration, do the following:

1. Navigate to the **Switching Parameters** tab under **Layer 3 » Switching**.
2. Configure the following parameter(s) as required:

Parameter	Description
IPsec	When enabled, IPsec traffic passing through the device will be hardware accelerated.

3. Commit the changes.

## 9.4 Managing Static ARP Table Entries

This section describes how to configure and manage static ARP table entries.

### 9.4.1 Viewing a List of ARP Table Entries

To view a list of static ARP table entries, navigate to the **ARP Table** tab under **Layer 3 » Switching**. If table entries have been configured, the **ARP Table** appears.

If no ARP table entries have been configured, add static ARP table entries as needed. For more information about adding static ARP table entries, refer to "Adding a Static ARP Table Entry" (Page 332).

### 9.4.2 Adding a Static ARP Table Entry

To add a static ARP table entry, do the following:

1. Navigate to the **ARP Table** tab under **Layer 3 » Switching**.
2. Click **Add Entry**. A dialog box appears.
3. Configure the following parameters as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string The IP address of the network device the entry describes.

4. Click **OK**.
5. Configure the following parameters as required:

#### Note

Letters in MAC addresses must be lowercase.

Parameter	Description
MAC	<b>Synopsis:</b> A string up to 17 characters long <b>Default:</b> 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 The VLAN Identifier of the VLAN upon which the MAC address operates.

6. Commit the changes.

### 9.4.3 Deleting a Static ARP Table Entry

To delete a static ARP table entry, do the following:

1. Navigate to the **ARP Table** tab under **Layer 3 » Switching**.
2. Select the address to be deleted then click **Delete Entry**.

3. Commit the changes.

## 9.5 Viewing a Static and Dynamic ARP Table Summary

To view a static and dynamic ARP table summary, navigate to the **ARP Table Summary** tab under **Layer 3 » Switching**. If ARP table entries have been configured, the **ARP Table Summary** appears.

The table provides the following information:

Parameter	Description
IP Address	<b>Synopsis:</b> A string The IP address of the network device the entry describes.
MAC	<b>Synopsis:</b> A string up to 17 characters long <b>Default:</b> 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
VLAN ID	<b>Synopsis:</b> An integer The VLAN Identifier of the VLAN upon which the MAC address operates.
Static	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Whether the entry is static or dynamic. Static entries are configured as a result of management activity. Dynamic entries are automatically learned by the device and can be unlearned.
Status	<b>Synopsis:</b> [ resolved   unresolved ] <b>Default:</b> unresolved The Address Resolution Protocol (ARP) entry resolution status: <ul style="list-style-type: none"> <li>Resolved: MAC-IP address pair is resolved and operational.</li> <li>Unresolved: the device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically.</li> </ul>

## 9.6 Viewing Routing Rules

To view a list of routing rules, navigate to the **Routing Rules Summary** tab under **Layer 3 » Switching**. If any static or dynamic ARP table entries are configured, the **Routing Rules Summary** table appears.

The table provides the following information:



Parameter	Description
Rule ID	<b>Synopsis:</b> An integer between 0 and 2999 Defines the order in which rules are matched on each ingress packet. The first matched rule is applied on the packet.
Rule Type	<b>Synopsis:</b> [ multicast   unicast   invalid   hidden ] Identifies the type of the rule: unicast,multicast,invalid.
In VLAN	<b>Synopsis:</b> An integer Identifies the ingress VLAN. To match the rule, the packet's ingress VLAN must match the number.
Out VLAN	<b>Synopsis:</b> An integer Identifies the egress VLAN. The matched multicast packet is sent to the identified VLAN.
Proto	<b>Synopsis:</b> An integer The IP Encapsulated Protocol number. Unless zero is specified, the incoming packet's IP protocol must match this number.
Source	<b>Synopsis:</b> A string or [ any ] Identifies the source IP address or subnet. To match the rule, the incoming packet's source IP address must belong to the subnet.
Destination	<b>Synopsis:</b> A string or [ any ] Defines the destination IP address or subnet. To match the rule, the incoming packet's destination IP address must belong to the subnet.
Gateway	<b>Synopsis:</b> A string Defines the nexthop IP address. The matched unicast packet is sent to the identified gateway.

## 9.7 Flushing Dynamic Hardware Routing Rules

Flushing dynamic hardware routing rules removed dynamic rules from the Routing Rules Summary table.

### Note

Only dynamic rules can be flushed. Static rules, enabled by activating hardware acceleration, never age out. For more information about enabling hardware acceleration, refer to "Layer 3 Switching Concepts" (Page 325).

To flush dynamic hardware routing rules, do the following:

1. Navigate to the **Routing Rules Summary** tab under **Layer 3 » Switching**.
2. Under **Flush Dynamic Hardware Routing Rules**, click **Perform**.

## Serial Server

This chapter describes how to manage and configure the serial server, including serial ports, protocols, remote hosts and the Device Address Tables.

---

### Note

Serial server functions are dependent on the installation of a serial line module. For more information about available serial line modules, refer to one of the following catalogs:

- "RUGGEDCOM Modules Catalog" for the RUGGEDCOM RX5000 series  
<https://support.industry.siemens.com/cs/us/en/view/109748779>
  - "RUGGEDCOM Modules Catalog" for the RUGGEDCOM MX5000 series  
<https://support.industry.siemens.com/cs/us/en/view/109748778>
  - "RUGGEDCOM Modules Catalog" for the RUGGEDCOM MX5000RE series  
<https://support.industry.siemens.com/cs/us/en/view/109748780>
- 

## 10.1 Managing Serial Ports

This section describes how to configure, monitor and manage serial ports on the device.

### 10.1.1 Viewing Serial Port Statistics

To view statistics collected on the serial ports, navigate to the **Serial Port Statistics** tab under **Interface » Serial Ports**. A list appears.

The following information is provided:

Parameter	Description
Serial Port	<b>Synopsis:</b> A string between 1 and 10 characters long The name of the serial interface.
Media	<b>Synopsis:</b> A string up to 31 characters long The type of port media { RS232 RS422 RS485 }.
Speed	<b>Synopsis:</b> [ auto   1.5M   2.4M   10M   100M   1G   10G   1.776M   3.072M   7.2M   1.2K   2.4K   9.6K   19.2K   38.4K   57.6K   115.2K   230.4K   4.8K   76.8K ] The speed (in Kilobits-per-second).

## 10.1.2 Viewing Transport Connection Statistics

Parameter	Description
Protocol	<b>Synopsis:</b> A string up to 31 characters long The serial protocol assigned to this port.
Transmit Characters	<b>Synopsis:</b> An integer The number of bytes transmitted over the serial port.
Transmit Packets	<b>Synopsis:</b> An integer The number of packets transmitted over the serial port.
Receive Characters	<b>Synopsis:</b> An integer The number of bytes received by the serial port.
Receive Packets	<b>Synopsis:</b> An integer The number of packets received by the serial port.
Packet Errors	<b>Synopsis:</b> An integer The number of packet errors on this serial port.
Parity Errors	<b>Synopsis:</b> An integer The number of parity errors on this serial port.
Framing Errors	<b>Synopsis:</b> An integer The number of framing errors on this serial port.
Overrun Errors	<b>Synopsis:</b> An integer The number of overrun errors on this serial port.

## 10.1.2 Viewing Transport Connection Statistics

To view the statistics collected for all transport connections, navigate to the **Transport Connection Status** tab under *Interface » Serial Ports*.

To view the statistics collected for a specific transport connection, navigate to the **Transport Connection Status** tab under *Interface » Serial Ports*, and then select a transport connection.

These tables and forms provide the following information:

Parameter	Description
Remote TCP/UDP IP	<b>Synopsis:</b> A string up to 32 characters long The IP address of the remote serial server.
Remote TCP/UDP Port	<b>Synopsis:</b> An integer The port of the remote serial server.

Parameter	Description
Local TCP/UDP Port	<b>Synopsis:</b> An integer The local port for the incoming connection.
Transport	<b>Synopsis:</b> A string up to 8 characters long The transport protocol (UDP or TCP) for this serial port.
RX Packets	<b>Synopsis:</b> An integer The number of packets received from TCP/UDP.
TX Packets	<b>Synopsis:</b> An integer The number of packets transmitted to TCP/UDP.
Target Port	<b>Synopsis:</b> A string up to 1024 characters long The target serial port.
Status	<b>Synopsis:</b> A string up to 31 characters long The connection status of the serial port.

### 10.1.3 Viewing DNP Device Table Statistics

To view the statistics collected for DNP device tables, navigate to the **DNP Device Table Status** tab under *Interface » Serial Ports*.

The following information is provided:

Parameter	Description
Device Address	<b>Synopsis:</b> A string up to 32 characters long The DNP device address.
Remote IP	<b>Synopsis:</b> A string up to 32 characters long The IP address of the remote host that provides a connection to the this DNP device address.
Serial Port	<b>Synopsis:</b> A string up to 128 characters long The target serial port.

### 10.1.4 Restarting the Serial Server

To restart the serial server, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Under **Restart serial port server**, click **Perform**.

## 10.2 Managing Serial Port Protocols

This section describes how to configure and manage serial protocols for serial ports.

### 10.2.1 Serial Port Protocol Concepts

This section describes some of the concepts important to the implementation of serial port protocols in RUGGEDCOM ROX II.

#### 10.2.1.1 Raw Socket Applications

The raw socket protocol transports streams of characters from one serial port on the device to a specified remote IP address and port. The raw socket protocol supports TCP and UDP transport.

#### Broadcast RTU Polling

Broadcast polling allows a single host connected to the device to broadcast a polling stream to a number of remote RTUs.

The host connects through a serial port to the device. Up to 32 TCP remote RTUs may connect to the device's host-end via the network. For UDP transport, the device can send a polling stream to up to 64 remote hosts (RTUs).

Initially, the remote hosts place TCP connections to the device's host-end. The host-end in turn is configured to accept the required number of incoming TCP connections. The host connected to the device then sequentially polls each remote host. When a poll is received, the device forwards (i.e. broadcasts) it to all the remote hosts. All remote hosts will receive the request and the appropriate remote host will issue a reply. The reply is returned to the device, where it is forwarded to the host.

#### Host and Remote Roles

The raw socket protocol can either initiate or accept a TCP connection for serial encapsulation. It can establish a connection initiated from a remote host, vice versa, or bidirectionally.

Configure the device at the host-end to establish a connection with the remote host when:

- The host-end uses a port redirector that must make the connection
- The host-end is only occasionally activated and will make the connection when it becomes active
- A host-end firewall requires the connection to be made outbound

If the host-end wants to open multiple connections with the remote-ends in order to implement broadcast polling, configure the device to accept connections with the remote-ends.

Configure the device to connect from each side (host or remote) to the other if both sides support this functionality.

### Message Packetization

The serial server buffers receive characters into packets in order to improve network efficiency and demarcate messages.

The serial server uses three methods to decide when to packetize and forward the buffered characters to the network:

- packetize on a specific character
- packetize on timeout
- packetize on a full packet

If configured to packetize on a specific character, the serial server will examine each received character, packetize and forward it upon receiving the specific character. The character is usually a <CR> or an <LF> character but may be any ASCII character.

If configured to packetize on a timeout, the serial server will wait for a configurable time after receiving a character before packetizing and forwarding it. If another character arrives during the waiting interval, the timer is restarted. This method allows characters transmitted as part of an entire message to be forwarded to the network in a single packet, when the timer expires after receiving the very last character of the message. This is usually the only packetizer selected when supporting Modbus TCP communications.

Finally, the serial server will always packetize and forward on a full packet, specifically when the number of characters fills its communications buffer (1024 bytes).

#### 10.2.1.2 Modbus TCP Applications

The Modbus TCP Server application is used to transport Modbus requests and responses across IP networks. The source of the polls is a Modbus *master*, a host computer that issues the polls to a remote host (RTU) connected to the serial port of the device running the Modbus TCP Server application. The Modbus polls encapsulated in TCP packets received by the device will be forwarded to the remote host via the serial port based on the host's address defined in the RTU list. The responses from remote host are TCP encapsulated and returned to the *master* that originated the polls.

### Port Numbers

The TCP port number dedicated to Modbus use is port 502. The Modbus TCP Server application can also be configured to accept a connection on a configurable port number. This auxiliary port can be used by masters that do not support port 502.

### Retransmissions

The Server Gateway offers the ability to resend a request to a remote host should the remote host receive the request in error or the Server Gateway receives the remote host response in error.

The decision to use retransmissions, and the number to use, depends upon factors such as:

- The probability of a line failure.
- The number of remote hosts and the amount of traffic on the port.
- The cost of retransmitting the request from the server versus timing-out and retransmitting at the master. This cost is affected by the speed of the ports and of the network.

### ModBus Exception Handling

If the Server Gateway receives a request for an un-configured remote host, it will respond to the originator with a special message called an exception (type 10). A type 11 exception is returned by the server if the remote host fails to respond to requests.

Native Modbus TCP polling packages will want to receive these messages. Immediate indication of a failure can accelerate recovery sequences and reduce the need for long timeouts.

#### 10.2.1.3 DNP Applications

RUGGEDCOM ROX II supports Distributed Network Protocol (DNP) version 3.0, commonly used by utilities in process automation systems. DNP3 protocol messages specify source and destination addresses. A destination address specifies which device should process the data, and the source address specifies which device sent the message. Having both destination and source addresses satisfies at least one requirement for peer-to-peer communication since the receiver knows where to direct a response.

Each device supporting DNP must have a unique address within the collection of devices sending and receiving DNP messages.

#### Address Learning for DNP

RUGGEDCOM ROX II implements both local and remote address learning for DNP. A local Device Address Table is populated with DNP Addresses learned for local and remote DNP devices. Each DNP address is associated with either a local serial port or a remote IP address.

When a message with an unknown DNP source address is received on a local serial port, the DNP source address and serial port number are entered into the Device Address Table. When a message with an unknown DNP source address is received from the IP network, on the IP interface that is configured as the DNP learning

interface, the DNP source address and the IP address of the sender are entered into the Device Address Table.

When a message with an unknown DNP destination address is received on a local serial port, the message is sent in a UDP broadcast to the network interface configured as the DNP learning interface. When a message with an unknown DNP destination address is received from the IP network, it is sent to all local serial ports configured as DNP ports.

---

**Note**

Learned addresses are not recorded in the Device Address Table.

---

UDP transport is used during the DNP address learning phase.

An aging timer is maintained for each DNP address in the table, and is reset whenever a DNP message is sent to or received for the specified address.

This learning facility makes it possible to configure the DNP3 protocol with a minimum number of parameters: a TCP/UDP port number, a learning network interface and an aging timer.

### DNP Broadcast Messages

DNP addresses 65521 through 65535 are reserved as DNP3 broadcast addresses. RUGGEDCOM ROX II supports DNP3 broadcast messages. DNP broadcast messages received on local serial ports are transmitted to all IP Addresses in the Device Address Table (whether learned or statically configured).

When a DNP broadcast message is received from the IP network, it is transmitted on all local serial ports configured as DNP ports.

#### 10.2.1.4 MicroLok Applications

RUGGEDCOM ROX II supports both MicroLok II and MicroLok ATCS protocols, which specify source and destination addresses of MicroLok peer devices.

The destination address specifies which device should process the data, and the source address specifies which device sent the message. Each device supporting this protocol must have a unique address within the collection of devices sending and receiving messages to and from each other. Non-MicroLok packets or non-conforming data packets are discarded.

RUGGEDCOM ROX II supports the transport of MicroLok frames over both TCP and UDP.

#### MicroLok Address Format

Standard MicroLok II Peer Protocol addresses are 16-bits in length. The message format includes five main components, in the following order: message synchronization, message header, data field (optional depending on the message type), message security, and a message terminator.



MicroLok Message Components	
1. Message Synchronization/Format Character	
2. Message Header	Destination Address Field
	Source Address Field
	Send Sequence Number
	Receive Sequence Number
	Message Type (ID)
	Message Flag Field
	Timestamp (optional)
3. Data Field (optional, depending on message type)	
4. Message Security	
5. Message Terminator	

### Framing Characters

Each message begins and ends with unique framing characters that must not appear elsewhere within the transmitted message. An escape character prevents these values from being transmitted as any of the other message bytes (i.e. header, data, or security). All framing characters are in the range \$F0-\$FF, with \$F0 being the escape character.

Description	Value
Escape Character	\$F0
Undefined	\$F1-\$F3
Header Format 1 - Normal two-byte addressing	\$F4
Header Format 2 - ATCS addressing	\$F5
Termination Character	\$F6
Undefined	\$F7-\$FD
HMAC Header	\$FE
Not Available	\$FF

### MicroLok II vs ATCS Message Formats

The destination and source addresses may be specified in either the MicroLok II address format or Advanced Train Control Systems (ATCS) address format. The destination and source address must be in the same format. Within a message, the destination address is always first, followed by the source address.

A MicroLok II address is a two-byte value, with the highest byte transmitted first.

- **MicroLok II message example:**

F4 00 02 00 01 EF 57 03 00 2C 04 01 20 13 30 03 09 00 00 00 8F E1 9F 62 F6

A MicroLok ATCS address field consists of a size byte common to both addresses and two four-to-eight byte address fields.

- **ATCS message example:**  
F5 EE 78 A2 A1 A1 A1 AA A1 78 A2 A1 A1 A1 A1 67 OF 03 00 2C 04 01 20 15  
11 40 09 00 00 00 94 2B E3 1D F6

### Determining Which Message Format to Use

When configuring the MicroLok address field in RUGGEDCOM ROX II, consider checking if the serial communication is MicroLok II or ATCS first to determine if the decimal (MicroLok II) or hexadecimal (ATCS) address notation should be used.

Use the following command:

```
traceserial protocol hex
```

For more information about using CLI commands, refer to "Using the Command Line Interface" (Page 45).

In the output, if the message starts with F5 then the ATCS address notation schema is used. If the message starts with F4 then the Microlok II address notation is used.

### MicroLok over IP

When the MICROLOK II Peer Protocol is transported over an Ethernet Link, it must be physically encapsulated in a TCP or UDP transport protocol. This encapsulation may be performed by the ASTS USA Network Interface Adapter (NIA) or by a compatible terminal server device.

In this scenario RUGGEDCOM ROX II acts as the NIA to communicate between the IP network and a MicroLok hub, or between the IP network and a MicroLok device.

When a RUGGEDCOM ROX II serial interface/port is configured with MicroLok, it listens for MicroLok frames at the configured interface/port. When a MicroLok frame is received, it is parsed and validated. Source and destination MicroLok addresses are extracted from the frame. These MicroLok addresses may correspond to a destination IP address in the device address table as configured by the user. The frame is then encapsulated in an IP packet and forwarded to the destination address or target MicroLok device using the configured transport protocol.

#### 10.2.1.5 Incoming/Outgoing Serial Connections

The RUGGEDCOM RX5000/MX5000/MX5000RE supports up to 32 TCP/UDP connections per serial port, up to a total of 128 TCP/UDP connections to the serial server.

### 10.2.2 Viewing a List of Serial Port Protocols

To view a list of serial port protocols configured on the device, navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port. If protocols have been configured, a list appears.

If no serial port protocols have been configured, add protocols as needed. For more information, refer to "Adding a Serial Port Protocol" (Page 344).

### 10.2.3 Adding a Serial Port Protocol

To add a serial port protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Configure the following parameter(s) as required:

Parameter	Description
protocol	<b>Synopsis:</b> [ rawsocket   tcpmodbus   dnp   vmserial   microlok ] The protocol of the serial port.

3. If **dnp**, **tcpmodbus**, **rawsocket** or **microlok** was selected, configure the protocol.
  - For information about configuring a DNP protocol, refer to "Configuring the DNP Protocol" (Page 344).
  - For information about configuring a TCP Modbus protocol, refer to "Configuring the Modbus TCP Protocol" (Page 345).
  - For information about configuring a raw socket protocol, refer to "Configuring the Raw Socket Protocol" (Page 346).
  - For information about configuring a MicroLok protocol, refer to "Configuring the MicroLok Protocol" (Page 348).
4. Commit the changes.

### 10.2.4 Configuring the DNP Protocol

To configure the DNP protocol for a serial port, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the selected serial port configured with the DNP protocol.
2. Select the **DNP** tab.
3. Under **DNP Protocols Configuration**, configure the following parameter(s) as required:

Parameter	Description
Address Learning	<b>Synopsis:</b> A string between 1 and 15 characters long The interface to learn the RTU address from.

Parameter	Description
Aging Timer	<p><b>Synopsis:</b> An integer between 60 and 10800</p> <p><b>Default:</b> 1000</p> <p>The length of time a learned DNP device in the Device Address Table may go without any DNP communication before it is removed from the table.</p>
Max Connection	<p><b>Synopsis:</b> An integer between 1 and 32</p> <p><b>Default:</b> 1</p> <p>The maximum number of incoming DNP connections.</p>

4. Add a Device Address table. For more information about adding Device Address tables, refer to "Adding a DNP Device Address Table" (Page 349).
5. Commit the changes.

## 10.2.5 Configuring the Modbus TCP Protocol

To configure the modbus TCP protocol for a serial port, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the selected serial port configured with the modbus TCP protocol.
2. Select the **TCP Modbus** tab.
3. Under **TCP Modbus Configuration**, configure the following parameter(s) as required:

Parameter	Description
Response Timer	<p><b>Synopsis:</b> An integer between 50 and 10000</p> <p><b>Default:</b> 100</p> <p>The maximum time from the last transmitted character of the outgoing poll until the first character of the response. If the RTU does not respond in this time, the poll will have been considered failed.</p>
Pack Timer	<p><b>Synopsis:</b> An integer between 5 and 1000</p> <p><b>Default:</b> 1000</p> <p>The maximum allowable time to wait for a response to a Modbus request to complete once it has started.</p>
Turn Around	<p><b>Synopsis:</b> An integer between 0 and 1000</p> <p><b>Default:</b> 0</p> <p>The amount of delay (if any) to insert after the transmissions of Modbus broadcast messages out the serial port.</p>

## 10.2.6 Configuring the Raw Socket Protocol

Parameter	Description
Retransmit	<p><b>Synopsis:</b> An integer between 0 and 2</p> <p><b>Default:</b> 0</p> <p>The number of times to retransmit the request to the RTU before giving up.</p>
Max Connection	<p><b>Synopsis:</b> An integer between 1 and 32</p> <p><b>Default:</b> 1</p> <p>The maximum number of incoming connections.</p>
Local Port	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 502</p> <p>The alternate local TCP port number. If this field is configured, a single connection (per serial port) may be made to this alternate port number. Note that Modbus TCP uses a default local port number of 502. There is no limit imposed on the number of connections to the default TCP port.</p>
RTU List	<p><b>Synopsis:</b> A string</p> <p>The ID of the RTU(s) connected to the serial port. Specify multiple RTUs with a space (e.g. 1 2 3 4) or a comma and space (e.g. 1, 2, 3, 4). A strictly comma-separated list (e.g. 1,2,3,4) is not permitted.</p>

4. Commit the changes.

## 10.2.6 Configuring the Raw Socket Protocol

To configure the raw socket protocol for a serial port, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the selected serial port configured with the raw socket protocol.
2. Select the **Raw Socket** tab.
3. Under **Raw Socket Configuration**, configure the following parameter(s) as required:

Parameter	Description
Pack Char	<p><b>Synopsis:</b> [ off ] or An integer between 0 and 255</p> <p><b>Default:</b> off</p> <p>The numeric value of the ASCII character which will force forwarding of accumulated data to the network.</p>
Pack Timer	<p><b>Synopsis:</b> An integer between 5 and 1000</p> <p><b>Default:</b> 1000</p> <p>The delay from the last received character until when data is forwarded.</p>

Parameter	Description
Pack Size	<b>Synopsis:</b> [ max ] or An integer between 16 and 1400 <b>Default:</b> max  The maximum number of bytes received from the serial port to be forwarded.
Turn Around	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0  The amount of delay (if any) to insert between the transmissions of individual messages out the serial port.
Call Direction	<b>Synopsis:</b> [ in   out   both ] <b>Default:</b> out  Whether to accept an incoming connection, place an outgoing connection or do both.
Max Connection	<b>Synopsis:</b> An integer between 1 and 32 <b>Default:</b> 1  The maximum number of incoming connections to permit when the call direction is incoming.
Remote IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The IP address used when placing an outgoing connection.
Remote Port	<b>Synopsis:</b> An integer between 1024 and 65535  The TCP destination port used in outgoing connections.
Local IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The IP address used to establish a connection. Leaving it blank allows an incoming connection to any interface.
Local Port	<b>Synopsis:</b> An integer between 1024 and 65535  The local TCP/UDP port to use to accept incoming connections.
Transport	<b>Synopsis:</b> [ tcp   udp ] <b>Default:</b> tcp  The transport connection protocol (UDP or TCP).

4. If the transport connection protocol is set to UDP, configure one or more remote hosts for the port. For more information about adding a remote host, refer to "Adding a Remote Host" (Page 360).
5. Commit the changes.

## 10.2.7 Configuring the MicroLok Protocol

To configure the MicroLok protocol for a serial port, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the selected serial port configured with the Microlok protocol.
2. Select the **MicroLok** tab.
3. Under **MicroLok Configuration**, configure the following parameter(s) as required:

Parameter	Description
Transport	<p><b>Synopsis:</b> [ tcp   udp ]</p> <p><b>Default:</b> udp</p> <p>The network transport used to transport protocol data over an IP network.</p>
Local Port	<p><b>Synopsis:</b> An integer between 1024 and 65535</p> <p><b>Default:</b> 60000</p> <p>The local port number on which the Microlok protocol listens for UDP datagrams or TCP connections. The local port number must match the destination local and possible remote port numbers.</p>
DSCP	<p><b>Synopsis:</b> An integer between 0 and 63</p> <p><b>Default:</b> 0</p> <p>The DSCP value for Microlok traffic priority. Only egress traffic is supported.</p>

4. Add a Device Address table. For more information about adding Device Address tables, refer to "Adding a MicroLok Device Address Table" (Page 350).
5. Commit the changes.

## 10.2.8 Deleting a Serial Port Protocol

To delete a serial port protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Under **Protocol**, select the elipsis (---) in the drop down list to replace the existing protocol.
3. Commit the change.

## 10.3 Managing DNP Device Address Tables

This section describes how to manage DNP addresses in the local Device Address Table.

### 10.3.1 Viewing a List of DNP Device Address Tables

To view a list of Device Address tables configured for a serial port using the DNP protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the selected serial port configured with the DNP protocol.
2. Select the **DNP** tab. If Device Address tables have been configured, a list appears.

If no Device Address tables have been configured, add tables as needed. For more information, refer to "Adding a DNP Device Address Table" (Page 349).

### 10.3.2 Adding a DNP Device Address Table

To add a Device Address table for a serial port using the DNP protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select a serial port configured with the DNP protocol, and then select the **DNP** tab.
3. Under **DNP Device Address Table Configuration**, click **Add Entry**. A dialog box appears.
4. Configure the following parameter(s) as required:

Parameter	Description
Device Address	<b>Synopsis:</b> An integer between 1 and 65520  The local or remote DNP device address. The address may be that of a DNP device connected to a local serial port or one available via the serial port of a remote IP host.

5. Click **OK** to create the Device Address table.
6. Configure the following parameter(s) as required:

Parameter	Description
Remote IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The IP address of the remote host that provides a connection to the DNP device with the configured address. Leave this field empty to forward DNP messages that match the configured address to the local serial port.
Remote Device	Enables forwarding of DNP messages that match the device address to the remote IP.

7. Commit the changes.



### 10.3.3 Deleting a Device Address Table

To delete a Device Address table, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select a serial port configured with the DNP protocol, and then select the **DNP** tab.
3. Under **DNP Device Address Table Configuration**, select the Device Address table to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 10.4 Managing MicroLok Device Address Tables

This section describes how to manage MicroLok addresses in the local Device Address Table.

### 10.4.1 Viewing a List of MicroLok Device Address Tables

To view a list of Device Address tables configured for a serial port using the MicroLok protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the selected serial port configured with the MicroLok protocol.
2. Select the **MicroLok** tab. If Device Address tables have been configured, a list appears.

If no Device Address tables have been configured, add tables as needed. For more information, refer to "Adding a MicroLok Device Address Table" (Page 350).

### 10.4.2 Adding a MicroLok Device Address Table

To add a Device Address table for a serial port using the MicroLok protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select a serial port configured with the MicroLok protocol, and then select the **MicroLok** tab.
3. Under **MicroLok Device Address Table Configuration**, click **Add Entry**. A dialog box appears.
4. Configure the following parameter(s) as required:

## 10.4.3 Deleting a MicroLok Device Address Table

Parameter	Description
Device Address	<p><b>Synopsis:</b> An integer between 1 and 65535 or A string between 8 and 15 characters long</p> <p>An integer from 1 to 65535, or 8 to 15 hexadecimal digits from '1' to 'a'. Represents the complete Microlok address of a device, which might be either local to the ROX device or remote. A local address is one associated with a device connected to the current serial port on this device. The corresponding serial port must be configured to match this address specification. A remote address is the address of a device connected to a serial port on a remote host over an IP network. In this case, 'Remote IP Address' must also be configured.</p>

- Click **OK** to create the Device Address table.
- Configure the following parameter(s) as required:

Parameter	Description
Device Name	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>The addressed Microlok device name</p>
Device Type	<p><b>Synopsis:</b> [ local   remote ]</p> <p><b>Default:</b> local</p> <p>Specifies if this Microlok device is local to the current ROX device or remote. Default value is 'local'. 'Remote IP Address' must be configured when this is set to 'remote'.</p>
Remote IP	<p><b>Synopsis:</b> A string between 7 and 15 characters long</p> <p>The IP address of a remote host to which a device with a configured remote address is connected. This must be configured if 'Device Type' is set to 'remote'.</p>

- Commit the changes.

### 10.4.3 Deleting a MicroLok Device Address Table

To delete a Device Address table, do the following:

- Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
- Select a serial port configured with the MicroLok protocol, and then select the **MicroLok** tab.
- Under **MicroLok Device Address Table Configuration**, select the Device Address table to be deleted, and then click **Delete Entry**.
- Commit the change.

## 10.5 Managing Serial Multicast Streaming

RUGGEDCOM ROX II supports the ingress and egress of raw-socket UDP serial multicast streams.

This section describes how to configure and manage serial multicast streaming.

### 10.5.1 Understanding Serial Multicast Streaming

Serial multicast streaming allows the transport of serial data streams to individual or groups of remote hosts via the UDP protocol.

An Ethernet multicast stream consists of a multicast group IP address (e.g. 232.1.1.1), destination UDP port (e.g. 1 to 65535) and an interface.

A serial port can act as both:

- A *sink* for data coming from IP multicast streams
- A *source* of data to be transmitted to multiple IP multicast receivers

#### 10.5.1.1 Sink vs. Source Ports

A serial port can act as either a *sink* and/or *source* port:

- **Sink Port**  
A sink port is a consumer of multicast packets. It registers itself to receive multicast traffic from a known multicast group IPv4 address and destination UDP port and then forwards the traffic along the serial link. The traffic is then received by a connected third-party serial device and processed.
- **Source Port**  
A source port is a producer of multicast packets. It receives serial traffic from a connected third-party serial device and packetizes it into multicast IPv4 packets. Each packet is assigned a specific multicast group IPv4 address, destination UDP port and source UDP port.

#### 10.5.1.2 Multicast Streaming Examples

Serial multicast streaming can be deployed in multiple ways:

##### Serial Interfaces Configured as a Sink for Multicast Streams

In this configuration, the source of the multicast data comes from the Ethernet network interfaces and is transmitted to multiple sink serial devices. The advantage of this scenario is the ease of configuration on the Ethernet networking side. Instead of indicating which serial port to send to via unicast packets, the controller can send a single multicast stream to all or some connected serial devices.

### Serial Interfaces Configured as a Source for Multicast Streams

In this configuration, the source of the multicast data comes from the serial port and device side and is transmitted to multiple Ethernet interfaces over one multicast stream. The advantage of this scenario is the ease of configuration of listening devices. There will be a lesser need to keep track of IP addresses of interfaces, and listeners can be easily substituted without concern over maintaining the same IP address.

### Serial Interfaces Configured as a Source and Sink for Multicast Streams

In this configuration, the serial data is forwarded to other serial devices, with the ability to transmit to multiple Ethernet interfaces via a single multicast stream. This is an extension of the two previous examples. The advantage of this configuration is to allow one serial source device to send data to multiple receivers whether they are another serial port or a listener device over an Ethernet network.

## 10.5.2 Configuring Serial Multicast Streaming

To configure serial multicast streaming, do the following:

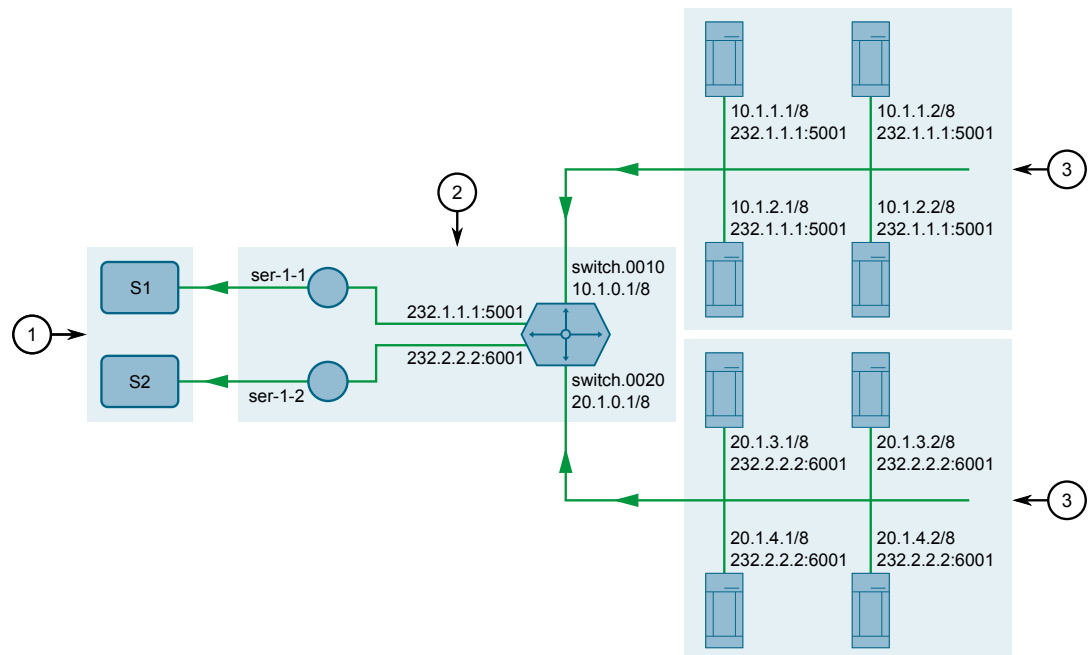
1. Configure the raw socket protocol for one or more serial ports. For more information, refer to "Adding a Serial Port Protocol" (Page 344).
2. Configure the remote host for the encapsulation of rawsocket serial over multicast with the destination multicast IP, UDP port, and interface(s). For more information, refer to "Adding a Remote Host" (Page 360) and "Adding a Remote Host Interface" (Page 363).
3. Configure the local port, local host multicast IP and local host interface(s) for the de-encapsulation of multicast stream(s) into raw socket serial. For more information, refer to "Adding a Local Host" (Page 361) and "Adding a Local Host Interface" (Page 364).
4. Verify that multicast traffic can be seen on the incoming and outgoing interface(s). For more information, refer to "Viewing Serial Port Statistics" (Page 335).

## 10.5.3 Example: Serial Interfaces Configured as a Sink for Multicast Streams

This configuration example shows multicast messages from group 232.1.1.1, directed to UDP port 5001, reaching ser-1-1 from the interface switch.0010 via raw socket connections. Ser-1-1, upon receiving these messages, passes on the data to serial device S1, to which it is directly connected.

### NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① Serial Devices
- ② Sink Device (RUGGEDCOM RX5000 Series Device)
- ③ Ethernet Network Interfaces

Figure 10.1 Topology – Serial Interfaces Configured as a Sink for Multicast Streams

### Step 1: Configure ser-1-1

1. Configure IP addresses for the interfaces (switch.0010 and switch.0020). For more information, refer to "Adding an IPv4 Address" (Page 225).
2. Create a raw socket connection for ser-1-1. For more information, refer to "Adding a Serial Port Protocol" (Page 344).
3. Set the raw socket of the local port to 5001. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
4. Set the transport method to *UDP*. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
5. Set the multicast group for the local host to 232.1.1.1. For more information, refer to "Adding a Local Host" (Page 361).
6. Set *switch.0010* as the interface for the local host. For more information, refer to "Adding a Local Host Interface" (Page 364).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
1. Create a raw socket connection for ser-1-2. For more information, refer to "Adding a Serial Port Protocol" (Page 344).

---

### 10.5.4 Example: Serial Interfaces Configured as a Source for Multicast Streams

2. Set the raw socket of the local port to 6001. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
3. Set the transport method to *UDP*. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
4. Set the multicast group for the local host to 232.2.2.2. For more information, refer to "Adding a Local Host" (Page 361).
5. Set *switch.0020* as the interface for the local host. For more information, refer to "Adding a Local Host Interface" (Page 364).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Verify the configuration by viewing the statistics collected on the serial ports. For more information, refer to "Viewing Serial Port Statistics" (Page 335).

#### Final Configuration Example

##### ser-1-1 Configuration

```
serial lml 1
no alias
protocols rawsocket
setrawsocket local-port 5001
setrawsocket transport udp
setrawsocket local-host 232.1.1.1
interface switch.0010
```

##### ser-1-2 Configuration

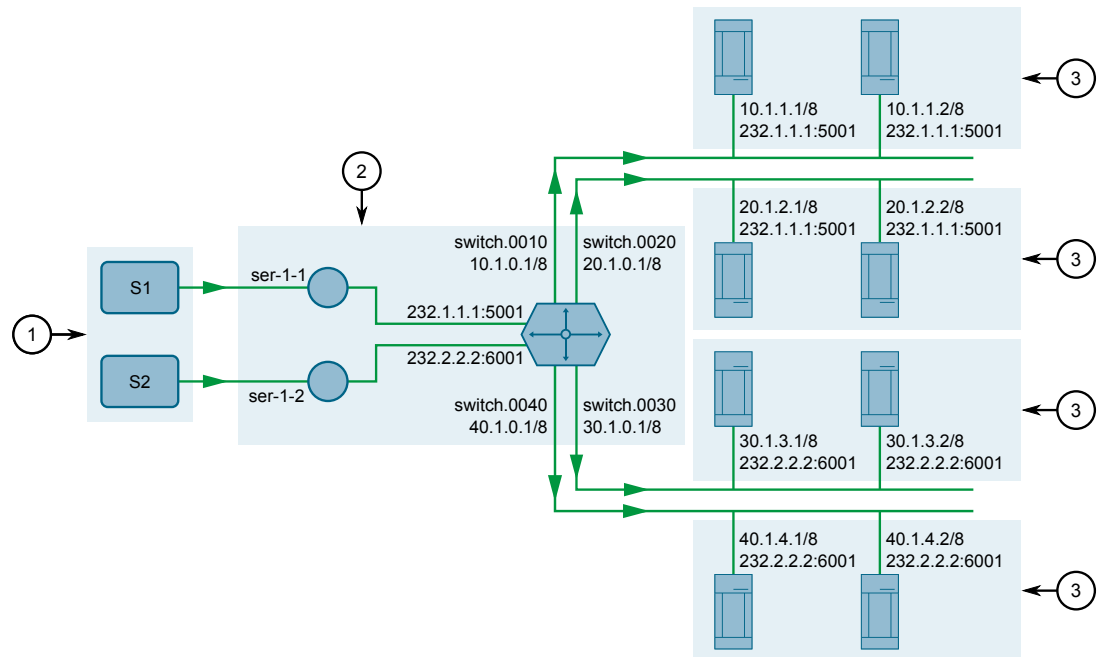
```
serial lml 2
no alias
protocols rawsocket
setrawsocket local-port 6001
setrawsocket transport udp
setrawsocket local-host 232.2.2.2
interface switch.0020
```

#### 10.5.4 Example: Serial Interfaces Configured as a Source for Multicast Streams

This configuration example shows ser-1-1 receiving data on the wire from S1, then creating multiple raw socket remote host interfaces to send the data to both interfaces switch.0010 and switch.0020. This data is then packetized as multicast packets and sent to destination group 232.1.1.1 and destination UDP port 5001.

#### NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① Serial Devices
- ② Source Device (RUGGEDCOM RX5000 Series Device)
- ③ Listeners

Figure 10.2 Topology – Serial Interfaces Configured as a Source for Multicast Streams

### Step 1: Configure ser-1-1

1. Configure IP addresses for the interfaces (switch.0010, switch.0020, switch.0030, and switch.0040). For more information, refer to "Adding an IPv4 Address" (Page 225).
2. Create a raw socket connection for ser-1-1. For more information, refer to "Adding a Serial Port Protocol" (Page 344).
3. Set the raw socket of the local port to 10001. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
4. Set the transport method to *UDP*. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
5. Set the multicast group for the remote host to 232.1.1.1 and the UDP destination port to 5001. For more information, refer to "Adding a Remote Host" (Page 360).
6. Set *switch.0010* and *switch.0020* as the interfaces for the remote host. For more information, refer to "Adding a Remote Host Interface" (Page 363).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

### 10.5.5 Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams

1. Create a raw socket connection for ser-1-2. For more information, refer to "Adding a Serial Port Protocol" (Page 344).
2. Set the raw socket of the local port to 10002. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
3. Set the transport method to *UDP*. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
4. Set the multicast group for the remote host to 232.2.2.2 and the UDP destination port to 6001. For more information, refer to "Adding a Remote Host" (Page 360).
5. Set *switch.0030* and *switch.0040* as the interfaces for the remote host. For more information, refer to "Adding a Remote Host Interface" (Page 363).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Verify the configuration by viewing the statistics collected on the serial ports. For more information, refer to "Viewing Serial Port Statistics" (Page 335).

#### Final Configuration Example

##### Serial Port 1 Configuration

```
serial lm1 1
  no alias
  protocols rawsocket
  setrawsocket local-port 10001
  setrawsocket transport udp
  setrawsocket remote-host 232.1.1.1 5001
  interface switch.0010
  !
  interface switch.0020
```

##### Serial Port 2 Configuration

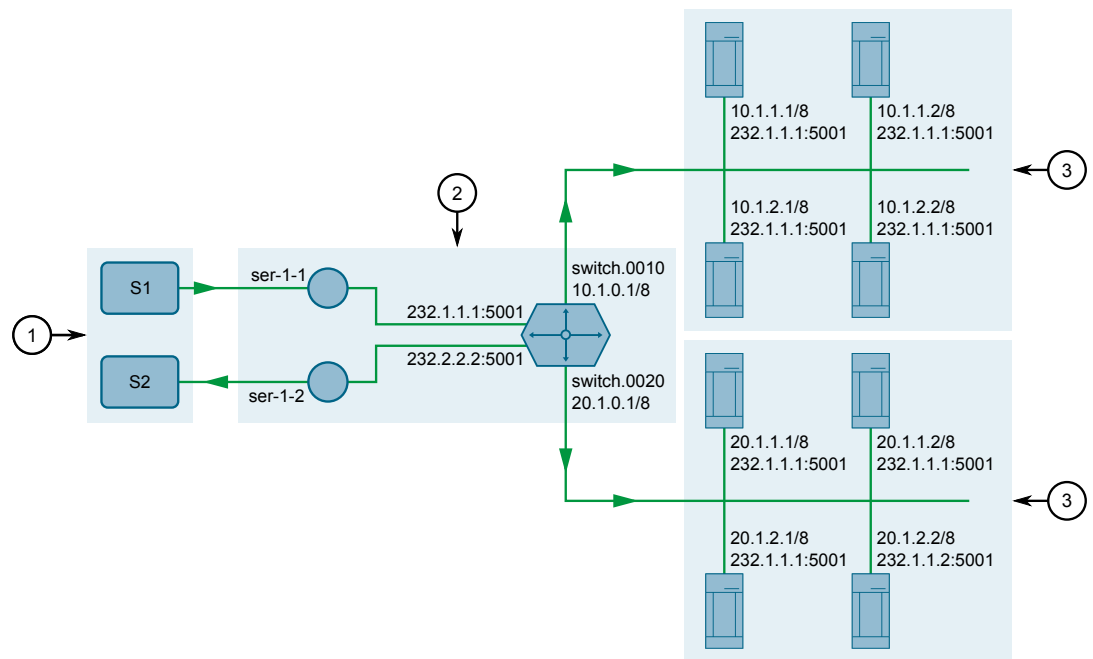
```
serial lm1 2
  no alias
  protocols rawsocket
  setrawsocket local-port 10002
  setrawsocket transport udp
  setrawsocket remote-host 232.2.2.2 6001
  interface switch.0030
  !
  interface switch.0040
```

### 10.5.5 Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams

This configuration example shows ser-1-1 receiving data on the wire from S1, then creating multiple raw socket connections to send the data to both interfaces switch.0010 and switch.0020. This data is then packetized as multicast packets and sent to destination group 232.1.1.1 and destination UDP port 5001. Additionally, ser-1-1 forwards the same data stream to ser-1-2, which then sends the data to S2.



**NOTICE**  
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① Serial Devices
- ② Source and Sink Device (RUGGEDCOM RX5000 Series Device)
- ③ Listeners
- ④ Ethernet Network Interfaces

Figure 10.3 Topology – Serial Interfaces Configured as a Source and Sink for Multicast Streams

### Configure ser-1-1 and ser-1-2

1. Configure IP addresses for the interfaces (switch.0010 and switch.0020). For more information, refer to "Adding an IPv4 Address" (Page 225).
2. Create a raw socket connection for ser-1-1. For more information, refer to "Adding a Serial Port Protocol" (Page 344).
3. Set the raw socket of the local port to 10001. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
4. Set the transport method to *UDP*. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
5. Set the multicast group for the remote host to 232.1.1.1 and the UDP destination port to 5001. For more information, refer to "Adding a Remote Host" (Page 360).

---

### 10.5.5 Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams

6. Set *switch.0010* and *switch.0020* as the interfaces for the remote host. For more information, refer to "Adding a Remote Host Interface" (Page 363).
7. Enable remote host loopback. For more information, refer to "Adding a Local Host" (Page 361).
8. Create a raw socket connection for ser-1-2. For more information, refer to "Adding a Serial Port Protocol" (Page 344).
9. Set the raw socket of the local port to 5001. This must be the same as the UDP destination port of the multicast remote host configured for ser-1-1. For more information, refer to "Adding a Local Host" (Page 361).
10. Set the transport method to *UDP*. For more information, refer to "Configuring the Raw Socket Protocol" (Page 346).
11. Set the multicast group for the local host to 232.1.1.1. This must be the same as the destination multicast group configured for the multicast remote host configured for ser-1-1. For more information, refer to "Adding a Local Host" (Page 361).
12. Enable local host loopback to indicate multicast messages are expected to arrive from another serial interface. For more information, refer to "Adding a Local Host" (Page 361).
13. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
14. Verify the configuration by viewing the statistics collected on the serial ports. For more information, refer to "Viewing Serial Port Statistics" (Page 335).

## Final Configuration Example

### Serial Port 1 Configuration

```
serial lml 1
  no alias
  protocols rawsocket
  setrawsocket local-port 10001
  setrawsocket transport udp
  setrawsocket remote-host 232.1.1.1 5001
  loopback true
  interface switch.0010
  !
  interface switch.0020
```

### Serial Port 2 Configuration

```
serial lml 2
  no alias
  protocols rawsocket
  setrawsocket local-port 5001
  setrawsocket transport udp
  setrawsocket local-host 232.1.1.1
  loopback true
```

## 10.6 Managing Remote Hosts

Remote hosts are required when the UDP transport connection protocol is selected for the raw socket protocol.

### 10.6.1 Viewing a List of Remote Hosts

To view a list of remote hosts configured for a serial port using the raw socket protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port configured with the raw socket protocol.
2. Select the **Raw Socket** tab, and then select **Remote Host**. If remote hosts have been configured, a list appears.

If no remote hosts have been configured, add hosts as needed. For more information, refer to "Adding a Remote Host" (Page 360).

### 10.6.2 Adding a Remote Host

To add a remote host for a serial port using the raw socket protocol, do the following:

---

#### Note

A maximum of two multicast remote host entries are permitted per serial interface.

---

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select a serial port configured with the raw socket protocol, and then select the **Raw Socket** tab.
3. Select **Remote Host**.
4. Click **Add Entry**. A dialog box appears.
5. Configure the following parameter(s) as required:

Parameter	Description
Remote IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The IP address of the remote host or destination multicast group.
Remote Port	<b>Synopsis:</b> An integer between 1 and 65535  The transport port of the remote host or destination multicast group.

6. Click **OK** to create the remote host.

7. [Optional] Add a remote host interface. For more information, refer to "Adding a Remote Host Interface" (Page 363).
8. Commit the changes.

### 10.6.3 Deleting a Remote Host

To delete a remote host, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select a serial port configured with the raw socket protocol, and then select the **Raw Socket** tab.
3. Select **Remote Host**.
4. Select the host to be deleted, and then click **Delete Entry**.
5. Commit the changes.

## 10.7 Managing Local Hosts

Local hosts are required when the UDP transport connection protocol is selected and multicast streams are to be received for the raw socket protocol.

### 10.7.1 Viewing a List of Local Hosts

To view a list of local hosts configured for a serial port using the raw socket protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Local Host**. If local hosts have been configured, a list appears.

If no local hosts have been configured, add hosts as needed. For more information, refer to "Adding a Local Host" (Page 361).

### 10.7.2 Adding a Local Host

To add a local host for a serial port using the raw socket protocol, do the following:

---

**Note**

A maximum of two multicast local host entries are permitted per serial interface.

---

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.

2. Select the **Raw Socket** tab, and then select **Local Host**.
3. Click **Add Entry**. A dialog box appears.
4. Configure the following parameter(s) as required:

Parameter	Description
Multicast IP	<p><b>Synopsis:</b> A string between 7 and 15 characters long</p> <p>The source multicast group IP address (2xx.xxx.xxx.xxx) of the local host. The listening UDP port for the multicast group implicitly uses the local port number defined for the serial port.</p>

5. Click **OK**.

---

#### Note

When a local host is added, either loopback must be enabled or a local host interface must be added.

---

6. If a local host interface is required, proceed to step 7 (Page 362). Otherwise, select **Loopback** to enable the local host to receive data from a loopback interface.
 

The loopback interface must have the same source multicast group IP address and local port number as the serial port. A matching remote host with loopback enabled must also be configured.
7. [Optional] Add a local host interface. For more information, refer to "Adding a Local Host Interface" (Page 364).
8. Commit the changes.

### 10.7.3 Deleting a Local Host

To delete a local host, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Local Host**.
3. Select the host to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 10.8 Managing Remote Host Interfaces

Remote host interfaces are required when the UDP transport connection protocol is selected for the raw socket protocol and when the remote host is a multicast stream.

### 10.8.1 Viewing a List of Remote Host Interfaces

To view a list of remote host interfaces configured for a serial port using the raw socket protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Remote Host**. The **Interface** column of the list indicates if interfaces have been configured.

If no remote host interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Remote Host Interface" (Page 363).

### 10.8.2 Adding a Remote Host Interface

---

#### Note

A maximum of ten interfaces are permitted for each remote host.

---

To add a remote host interface for a serial port using the raw socket protocol, do the following:

1. Make sure a remote host has been configured. For more information, refer to "Adding a Remote Host" (Page 360).
2. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
3. Select the **Raw Socket** tab, and then select **Remote Host**.
4. Select a remote host, and then select an interface from the **Interface** list.
5. Commit the changes.

### 10.8.3 Deleting a Remote Host Interface

To delete a remote host interface, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Remote Host**.
3. Select the remote host to be configured.
4. Under **Interface**, click the **X** beside the interface to be deleted.
5. Commit the change.

## 10.9 Managing Local Host Interfaces

Local host interfaces are required when the UDP transport connection protocol is selected for the raw socket protocol and when a local host is configured.

### 10.9.1 Viewing a List of Local Host Interfaces

To view a list of local host interfaces configured for a serial port using the raw socket protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Local Host**. The **Interface** column of the list indicates if interfaces have been configured.

If no local host interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Local Host Interface" (Page 364).

### 10.9.2 Adding a Local Host Interface

---

#### Note

A maximum of two interfaces are permitted for each local host.

---

To add a local host interface for a serial port using the raw socket protocol, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Local Host**.
3. Select a local host, and then select an interface from the **Interface** list.
4. Commit the changes.

### 10.9.3 Deleting a Local Host Interface

To delete a local host interface, do the following:

1. Navigate to the **Ports - { interface }** tab under **Serial Server**, where { interface } is the serial port.
2. Select the **Raw Socket** tab, and then select **Local Host**.
3. Select the remote host to be configured.
4. Under **Interface**, click the **X** beside the interface to be deleted.
5. Commit the change.

## Tunneling and VPNs

This chapter describes how to configure various tunnels and Virtual Private Networks (VPNs).

### 11.1 Configuring L2TP Tunnels

The Layer Two Tunneling Protocol (L2TP) is used primarily to tunnel Point-to-Point Protocol (PPP) packets through an IP network, although it is also capable of tunneling other Layer 2 protocols.

RUGGEDCOM ROX II utilizes L2TPD in conjunction with Libreswan and PPP to provide support for establishing a secure, private connection with the router using the Microsoft Windows VPN/L2TP client.

#### NOTICE

L2TPD listens on UDP port 1701. If a firewall is enabled, it must be configured to only allow connections to L2TPD through IPsec. Direct connections to L2TPD must be prevented.

To configure L2TP tunnels, do the following:

1. Navigate to the **L2TP** tab under **Tunnel**.
2. Under **DNS Server**, configure the following parameter(s) as required:

Parameter	Description
Primary	<b>Synopsis:</b> A string between 7 and 15 characters long The primary DNS server.
Secondary	<b>Synopsis:</b> A string between 7 and 15 characters long The secondary DNS server.

3. Under **WINS Server**, configure the following parameter(s) as required:

Parameter	Description
Primary	<b>Synopsis:</b> A string between 7 and 15 characters long The primary WINS server.
Secondary	<b>Synopsis:</b> A string between 7 and 15 characters long The secondary WINS server.

4. Under **PPP Options**, configure the following parameter(s) as required:



**Note**

If **Authorize Locally** is not enabled, L2TP will use RADIUS authentication. For more information about configuring RADIUS authentication for the PPP services, refer to "Configuring RADIUS Authentication for PPP Services" (Page 148).

Parameter	Description
Authorize Locally	Authorizes locally instead of using radius server.
MTU	<b>Synopsis:</b> An integer between 68 and 9216 <b>Default:</b> 1410 Maximum transmission unit (largest packet size allowed for this interface).
MRU	<b>Synopsis:</b> An integer between 68 and 9216 <b>Default:</b> 1410 The Maximum Receive Unit (MRU) or maximum packet size passed when received.

5. Under **L2TP**, configure the following parameter(s) as required:

Parameter	Description
Enable L2TP	Enables L2TP.
Local IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The local IP address. When set, all L2TP interfaces (l2tp-ppp-0, l2tp-ppp-1, etc.) will use the same IP address. To use different local IP addresses (chosen from an IP pool) for different L2TP interfaces, leave this parameter empty.
First IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The first address in the IP address pool. If local-ip is not set, both local and remote IP addresses will be taken from this pool.
Maximum Number of Connections	<b>Synopsis:</b> An integer between 1 and 10 The maximum number of connections.
Closing Wait Timeout	<b>Synopsis:</b> An integer between 5 and 120 <b>Default:</b> 60 The number of seconds to wait before the tunnel is cleaned up after the tunnel moves to closing-wait state.

6. Commit the changes.

## 11.2 Managing Virtual Switches

Virtual switches bridge different network segments together in a way that is independent of any particular protocol.

Network traffic between segments is forwarded regardless of the IP and MAC addresses defined in the packet. In a virtual switch, forwarding is done in Layer 2 and allows all network traffic, including Layer 2 Multicast (i.e. GOOSE, ISO), IP Multicast, Unicast and Broadcast messages, to travel through the virtual switch tunnel without any modifications.

A virtual switch can be useful, in particular, for GOOSE messaging when the sender and receiver need to communicate through a routable IP network. Since there is no IP encapsulation for the Layer 2 traffic going through the virtual switch, network latency is minimized for the traffic between end devices.

The virtual switch appears on the device as a virtual Ethernet interface over a physical interface (i.e. T1/E1 HDLC-ETH or Ethernet port) between two routers. Physically, the two routers can be in different locations.

There can be multiple virtual switch instances in a router. Each instance can include two or more interfaces, but an interface can only be a member of one virtual switch instance.

---

**Note**

There can be multiple virtual switch interfaces over a T1/E1 HDLC-ETH interface, in which the virtual switch interfaces are separated by creating a VLAN over the T1/E1 HDLC-ETH interface.

---

A virtual switch interface in a router can be a routable interface when an IP address is assigned either statically or through DHCP. The network address assigned to the virtual switch interface can be included in the dynamic routing protocol. The interface can also call a routing update. The IP address assigned to the virtual switch can be used as the default gateway for the end devices connected to the virtual switch interface. Network services, such as SSH, DHCP, NTP, VRRP, etc., can be configured to run on the virtual switch interface.

Network traffic can be filtered for select virtual switch interfaces based on destination MAC address, source MAC address, and/or protocol (e.g. iso, arp, ipv4, ipv6, etc.). If a packet meets the filter criteria, it is routed to the appropriate destination. Otherwise, it is dropped.

When configuring a virtual switch, be aware of the following:

- Be careful when adding a VLAN interface (assigned to a switch port on a given line module) in the virtual switch. The VLAN tag on a tagged frame received on the VLAN interface of a switch port may not be preserved when the traffic is egressed through a routable interface (i.e. T1/E1 HDLC-ETH or FE-CM-1), which is also part of the same virtual switch instance. However, a VLAN tag is preserved when tagged traffic is received on a routable interface.
- Any IP address assigned to an interface becomes inactive and hidden when the interface is added to the virtual switch. The address on the interface is reactivated after removing the interface from the virtual switch.
- Be careful when adding interfaces to the virtual switch. Any network services running on the individual interfaces will need to be reconfigured after adding the interface to the virtual switch. For example, if a DHCP server running on FE-

CM-1 is subsequently made a member of the VirtualSwitch vsw-1, the DHCP configuration must be changed to refer to vsw-1.

- The virtual switch is implemented in the RUGGEDCOM ROX II software. Therefore, a CPU resource is needed to forward broadcast, multicast and unicast traffic.
- If the router is running as a firewall, the **routeback** parameter under **firewall » fwconfig » fwinterface** must be enabled for the virtual switch interface. For more information, refer to "Managing Interfaces" (Page 204).

### 11.2.1 Viewing a List of Virtual Switches

To view a list of virtual switches, navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**. If virtual switches have been configured, a list appears.

If no virtual switches have been configured, add virtual switches as needed. For more information, refer to "Adding a Virtual Switch" (Page 368).

### 11.2.2 Adding a Virtual Switch

To add a virtual switch, do the following:

1. Navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string between 1 and 6 characters long</p> <p>The virtual switch interface name - the interface name must start with a lowercase letter, but may contain any combination of lowercase letters, numbers and dashes up to 6 characters. The prefix 'vsw-' will be added to this interface name.</p>

4. Click **OK** to create the new switch.
5. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables this interface.</p>

Parameter	Description
Retain IP on Bridge Device	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Retain IP on bridge device.
Forward Delay	<b>Synopsis:</b> An integer <b>Default:</b> 15 Delay (in seconds) of the listening and learning state before goes to forwarding state.
Alias	<b>Synopsis:</b> A string up to 64 characters long The SNMP alias name of the interface
IP Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
IPv6 Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IPv6 address is static or dynamically assigned via DHCPv6.
Proxy ARP	Enables/Disables whether the port will respond to ARP requests for hosts other than itself

6. Add one or more interfaces for the virtual switch. For more information, refer to "Adding a Virtual Switch Interface" (Page 370).
7. [Optional] If **IP Address Source** or **IPv6 Address Source** is set to **static**, assign an IP address to the virtual switch if required. For more information, refer to either "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).
8. [Optional] Assign one or more VLANs to the virtual switch. For more information, refer to "Adding a Virtual Switch VLAN" (Page 376).
9. Commit the changes.

### 11.2.3 Deleting a Virtual Switch

To delete a virtual switch, do the following:

1. Navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**.
2. Select the switch to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.2.4 Managing Virtual Switch Interfaces

This section describes how to configure and manage interfaces for virtual switches.

### 11.2.4.1 Viewing a List of Virtual Switch Interfaces

1. To view a list of virtual switch interfaces, navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**, and then select a virtual switch.
2. Select the **Parameters** tab, and then **Interface**. A list of available interfaces appears.

If no virtual switch interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Virtual Switch Interface" (Page 370).

### 11.2.4.2 Adding a Virtual Switch Interface

To add a virtual switch interface, do the following:

---

**Note**

At least two interfaces are required for a virtual switch bridge.

---

** NOTICE****Accessibility hazard – risk of access disruption**

Do not select the interface used to access the Web interface. Active Web sessions will be lost and the Web interface will be unreachable until the virtual switch is disabled.

---

**Note**

The *wlan-cl1* interface is not supported as a virtual switch interface.

---

1. Navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**, and then select a virtual switch.
2. Select the **Parameters** tab, and then **Interface**.
3. Select the **Enabled** check box for the desired interface.  
The new virtual switch is now visible under the **IP Interfaces** menu with the prefix *vsw-* (i.e. *vsw-vs1*, *vsw-vs2*, etc.).
4. Assign an IPv4 or IPv6 address to the interface. For more information, refer to "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).
5. If necessary, add one or more VLANs to the virtual switch interface. For more information, refer to "Adding a Virtual Switch VLAN" (Page 376).
6. Commit the changes.

### 11.2.4.3 Deleting a Virtual Switch Interface

To delete a virtual switch interface, do the following:

1. Navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**, and then select a virtual switch.
2. Select the **Parameters** tab, and then **Interface**.
3. Deselect the **Enabled** check box for the desired interface.
4. Commit the changes.

## 11.2.5 Filtering Virtual Switch Traffic

Packets traversing a virtual switch can be filtered based on source MAC address, destination MAC address, and/or protocol (e.g. iso, arp, ipv4, ipv6, etc.). Rules are defined separately and can be applied uniquely to each virtual switch as needed. For example, a single filter can detect traffic destined for a specific MAC address entering via fe-cm-1 and reroute it to switch-001. At the same time, It can also detect and drop any other type of traffic. By default, virtual switch filters drop packets unless otherwise configured.

### 11.2.5.1 Enabling/Disabling Virtual Switch Filtering

To enable or disable virtual switch filtering, do the following:

1. Navigate to the **General** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**.
2. Click **Enabled** to enable virtual switch filtering, or clear **Enabled** to disable virtual switch filtering.
3. If enabled, enable **Retain IP on Bridge Device** for the appropriate virtual switches. This feature enables/disables the switch's ability to retain an Ethernet interface's IP address when it is added to the bridge. When enabled, the IP address is retained and the router can be remotely accessed via the Ethernet interface. When disabled, the IP address must be assigned to the bridge to remotely access the router.

For more information about enabling/disabling the **Retain IP on Bridge Device** feature, refer to "Adding a Virtual Switch" (Page 368).

4. Commit the changes.

### 11.2.5.2 Viewing a List of Virtual Switch Filters

To view a list of virtual switch filters, navigate to the **Virtual Switch Table** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**. A list of available filters appears.

If no virtual switch filters have been configured, add filters as needed. For more information, refer to "Adding a Virtual Switch Filter" (Page 372).

### 11.2.5.3 Adding a Virtual Switch Filter

To add a virtual switch filter, do the following:

1. Make sure one or more virtual switches are configured and **Retain IP on Bridge Device** is enabled. For more information, refer to "Adding a Virtual Switch" (Page 368).
2. Navigate to the **Virtual Switch Table** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**.
3. Select the **Enabled** check box for the desired virtual switch filter.
4. Configure one or more rules to be used when filtering. For more information, refer to "Adding a Rule" (Page 373).
5. Add the desired rules to the virtual switch filter. For more information, refer to "Adding a Rule to a Virtual Switch Filter" (Page 374).
6. Commit the changes.

### 11.2.5.4 Deleting a Virtual Switch Filter

To delete a virtual switch filter, do the following:

1. Navigate to the **Virtual Switch Table** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**.
2. Deselect the **Enabled** check box for the desired virtual switch filter.
3. Commit the change.

## 11.2.6 Managing Filtering Rules

A virtual switch filter can apply one or more rules to traffic traversing a virtual switch.

### 11.2.6.1 Viewing a List of Rules

To view a list of rules that can be used by a virtual switch filter, navigate to the **Rules** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**. If rules have been configured, a list appears.

If no rules have been configured, add rules as needed. For more information, refer to "Adding a Rule" (Page 373).

### 11.2.6.2 Viewing a List of Rules Assigned to a Virtual Switch Filter

1. To view a list of rules assigned to a virtual switch filter, navigate to the **Virtual Switch - { name }** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter » Virtual Switch Table**, where { name } is the name of the virtual switch filter.

2. Enable the virtual switch, and then select the **Rule** tab. If filters have been configured, a list appears.

If no rules have been assigned, assign them as needed. For more information, refer to "Adding a Rule to a Virtual Switch Filter" (Page 374).

### 11.2.6.3 Adding a Rule

To add a rule that can be used by a virtual switch filter, do the following:

1. Navigate to the **Rules** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string up to 32 characters long Description of virtual switch rule

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ accept   drop ] <b>Default:</b> accept The action taken when an incoming frame meets the criteria.
Source MAC Address	<b>Synopsis:</b> A string up to 17 characters long The required source MAC address for incoming frames.
Destination MAC Address	<b>Synopsis:</b> A string up to 17 characters long The required destination MAC address for incoming frames.
Protocol	<b>Synopsis:</b> A string or [ iso   arp   ipv4   ipv6   goose ] The pre-defined protocol or hex-string (i.e. 0x88A2) used to create the frames.
GOOSE IED Name	<b>Synopsis:</b> A string up to 32 characters long The name of the IED device. Only applicable to the GOOSE protocol.

6. Commit the change.
7. Add the rule to a virtual switch filter. For more information, refer to "Adding a Rule to a Virtual Switch Filter" (Page 374).



#### 11.2.6.4 Adding a Rule to a Virtual Switch Filter

To add a rule to a virtual switch filter, do the following:

1. Navigate to the **Virtual Switch - { name }** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter » Virtual Switch Table**, where { name } is the name of the virtual switch filter.
2. Enable the virtual switch, and then select the **Rule** tab.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string up to 32 characters long The rule applied to traffic traversing the virtual switch.

4. Click **OK** to create the rule.
5. Select the check box under **Enable Route**.
6. Configure the in/out interfaces for the rule. For more information, refer to "Adding an In/Out Interface" (Page 375).
7. Commit the changes.

#### 11.2.6.5 Deleting a Rule

To delete a rule used to filter virtual switch traffic, do the following:

1. Navigate to the **Rules** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter**.
2. Select the rule to be deleted, and then click **Delete Entry**.
3. Commit the change.

#### 11.2.6.6 Deleting a Rule from a Virtual Switch Filter

To delete a rule from a virtual switch filter, do the following:

1. Navigate to the **Virtual Switch - { name }** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter » Virtual Switch Table**, where { name } is the name of the virtual switch filter.
2. Enable the virtual switch, and then select the **Rule** tab.
3. Select the rule to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 11.2.7 Managing In/Out Interfaces

In/out interfaces for virtual switch filters represent the interface being monitored by the filter (*in* interface) and the destination interface (*out* interface) for network traffic that meets the filter's criteria.

### 11.2.7.1 Viewing a List of In/Out Interfaces

1. To view a list of in/out interfaces that can be used by a virtual switch filter, navigate to the **Virtual Switch - { name }** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter » Virtual Switch Table**, where { name } is the name of the virtual switch filter.
2. Enable the virtual switch, and then select the **Rule** tab. If in/out interfaces have been configured, a list appears.

If no in/out interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an In/Out Interface" (Page 375).

### 11.2.7.2 Adding an In/Out Interface

To add an in/out interface that can be used by a virtual switch filter, do the following:

1. Navigate to the **Virtual Switch - { name }** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter » Virtual Switch Table**, where { name } is the name of the virtual switch filter.
2. Enable the virtual switch, and then select the **Rule** tab.
3. Click **Add Entry**.
4. Select a name from the list, and then click **OK**.
5. Under **In Interface** and/or **Out Interface**, select the interface(s) to be monitored from the list.
6. Commit the changes.

### 11.2.7.3 Deleting an In/Out Interface

To delete an in/out interface that can be used by a virtual switch filter, do the following:

1. Navigate to the **Virtual Switch - { name }** tab under **Layer 2 » Virtual Switch » Virtual Switch Filter » Virtual Switch Table**, where { name } is the name of the virtual switch filter.
2. Enable the virtual switch, and then select the **Rule** tab.
3. Under **In Interface** and/or **Out Interface**, deselect the interface(s) to be monitored from the list.
4. Commit the changes.

## 11.2.8 Managing VLANs for Virtual Switches

This section describes how to configure and manage VLANs for virtual switches.

### 11.2.8.1 Viewing a List of Virtual Switch VLANs

To view a list of virtual switch VLANs, navigate to the **VLAN Interfaces** tab under **Interface**. If VLANs have been configured, a list appears.

If no virtual switch VLANs have been configured, add VLANs as needed. For more information, refer to "Adding a Virtual Switch VLAN" (Page 376).

### 11.2.8.2 Adding a Virtual Switch VLAN

To add virtual switch VLAN, do the following:

1. Navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**, and then select a virtual switch.
2. Select the **Parameters** tab, and then **VLAN**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 VLAN ID for this routable logical interface

5. Click **OK** to create the new VLAN.
6. Configure the following parameter(s) as required:

Parameter	Description
IP Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
IPv6 Address Source	<b>Synopsis:</b> [ static   dynamic ] <b>Default:</b> static Whether the IPv6 address is static or dynamically assigned via DHCPv6

7. [Optional] Add a QoS map. For more information, refer to "Adding a QoS Map" (Page 743).
8. Commit the changes.

### 11.2.8.3 Deleting a Virtual Switch VLAN

To delete a virtual switch VLAN, do the following:

1. Navigate to the **Virtual Switch** tab under **Layer 2 » Virtual Switch » Virtual Switch Interface**, and then select a virtual switch.
2. Select the **Parameters** tab, and then **VLAN**.
3. Select the VLAN to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 11.3 Managing the Layer2 Tunnel Daemon

RUGGEDCOM ROX II is capable of extending the range of services that communicate solely via Layer 2 protocols (i.e. at the level of Ethernet) by tunneling them over routed IP networks. The Layer 2 Tunnel Daemon supports the IEC61850 GOOSE protocol as well as a generic mechanism for tunneling by Ethernet type.

### 11.3.1 Viewing Round Trip Time Statistics

The round trip time statistics reflect the measured round trip time to each remote daemon. The minimum, average, maximum and standard deviation of times is presented. Entries with a large difference between the **Transmitted** and **Received** parameters indicate potential problems.

To view the round trip time statistics, navigate to the **Round Trip Time** tab under **Tunnel » L2TunnelID » Status**.

---

#### Note

Round trip time statistics are only available when remote daemon IP addresses are configured for generic tunnels. For more information about remote daemon IP addresses, refer to "Managing Remote Daemon IP Addresses for Generic Tunnels" (Page 400).

---

This table provides the following information:


Parameter	Description
Transmitted	<b>Synopsis:</b> An integer The number of beacon frames transmitted through the tunnel.
Received	<b>Synopsis:</b> An integer The number of beacon frames received through the tunnel.
Minimum-rtt	<b>Synopsis:</b> A string up to 32 characters long The Minimum Beacon Round-Trip-Time.

11.3.2 Configuring the Layer 2 Tunnel Daemon

Parameter	Description
Average-rtt	<b>Synopsis:</b> A string up to 32 characters long The Average Beacon Round-Trip-Time.
Maximum-rtt	<b>Synopsis:</b> A string up to 32 characters long The Maximum Beacon Round-Trip-Time.
Deviation	<b>Synopsis:</b> A string up to 32 characters long The standard deviation.

11.3.2 Configuring the Layer 2 Tunnel Daemon

To configure the Layer 2 tunnel daemon, do the following:

<p> <b>NOTICE</b></p> <p>Make sure there are no traffic loops possible between the substation LAN and other LANs that could forward GOOSE frames to the LAN. Do not employ a GOOSE gateway between substations that are already connected. The GOOSE daemon issues packets to the network with a built in Time-To-Live (TTL) count that is decremented with each transmission. This prevents an infinite loop of packets, but will not prevent excessive network utilization.</p>
--

1. Navigate to the **Parameters** tab under **Tunnel » L2TunnelID**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enable L2 Tunnel Daemon	Enables the Layer 2 protocols server.
UDP Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1311 The UDP port to communicate with the other daemon.
Beacon Interval	<b>Synopsis:</b> An integer between 10 and 3600 or [ off ] <b>Default:</b> 60 The Round Trip Time (RTT) of the sent message

3. Add GOOSE or generic tunnels as required. For more information, refer to "Adding a GOOSE Tunnel" (Page 395) or "Adding a Generic Tunnel" (Page 400).
4. Commit the change.

## 11.4 Managing L2TPv3 Tunnels

L2TPv3 (Layer 2 Tunneling Protocol Version 3) provides a pseudo-wire service that encapsulates multi-protocol Layer 2 traffic over IP networks. There are no restrictions on the Layer 2 data formats that can be transmitted or received, unlike L2TP.

L2TPv3 is a simplified alternative to MPLS (Multiprotocol Label Switching) that offers improved performance (e.g. high data packet rate and low CPU consumption) over L2TP and IP networks.

Two types of L2TPv3 tunnels are available:

- **Static**  
A static L2TPv3 tunnel is a fixed connection between two Provider Edge devices (PE), where the session IDs and cookies are defined on both devices. This allows the devices to route Layer 2 traffic as soon as the session connects with the attachment circuit.
- **Dynamic**  
A dynamic L2TPv3 tunnel creates sessions based on the dynamic exchange of control messages between the PE devices to determine the type of Layer 2 traffic that needs to be routed. Session IDs and cookies are generated by the devices themselves for each session. This allows L2TPv3 to reestablish sessions automatically in the case of a network failure.

### ⚠ NOTICE

RUGGEDCOM ROX II supports a maximum of 128 tunnel sessions, which in turn support a maximum of 128 VLANs each.

### 11.4.1 L2TPv3 Tunnel Scenarios

The following illustrates some of the ways in which L2TPv3 tunnels can be implemented.

#### Basic L2TPv3 Tunnel

In the following topology, an L2TPv3 tunnel is established between routers R1 and R2 over a WAN interface. The tunnel interface is assigned an IPv4 address on both devices. Traffic routed from R1 is encapsulated in an L2TPv3 header and decapsulated by R2. The reverse is true when traffic is routed from R2.

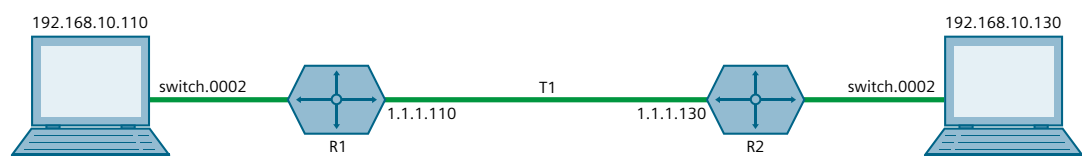


Figure 11.1 Basic L2TPv3 Tunnel

### Multiple Sessions

In the following topology, separate bridges have been created between routers R1 and R2 using sessions. Traffic sent via virtual switch switch.0002 traverses the I2t-1-1 tunnel. Traffic sent via virtual switch switch.0003 traverses the I2t-1-2 tunnel.

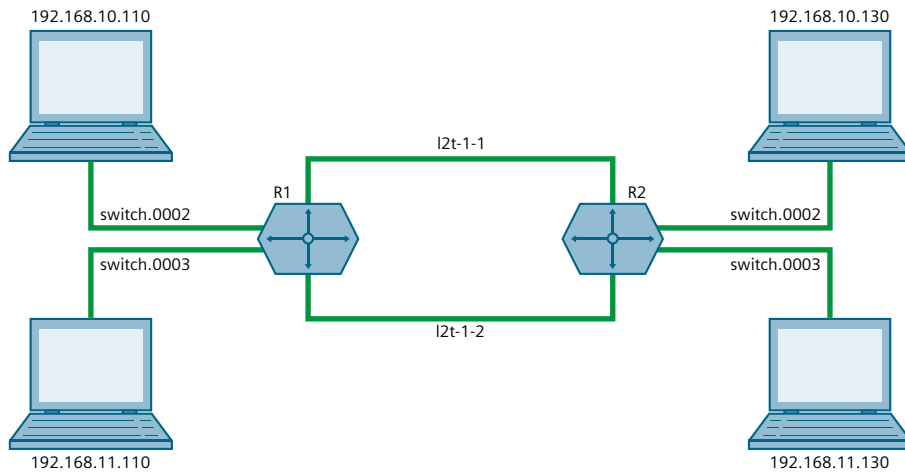


Figure 11.2 Multiple LAN Extensions Over a Single L2TPv3 Tunnel

### Multiple L2TPv3 Tunnels

In the following topology, two L2TPv3 tunnels are configured: one from router R1 to R2, and another from R1 to R3. Each is converted to a bridge by the switch.0002 virtual switch.

Traffic sent from 192.158.10.110 to 192.168.10.130 traverses the I2t-1-1 bridge, and vice versa.

Traffic sent from 192.158.10.110 to 192.168.11.110 traverses the I2t-2-1 bridge, and vice versa.

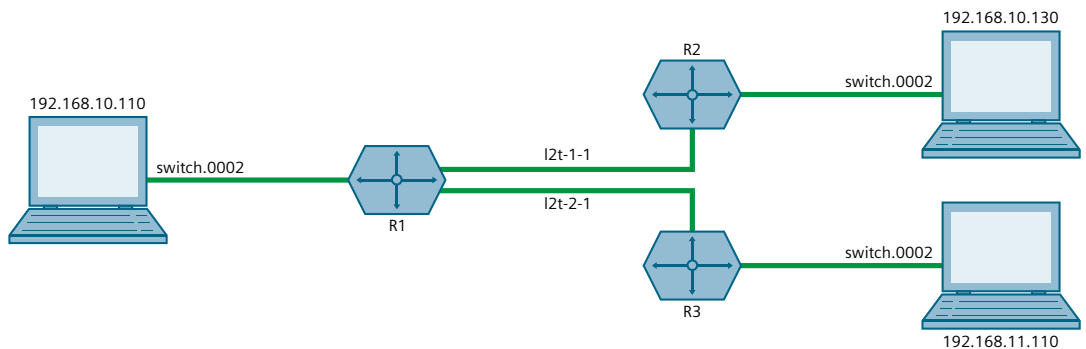


Figure 11.3 Multiple LAN Extensions Over Multiple L2TPv3 Tunnels

## 11.4.2 Creating an L2TPv3 Tunnel

To create an L2TPv3 tunnel with another Provider Edge (PE) device, do the following:

### 1. Create the L2TPv3 Tunnel Interface

An L2TPv3 tunnel interface is created automatically by RUGGEDCOM ROX II whenever a session is defined. The interface is listed under **ip** in the menu and adheres to the following naming convention:

```
l2t-{tunnel-name}-{session-name}
```

For example:

```
l2t-1-2
```

If the session is assigned a VLAN ID, an additional interface is generated in the form of:

```
l2t-{tunnel-name}-{session-name}.{vlan-id}
```

For example:

```
l2t-1-2.0004
```

To create the tunnel interface, start by adding a static or dynamic L2TPv3 tunnel. For more information, refer to either "Adding a Static L2TPv3 Tunnel" (Page 382) or "Adding a Dynamic L2TPv3 Tunnel" (Page 384).

### 2. Create a Virtual Switch or Assign an IP Address

The L2TPv3 tunnel interface is an Ethernet-like interface. As such, it can be added to a virtual switch to form a bridge, or assigned an IP address to route Layer 3 traffic.

For information about adding the L2TPv3 tunnel interface to a virtual switch, refer to "Adding a Virtual Switch Interface" (Page 370).

For information about assigning an IP address to the L2TPv3 tunnel interface, refer to either "Managing IPv4 Addresses" (Page 225) or "Managing IPv6 Addresses" (Page 226).

## 11.4.3 Managing Static L2TPv3 Tunnels

Configure static L2TPv3 tunnels to manually control tunnel and sessions parameters at both ends of the bridge. These fixed tunnels are referred to as *unmanaged*.

### 11.4.3.1 Enabling/Disabling Static L2TPv3 Tunnels

To enable or disable static L2TPv3 tunnels, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Static**.



2. Under **Static L2TPv3 Tunnels Service**, select **Enabled** to enable static L2TPv3 tunnels, or clear **Enabled** to disable static L2TPv3 tunnels.
3. Commit the change.

### 11.4.3.2 Viewing a List of Static L2TPv3 Tunnels

To view a list of static L2TPv3 tunnels, navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Static**. If tunnels have been configured, a list appears.

If no tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Static L2TPv3 Tunnel" (Page 382).

### 11.4.3.3 Adding a Static L2TPv3 Tunnel

To add a static L2TPv3 tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Static**.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Tunnel Name	<b>Synopsis:</b> A string between 1 and 3 characters long  Tunnel name, contains any lower case letter or numerical digit. Prefix 'l2t-' will be added to tunnel name and session name to create l2tpv3 system interface name (ie. l2tp-1-1)

4. Click **OK** to create the new tunnel.
5. Configure the following parameters as required:

Parameter	Description
Enabled	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true  Enables/Disables the tunnel
Tunnel ID	<b>Synopsis:</b> An integer between 1 and 65535  The local tunnel-id
Remote Tunnel ID	<b>Synopsis:</b> An integer between 1 and 65535  Tunnel-id of remote tunnel endpoint
Transport Encapsulation	<b>Synopsis:</b> [ udp   ip ] <b>Default:</b> udp  The transport protocol (UDP or IP) to encapsulate the tunnel messages

Parameter	Description
Local IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long Ip address of local interface
Local Port	<b>Synopsis:</b> An integer between 1024 and 65535 Local listening transport port for tunnel service
Remote IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long Ip address of remote tunnel endpoint
Remote Port	<b>Synopsis:</b> An integer between 1024 and 65535 The listening transport port of remote device for tunnel service

6. Add one or more sessions to the tunnel configuration. For more information, refer to either:
  - "Adding a Session for a Static L2TPv3 Tunnel" (Page 387)
  - "Adding a Session for a Dynamic L2TPv3 Tunnel" (Page 388)
7. Select **Enable** to enable the tunnel.
8. Commit the changes.

#### 11.4.3.4 Deleting a Static L2TPv3 Tunnel

To delete a static L2TPv3 tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Static**.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 11.4.4 Managing Dynamic L2TPv3 Tunnels

Configure dynamic L2TPv3 tunnels to carry Point-to-Point Protocol (PPP) traffic, as with L2TPv2, or when static L2TPv3 tunnels are not supported by the peer device. Dynamic L2TPv3 tunnels have the ability to automatically negotiate connections, and reestablish connections in the case of a network failure.

#### 11.4.4.1 Enabling and Configuring Dynamic L2TPv3 Tunnels

To enable and configure dynamic L2TPv3 tunnels, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Dynamic**.

- Under **Dynamic L2TPv3 Tunnels Service**, select **Enabled** and then configure the following parameters as required:

Parameter	Description
Mode	<b>Synopsis:</b> [ lac   lns ] <b>Default:</b> lns The l2tp operational mode
Log Level	<b>Synopsis:</b> [ none   error   warning   notice   info   all ] <b>Default:</b> none Logging message level
Log Message	<b>Synopsis:</b> [ none   protocol   fsm   api   transport   data   ppp   avp   func   system   all ] <b>Default:</b> none Logging message category

- Commit the changes.

#### 11.4.4.2 Viewing a List of Dynamic L2TPv3 Tunnels

To view a list of dynamic L2TPv3 tunnels, navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Dynamic**. If tunnels have been configured, a list appears.

If no tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Dynamic L2TPv3 Tunnel" (Page 384).

#### 11.4.4.3 Adding a Dynamic L2TPv3 Tunnel

To add a dynamic L2TPv3 tunnel, do the following:

- Navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Dynamic**.
- Click **Add Entry**.
- Configure the following parameters as required:

Parameter	Description
Tunnel Name	<b>Synopsis:</b> A string Tunnel name

- Click **OK** to create the new tunnel.
- Configure the following parameters as required:

**Note**

Transport encapsulation is only configurable when Dynamic L2TPv3 is in **lac** mode.

Parameter	Description
Enabled	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Enables/Disables the tunnel
Remote IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long Ip address of remote tunnel endpoint
Hostname	<b>Synopsis:</b> A string between 1 and 63 characters long Hostname used in AVP
Local IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long IP address of local interface that is used as Source IP address of outbound traffic over tunnel.
Transport Encap	<b>Synopsis:</b> [ udp   ip ] <b>Default:</b> udp The transport protocol (UDP or IP) to encapsulate the tunnel messages
Authentication	<b>Synopsis:</b> [ none   challenge ] <b>Default:</b> none The authentication of tunnel
Secret	<b>Synopsis:</b> A string between 1 and 63 characters long The password of tunnel negotiation
Digest	<b>Synopsis:</b> [ md5   sha1 ] <b>Default:</b> md5 Message digest AVP encryption
Interop	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 0 Specify a bitmask of flags to control non-standard behaviour for interoperability with other L2TPv3 implementation
Persist Pending Time out	<b>Synopsis:</b> An integer between 10 and 6000 <b>Default:</b> 60 The time (in seconds) that a persisting tunnel will wait in RETRY state before trying to establish itself again

Parameter	Description
Hello	<b>Synopsis:</b> An integer between 5 and 1000 <b>Default:</b> 60 timeout used for periodic L2TP Hello messages (in seconds)
Hidden	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Enables/Disabled AVP hidden
Receive Windows	<b>Synopsis:</b> An integer between 5 and 512 <b>Default:</b> 10 Received windows size
Established Timeout	<b>Synopsis:</b> An integer between 30 and 1000 <b>Default:</b> 120 The time (in seconds) that a tunnel will wait for the peer to complete the tunnel setup message exchange
Log	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Enables/Disables logging tunnel control messages
Retransmit Max Retries	<b>Synopsis:</b> An integer between 1 and 1000 <b>Default:</b> 5 The maximum number of retransmits of unacknowledged control frames
Retransmit Retry Time out	<b>Synopsis:</b> An integer between 1 and 8 <b>Default:</b> 1 The delay (in seconds) before sending the first retry of unacknowledged control frames

6. Add one or more sessions to the tunnel configuration. For more information, refer to either:
  - "Adding a Session for a Static L2TPv3 Tunnel" (Page 387)
  - "Adding a Session for a Dynamic L2TPv3 Tunnel" (Page 388)
7. Commit the changes.

#### 11.4.4.4 Deleting a Dynamic L2TPv3 Tunnel

To delete a dynamic L2TPv3 tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TPv3 » Dynamic**.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.4.5 Managing Sessions for L2TPv3 Tunnels

This section describes how to create and manage sessions for L2TPv3 tunnels. A single L2TPv3 can support up to 128 active sessions.

### 11.4.5.1 Viewing a List of Sessions

To view a list of sessions defined for an L2TPv3 tunnel, navigate to the **Session** tab under **Tunnel » L2TPv3 » Static | Dynamic » Tunnel - { name }**, where { name } is the name of the L2TPv3 tunnel. If sessions have been configured, a list appears.

If no sessions have been configured, add sessions as needed. For more information, refer to either:

- "Adding a Session for a Static L2TPv3 Tunnel" (Page 387)
- "Adding a Session for a Dynamic L2TPv3 Tunnel" (Page 388)

### 11.4.5.2 Adding a Session for a Static L2TPv3 Tunnel

To add a session to a static L2TPv3 tunnel, do the following:

1. Navigate to the **Session** tab under **Tunnel » L2TPv3 » Static » Tunnel - { name }**, where { name } is the name of the static L2TPv3 tunnel.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Session Name	<p><b>Synopsis:</b> A string between 1 and 2 characters long</p> <p>Session name, contains any lower case letter or numerical digit. Prefix 'l2t-' will be added to tunnel name and session name to create l2tpv3 system interface name (ie. l2tp-1-1)</p>

4. Click **OK** to create the new session.
5. Configure the following parameters as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables/Disables the session</p>
Local Session ID	<p><b>Synopsis:</b> An integer between 1 and 65535</p> <p>The local session-id provides the necessary context for all further packet processing</p>

Parameter	Description
Remote Session ID	<b>Synopsis:</b> An integer between 1 and 65535  The remote session-id is used to identify the received data messages from remote session endpoint
L2TP-Specific Sublayer	<b>Synopsis:</b> [ default   none ] <b>Default:</b> default  L2TP specific sublayer processing type
MTU	<b>Synopsis:</b> An integer between 68 and 9216 <b>Default:</b> 1488  Maximum transmission unit (largest packet size allowed for this interface).

6. Configure local and remote cookies. For more information, refer to "Configuring Local and Remote Cookies" (Page 389).
7. Commit the changes.

### 11.4.5.3 Adding a Session for a Dynamic L2TPv3 Tunnel

To add a session to a dynamic L2TPv3 tunnel, do the following:

1. Navigate to the **Session** tab under **Tunnel » L2TPv3 » Dynamic » Tunnel - { name }**, where { name } is the name of the dynamic L2TPv3 tunnel.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Session Name	<b>Synopsis:</b> A string between 1 and 2 characters long  Session name, contains any lower case letter or numerical digit. Prefix 'l2t-' will be added to tunnel name and session name to create l2tpv3 system interface name (ie. l2tp-1-1)

4. Click **OK** to create the new session.
5. Configure the following parameters as required:

Parameter	Description
Enabled	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true  Enables/Disables the session
Remote End ID	<b>Synopsis:</b> An integer between 1 and 65535  Remote endpoint ID to identify session with remote system

Parameter	Description
L2TP-Specific Sub Layer	<b>Synopsis:</b> [ default   none ] <b>Default:</b> default L2TP specific sublayer processing type
MTU	<b>Synopsis:</b> An integer between 68 and 9216 <b>Default:</b> 1488 Maximum transmission unit (largest packet size allowed for this interface).
Log	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Enables/Disables logging session control messages

- Configure local and remote cookies. For more information, refer to "Configuring Local and Remote Cookies" (Page 389).
- Commit the changes.

#### 11.4.5.4 Configuring Local and Remote Cookies

To configure local and remote cookies for static and dynamic L2TPv3 tunnels, do the following:

##### NOTICE

Configuration of the local cookie should match the configuration of the remote cookie on the device at the other end of the L2TPv3 tunnel.

Configuration of the remote cookie should match the configuration of the local cookie on the device at the other end of the L2TPv3 tunnel.

- Navigate to the **Session** tab under **Tunnel » L2TPv3 » { tunnel-type } » Tunnel - { name }**, where { tunnel-type } is the tunnel type (static or dynamic) and { name } is the name of the static L2TPv3 tunnel.
- Select a session and then select the **Session** tab.
- Under **Cookie**, configure the following parameters as required:

Parameter	Description
Local Cookie Size	<b>Synopsis:</b> [ 4   8 ] Cookie size in byte.
Local Cookie Low Value	<b>Synopsis:</b> An integer Lower value of cookie. This value must match with low-value of other endpoint's remote cookie



Parameter	Description
Local Cookie High Value	<b>Synopsis:</b> An integer Higher value of cookie if the cookie size is 8. This value must match with high-value of other endpoint's remote cookie
Remote Cookie Size	<b>Synopsis:</b> [ 4   8 ] Cookie size in byte
Remote Cookie Low Value	<b>Synopsis:</b> An integer Lower value of cookie. This value must match with low-value of other endpoint's local cookie
Remote Cookie High Value	<b>Synopsis:</b> An integer Higher value of cookie if its size is 8. This value must match with high-value of other endpoint's local cookie

4. Commit the changes.

#### 11.4.5.5 Deleting a Session

To delete a session for a static or dynamic L2TPv3 tunnel, do the following:

1. Navigate to the **Session** tab under **Tunnel » L2TPv3 » Static | Dynamic » Tunnel - { name }**, where { name } is the name of the L2TPv3 tunnel.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 11.4.6 Managing VLANs for L2TPv3 Tunnels

This section describes how to manage VLANs for L2TPv3 tunnel sessions. Each session supports up to 128 VLAN memberships.

#### 11.4.6.1 Viewing a List of VLANs

To view a list of the VLANs configured for a static or dynamic L2TPv3 tunnel session, navigate to the **VLAN** tab under **Tunnel » L2TPv3 » Static | Dynamic » Tunnel » { name } » Session » { session }**, where { name } is the name of the L2TPv3 tunnel and { session } is the name of the tunnel session.

If no VLANs have been configured, add VLANs as needed. For more information, refer to "Adding a VLAN" (Page 391).

### 11.4.6.2 Adding a VLAN

To add a VLAN to a static or dynamic L2TPv3 tunnel session, do the following:

1. Navigate to the **VLAN** tab under **Tunnel » L2TPv3 » Static | Dynamic » Tunnel » { name } » Session » { session }**, where { name } is the name of the L2TPv3 tunnel and { session } is the name of the tunnel session.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer Vlan id

4. Click **OK** to create the new VLAN.
5. Commit the change.

### 11.4.6.3 Deleting a VLAN

To delete a VLAN for a static or dynamic L2TPv3 tunnel session, do the following:

1. Navigate to the **VLAN** tab under **Tunnel » L2TPv3 » Static | Dynamic » Tunnel » { name } » Session » { session }**, where { name } is the name of the L2TPv3 tunnel and { session } is the name of the tunnel session.
2. Select the VLAN ID to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.4.7 Example: Establishing an L2TPv3 Tunnel Between Routers

In the following topology, an L2TPv3 tunnel is established between two RUGGEDCOM ROX II routers (A and B) to allow for bi-directional communication. Both routers are connected to devices that exchange GOOSE messages.

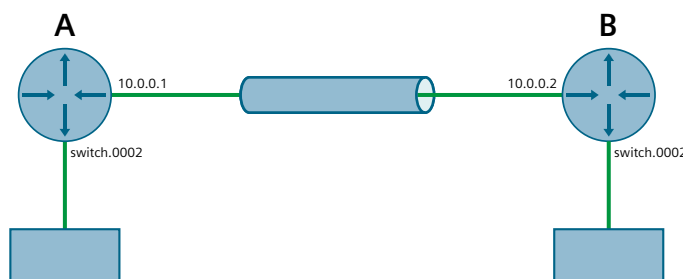


Figure 11.4 L2TPv3 Tunnel Between Routers

**Note**

GOOSE tunnels are established between two routable interfaces connected either directly or through multiple hops. The interface on either end of the tunnel can be a WAN interface (T1/E1), a cellular modem interface, or an Ethernet interface. For the purpose of this example, an Ethernet interface is used.

To replicate this configuration, do the following:

- **Configuring Router A**

1. Select a switched Ethernet port and disable switchport mode to make it routable. This will be the port that connects to router B via the L2TPv3 tunnel. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276).

When switch port mode is disabled, an interface labeled fe-{ port } (e.g. fe-1) is created under **ip**.

2. Assign the IP address **10.0.0.1/16** to the routable Ethernet port. For more information, refer to "Adding an IPv4 Address" (Page 225).
3. Select a second switched Ethernet port and assign it to VLAN 2. This will be the port that connects to the host.

Once the change is committed, the VLAN interface switch.0002 is available under **ip**, if it did not exist previously. For more information about assigning an Ethernet port to a VLAN, refer to "Configuring VLANs for Switched Ethernet Ports" (Page 320).

4. Add a static L2TPv3 tunnel with the following settings:

<b>name</b>	tunnel1
<b>tunnel-id</b>	1
<b>remote-tunnel-id</b>	1
<b>local-ip</b>	10.0.0.1
<b>local-port</b>	5000
<b>remote-ip</b>	10.0.0.2
<b>remote-port</b>	5001

For more information about adding a static L2TPv3 tunnel, refer to "Adding a Static L2TPv3 Tunnel" (Page 382).

5. Add a session to the new static tunnel with the following settings:

<b>name</b>	session1
<b>local-session-id</b>	1
<b>remote-session-id</b>	1

Once the change is committed, the interface l2t-1-1 is available under **ip**. For more information about adding a session, refer to "Adding a Session for a Static L2TPv3 Tunnel" (Page 387).

6. Combine the VLAN interface switch.0002 and the L2TPv3 session interface l2t-1-1 into a virtual switch. Once the change is committed, the interface vsw-1 is available under **ip**.

- **Configuring Router B**

1. Select a switched Ethernet port and disable switchport mode. This will be the port that connects to router A via the L2TPv3 tunnel. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276).
2. Assign the IP address **10.0.0.2/16** to the interface for the switched Ethernet port. For more information, refer to "Adding an IPv4 Address" (Page 225).
3. Select a second switched Ethernet port and assign it to VLAN 2. This will be the port that connects to the host.

Once the change is committed, the VLAN interface switch.0002 is available under **ip**, if it did not exist previously. For more information about assigning an Ethernet port to a VLAN, refer to "Configuring VLANs for Switched Ethernet Ports" (Page 320).

4. Add a static L2TPv3 tunnel with the following settings:

<b>name</b>	tunnel1
<b>tunnel-id</b>	1
<b>remote-tunnel-id</b>	1
<b>local-ip</b>	10.0.0.2
<b>local-port</b>	5001
<b>remote-ip</b>	10.0.0.1
<b>remote-port</b>	5000

For more information about adding a static L2TPv3 tunnel, refer to "Adding a Static L2TPv3 Tunnel" (Page 382).

5. Add a session to the new static tunnel with the following settings:

<b>name</b>	session1
<b>local-session-id</b>	1
<b>remote-session-id</b>	1

Once the change is committed, the interface l2t-1-1 is available under **ip**. For more information about adding a session, refer to "Adding a Session for a Static L2TPv3 Tunnel" (Page 387).

6. Combine the VLAN interface switch.0002 and the L2TPv3 session interface l2t-1-1 into a virtual switch. Once the change is committed, the interface vsw-1 is available under **IP**.

## 11.5 Managing GOOSE Tunnels

The GOOSE tunnel feature provides the capability to bridge GOOSE frames over a Wide Area Network (WAN).

GOOSE tunnels provide the following features:

- GOOSE traffic is bridged over the WAN via UDP/IP.
- One GOOSE traffic source can be mapped to multiple remote router Ethernet interfaces in mesh fashion.
- To reduce bandwidth consumption, GOOSE daemons may be located at each of the *legs* and at the center of a star network. The centrally located daemon will accept GOOSE packets and re-distribute them.
- Statistics report availability of remote GOOSE daemons, packet counts and Round Trip Time (RTT) for each remote daemon.
- When the Virtual Router Redundancy Protocol (VRRP) is employed, GOOSE transport is improved by sending redundant GOOSE packets from each VRRP gateway.
- You can enable GOOSE forwarding by configuring a generic Layer 2 tunnel. When configured, the device listens for GOOSE packets on one VLAN and forwards them to another VLAN.

The GOOSE protocol is supported by the Layer 2 Tunnel Daemon. The daemon listens to configured Ethernet interfaces and to the network itself (i.e. for tunnel connections from other daemon instances) on a configurable UDP port.

The Media Access Control (MAC) destination address of frames received from Ethernet is inspected in order to determine which GOOSE group they are in. The frames are then encapsulated in network headers and forwarded (with MAC source and destination addresses intact) to the network as GOOSE packets.

IEC61850 recommends that the MAC destination address should be in the range 01:0c:cd:01:00:00 to 01:0c:cd:01:01:ff.

GOOSE packets received from the network are stripped of their network headers and forwarded to Ethernet ports configured for the same multicast address. The forwarded frames contain the MAC source address or the originating device, and not that of the transmitting interface. The VLAN used will be that programmed locally for the interface and may differ from the original VLAN. The frame will be transmitted with the highest 802.1p priority level (p4).

Packets received from the network will also be forwarded to any other remote daemons included in the group.

To enable forwarding for GOOSE packets, configure a generic Layer 2 tunnel to listen for GOOSE packets on one VLAN and forward them to a second VLAN. To configure the generic Layer 2 tunnel for this operation, set the following for the tunnel:

- Ethernet Interface: select the VLAN on which the GOOSE packets originate
- Ethernet Type: set as 0x88b8
- Remote Daemon: select the VLAN to which to forward the GOOSE packets

## 11.5.1 Viewing the GOOSE Tunnel Statistics

To view the GOOSE tunnel statistics, navigate to the **GOOSE** tab under **Tunnel » L2TunnelID » Status » Goose**.

This table provides the following information:

Parameter	Description
Ifname	<b>Synopsis:</b> A string between 1 and 15 characters long The name of the VLAN interface.
MAC	<b>Synopsis:</b> A string up to 17 characters long The Multicast Destination MAC Address of the Goose message.
RX-frames	<b>Synopsis:</b> An integer The number of frames received through the tunnel.
TX-Frames	<b>Synopsis:</b> An integer The number of frames transmitted through the tunnel.
RX-Chars	<b>Synopsis:</b> An integer The number of bytes received through the tunnel.
TX-Chars	<b>Synopsis:</b> An integer The number of bytes transmitted through the tunnel.
Errors	<b>Synopsis:</b> An integer The number of errors through the tunnel.

## 11.5.2 Viewing a List of GOOSE Tunnels

To view a list of GOOSE tunnels, navigate to the **TUNNEL** tab under **Tunnel » L2TunnelID » Goose**. If tunnels have been configured, a list appears.

If no GOOSE tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a GOOSE Tunnel" (Page 395).

## 11.5.3 Adding a GOOSE Tunnel

To configure a GOOSE tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TunnelID » Goose**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string up to 32 characters long Description of the GOOSE tunnel.

4. Click **OK** to create the tunnel.
5. Configure the following parameter(s) as required:

Parameter	Description
Interface	<b>Synopsis:</b> A string The interface to listen on for GOOSE frames.
Multicast MAC	<b>Synopsis:</b> A string up to 17 characters long The multicast MAC address to listen for.

6. If necessary, configure one or more remote daemons for the tunnel. For more information, refer to "Adding a Remote Daemon" (Page 397).
7. Commit the change.

## 11.5.4 Deleting a GOOSE Tunnel

To delete a GOOSE tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TunnelID » Goose**.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.5.5 Managing Remote Daemons for GOOSE Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

### 11.5.5.1 Viewing a List of Remote Daemons

To view a list of remote daemons configured for a GOOSE tunnel, navigate to the **Parameters** tab under **Tunnel » L2TunnelID » Goose » Tunnel - { name }**, where { name } is the name of the GOOSE tunnel. If remote daemons have been configured, a list appears under **Remote Daemon**.

If no remote daemons have been configured, add daemons as needed. For more information, refer to "Adding a Remote Daemon" (Page 397).

### 11.5.5.2 Adding a Remote Daemon

To configure a remote daemon for a GOOSE tunnel, do the following:

1. Navigate to the **Parameters** tab under **Tunnel » L2TunnelID » Goose » Tunnel - { name }**, where { name } is the name of the GOOSE tunnel.
2. Under **Remote Daemon**, click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The IP address of the remote Layer 2 protocol server.

4. Click **Add** to create the daemon.
5. Click **OK** to create the daemon.
6. Commit the change.

### 11.5.5.3 Deleting a Remote Daemon

To delete a remote daemon, do the following:

1. Navigate to the **Parameters** tab under **Tunnel » L2TunnelID » Goose » Tunnel - { name }**, where { name } is the name of the GOOSE tunnel.
2. Select the daemon to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.5.6 Example: Establishing a GOOSE Tunnel Between Routers

In the following topology, a GOOSE tunnel is established between two RUGGEDCOM ROX II routers (A and B) to allow for bi-directional communication. Both routers are connected to publisher/subscriber devices.

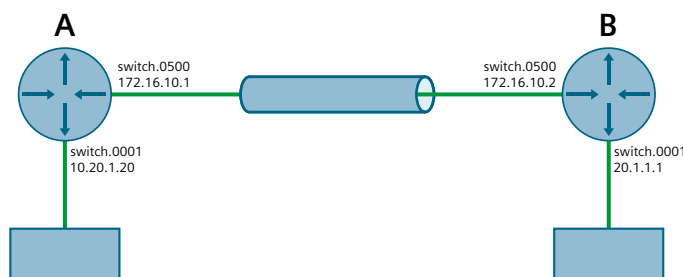


Figure 11.5 GOOSE Tunnel Between Routers

To replicate this configuration, do the following:



- **Configuring Router A**

1. Add a GOOSE tunnel for incoming traffic from the publisher/describer with the following settings:

<b>name</b>	incoming-traffic
<b>interface</b>	switch.0001
<b>multicast-mac</b>	01:0c:cd:01:00:44

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 395).

2. Add a GOOSE tunnel for outgoing traffic to router B with the following settings:

<b>name</b>	outgoing-traffic
<b>interface</b>	switch.0500
<b>multicast-mac</b>	01:0c:cd:01:00:41

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 395).

3. For the outgoing-traffic tunnel, add a remote daemon with the IP address **172.16.10.2**. For more information, refer to "Configuring the Layer 2 Tunnel Daemon" (Page 378).

- **Configuring Router B**

1. Add a GOOSE tunnel for incoming traffic from the publisher/describer with the following settings:

<b>name</b>	incoming-traffic
<b>interface</b>	switch.0001
<b>multicast-mac</b>	01:0c:cd:01:00:41

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 395).

2. Add a GOOSE tunnel for outgoing traffic to router A with the following settings:

<b>name</b>	outgoing-traffic
<b>interface</b>	switch.0500
<b>multicast-mac</b>	01:0c:cd:01:00:44

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 395).

3. For the outgoing-traffic tunnel, add a remote daemon with the IP address **172.16.10.1**. For more information, refer to "Configuring the Layer 2 Tunnel Daemon" (Page 378).

## 11.6 Managing Generic Tunnels

The Layer 2 Tunnel Daemon supports a generic mode of operation based on the Ethernet type of Layer 2 data traffic seen by the router. Multiple tunnels may be configured, each one with:

- an Ethernet type
- a tunnel ingress (Ethernet interface)
- a tunnel egress (either another locally connected Ethernet interface, or the remote IP address of another Layer 2 Tunnel daemon instance running on another Router)

### 11.6.1 Viewing the Generic Tunnel Statistics

To view the generic tunnel statistics, navigate to the **Generic** tab under **Tunnel » L2TunnelID » Status**.

This table provides the following information:

Parameter	Description
Tunnel Name	<b>Synopsis:</b> A string up to 32 characters long The generic tunnel name.
Ifname	<b>Synopsis:</b> A string between 1 and 15 characters long The name of the ingress interface.
RX-Frames	<b>Synopsis:</b> An integer The number of frames received through the tunnel.
TX-Frames	<b>Synopsis:</b> An integer The number of frames transmitted through the tunnel.
RX-Chars	<b>Synopsis:</b> An integer The number of bytes received through the tunnel.
TX-Chars	<b>Synopsis:</b> An integer The number of bytes transmitted through the tunnel.
Errors	<b>Synopsis:</b> An integer The number of errors received through the tunnel.

### 11.6.2 Viewing a List of Generic Tunnels

To view a list of generic tunnels, navigate to the **Tunnel** tab under **Tunnel » L2TunnelID » Generic**. If tunnels have been configured, a list appears.

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Generic Tunnel" (Page 400).

### 11.6.3 Adding a Generic Tunnel

To configure a generic tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TunnelID » Generic**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string up to 32 characters long A description of the generic tunnel.

4. Click **OK** to create the tunnel.
5. Configure the following parameter(s) as required:

Parameter	Description
Ingress Interface	<b>Synopsis:</b> A string The interface to listen on for Ethernet type frames.
Replace MAC	Replaces the sender's MAC with the out-interface's MAC.

6. If necessary, configure one or more remote daemon IP addresses for the tunnel. For more information, refer to "Adding an IP Address" (Page 401).
7. If necessary, define one or more Ethernet types to be forwarded. For more information, refer to "Adding an Ethernet Type" (Page 403).
8. Commit the change.

### 11.6.4 Deleting a Generic Tunnel

To delete a generic tunnel, do the following:

1. Navigate to the **Tunnel** tab under **Tunnel » L2TunnelID » Generic**.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 11.6.5 Managing Remote Daemon IP Addresses for Generic Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

**Note**

When a remote daemon IP address is configured, the interface on the receiver side, where traffic leaves, should be configured on the ingress interface (instead of egress interface).

**11.6.5.1 Viewing a List of IP Addresses**

1. To view a list of remote Layer 2 protocol server IP addresses for a generic tunnel configuration, navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
  2. Select the **Parameters** tab. If IP addresses have been configured, a list appears.
- If no generic tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Generic Tunnel" (Page 400).

**11.6.5.2 Adding an IP Address**

To add the IP address of a remote Layer 2 protocols server to a generic tunnel configuration, do the following:

1. Navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The IP address of the remote L2 protocol server.

4. Click **Add** to add the IP address.
5. Click **OK** to add the IP address.
6. Commit the change.

**11.6.5.3 Deleting an IP Address**

To delete the IP address of a remote Layer 2 protocols server from a generic tunnel configuration, do the following:

1. Navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab..
3. Select the IP address to be deleted, and then click **Delete Entry**.

4. Commit the change.

## 11.6.6 Managing Remote Daemon Egress Interfaces for Generic Tunnels

This section describes how to create and manage remote daemon egress interfaces for generic tunnels.

### 11.6.6.1 Viewing a List of Egress Interfaces

1. To view a list of egress interfaces configured for a generic tunnel, navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab. If egress interfaces have been configured, a list appears under **Remote Daemon**.

If no egress interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an Egress Interface" (Page 402).

### 11.6.6.2 Adding an Egress Interface

To add an egress interface for a generic tunnel, do the following:

1. Navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab, and then click **Add Entry** under **Remote Daemon**.
3. Configure the following parameter(s) as required:

Parameter	Description
Egress Interface	<b>Synopsis:</b> A string The egress interface for Ethernet type frames.

4. Click **OK** to add the egress interface.
5. Commit the change.

### 11.6.6.3 Deleting an Egress Interface

To delete an egress interface for a generic tunnel, do the following:

1. Navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab.
3. Under **Remote Daemon**, select the egress interface to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 11.6.7 Managing Ethernet Types for Generic Tunnels

This section describes how to define the types of Ethernet protocols that can be forwarded by generic tunnels.

### 11.6.7.1 Viewing a List of Ethernet Types

1. To view a list of Ethernet types configured for a generic tunnel, navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab. If Ethernet types have been configured, a list appears under **Ethernet Type**.

If no Ethernet types have been configured, add types as needed. For more information, refer to "Adding an Ethernet Type" (Page 403).

### 11.6.7.2 Adding an Ethernet Type

To add an Ethernet type for a generic tunnel, do the following:

1. Navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab, and then click **Add Entry** under **Ethernet Type**.
3. Configure the following parameter(s) as required:

Parameter	Description
Type	<b>Synopsis:</b> [ iso ] or A string The Ethernet type to be forwarded (ie. 0xFEFE).

4. Click **OK** to add the Ethernet type.
5. Commit the change.

### 11.6.7.3 Deleting an Ethernet Type

To delete an Ethernet type for a generic tunnel, do the following:

1. Navigate to the **Generic** tab under **Tunnel » L2TunnelID**, and then select a tunnel.
2. Select the **Parameters** tab.
3. Under **Ethernet Type**, select the Ethernet Type to be deleted and then click **Delete Entry**.
4. Commit the change.

## 11.7 Managing Generic Routing Encapsulation Tunnels

RUGGEDCOM ROX II can employ the Generic Routing Encapsulation (GRE) protocol to encapsulate multicast traffic and IPv6 packets together and transport them through an IPv4 network tunnel. As such, GRE tunnels can transport traffic through any number of intermediate networks.

The key parameters for GRE tunnels is the tunnel name, local router address, remote router address and remote subnet.

The following illustrates a typical GRE tunnel configuration:



Figure 11.6 Example – GRE Tunnel Configuration

In this example, Router 1 establishes a GRE tunnel to Router 2 using a local router address of 172.16.17.18, a remote router address of 172.19.20.21, and a remote subnet of 192.168.2.0/24.

### Note

When connecting a Cisco router (in place of Router 1 in the previous example), the local router address corresponds to the Cisco IOS *source* address and the remote router address corresponds to the *destination* address.

The cost of the GRE tunnel can also be set if another method of routing between Router 1 and Router 2 becomes available. When GRE failover is enabled, the packets will automatically flow through the lowest cost route.

Packets can also be restricted by specifying a local egress device, such as w1pp in the case of Router 1 in the previous example.

### 11.7.1 Viewing Statistics for GRE Tunnels

To view the statistics collected for GRE tunnels, navigate to the **Status** tab under **Tunnel » GRE**.

This table provides the following information:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 10 characters long The name of the GRE tunnel.

Parameter	Description
Interface Status	<p><b>Synopsis:</b> A string between 1 and 20 characters long</p> <p>The status of the GRE tunnel interface, possible values include:</p> <ul style="list-style-type: none"> <li>• <b>Active</b> - GRE tunnel interface is up;</li> <li>• <b>Inactive</b> - GRE tunnel interface is down</li> </ul>
Tunnel Status	<p><b>Synopsis:</b> A string</p> <p>The status of the GRE tunnel:</p> <ul style="list-style-type: none"> <li>• <b>Up</b> - GRE tunnel is up and running;</li> <li>• <b>Down</b> - GRE tunnel interface is inactive or tunnel remote end point is not reachable;</li> <li>• <b>Keepalives Disabled</b> - Keepalive messages have been disabled, not able to know if the tunnel remote endpoint is reachable or not</li> </ul>
RX Packets	<p><b>Synopsis:</b> An integer</p> <p>The number of packets received through the tunnel.</p>
RX Errors	<p><b>Synopsis:</b> An integer</p> <p>The error packets received through the tunnel.</p>
RX Drops	<p><b>Synopsis:</b> An integer</p> <p>The number of packets dropped by the tunnel.</p>
TX Packets	<p><b>Synopsis:</b> An integer</p> <p>The number of packets transmitted through the tunnel.</p>
TX Errors	<p><b>Synopsis:</b> An integer</p> <p>The number of error packets transmitted through the tunnel.</p>
TX Drops	<p><b>Synopsis:</b> An integer</p> <p>The number of packets dropped by the tunnel.</p>

## 11.7.2 Viewing a List of GRE Tunnels

To view a list of GRE tunnels, navigate to the **GRE** tab under **Tunnel » GRE**. If tunnels have been configured, a list appears.

If no GRE tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a GRE Tunnel" (Page 405).

## 11.7.3 Adding a GRE Tunnel

To add a GRE tunnel, do the following:

1. Navigate to the **GRE** tab under **Tunnel » GRE**.



2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string between 1 and 10 characters long</p> <p>The GRE tunnel network interface name - the interface name must start with a lowercase letter, but may contain any combination of lowercase letters, numbers and dashes up to a maximum of 10 characters. The prefix 'gre-' will be added to this interface name.</p>

4. Click **OK** to add the GRE tunnel.
5. Configure the following parameter(s) as required:

Parameter	Description
Local IP	<p><b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long</p> <p>The IP address of the local end of the tunnel.</p>
Remote IP	<p><b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long</p> <p>The IP address of the remote end of the tunnel.</p>
Remote Network	<p><b>Synopsis:</b> A string between 9 and 18 characters long or A string between 4 and 43 characters long</p> <p>The target network of remote end of the tunnel.</p>
MTU	<p><b>Synopsis:</b> An integer between 68 and 9216</p> <p><b>Default:</b> 1476</p> <p>The MTU of the GRE interface.</p>
Multicast	Enables multicast traffic on the tunnel interface.
Cost	<p><b>Synopsis:</b> An integer between 1 and 255</p> <p><b>Default:</b> 1</p> <p>The routing cost associated with networking routing that directs traffic through the tunnel.</p>
Key	<p><b>Synopsis:</b> [ none   input   output   both ]</p> <p><b>Default:</b> none</p> <p>The key for tunneled packets</p>
Key ID	<p><b>Synopsis:</b> An integer between 0 and 4294967295</p> <p><b>Default:</b> 0</p> <p>The key ID for tunneled packets</p>

Parameter	Description
Checksum	<p><b>Synopsis:</b> [ none   input   output   both ]</p> <p><b>Default:</b> none</p> <p>The checksum for tunneled packets</p>
Sequence	<p><b>Synopsis:</b> [ none   input   output   both ]</p> <p><b>Default:</b> none</p> <p>The sequence number for tunneled packets</p>
Tunnel Alarms	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables or disables tunnel up and down alarms. Disabling tunnel alarms will prevent alarms from being sent for that tunnel. GRE tunnel alarms may also be controlled for the whole system under <b>admin &gt; alarm-cfg</b>.</p>

6. [Optional] Enable keepalive messages so as to monitor the status of the tunnel's remote endpoint. For more information, refer to "Enabling/Disabling Keepalive Messages" (Page 408).
7. [Optional] Configure the method for assigning Differentiated Services Code Point (DSCP) marks to packets traveling through the GRE tunnel. For more information, refer to "Configuring a DSCP Marking for GRE Tunnel Traffic" (Page 407).

---

#### Note

An interface in the form of *gre-{ tunnel }* (e.g. gre-t1) is added automatically to the **ip** menu.

---

8. Assign an IP address to the tunnel. For more information, refer to either "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).
9. Commit the changes.

## 11.7.4 Configuring a DSCP Marking for GRE Tunnel Traffic

Each packet traversing a GRE tunnel can be assigned a Differentiated Services Code Point (DSCP) mark either defined by the device or inherited by the original IP header.

To configure how DSCP marks are assigned for a specific GRE tunnel, do the following:

1. Navigate to the **GRE** tab under **Tunnel » GRE**.
2. Select a GRE tunnel, and then select the check box under **DSCP Marking** to enable DSCP marking.
3. Under **DSCP Mark**, select one of the following options:

- **mark** – Assigns the DSCP marking set by **DSCP Mark** to packets traversing the tunnel
  - **forward** – Assigns the DSCP marking defined in the original IP header of each packet traversing the tunnel
4. If **mark** is selected, under **DSCP Mark**, select a DSCP mark to assign. Options include: **BE, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, CS1, CS2, CS3, CS4, CS5, CS6, CS7, EF**.
  5. Commit the changes.

### 11.7.5 Enabling/Disabling Keepalive Messages

Keepalive messages enable endpoints of a GRE tunnel to determine one another's current operational status.

Traditionally, GRE tunnels are stateless, meaning that remote endpoints retain no information about one another. As a result, an endpoint will not know when the other endpoint becomes unreachable and continue sending frames, even though the other end is unable to receive them.

With keepalive messages enabled, RUGGEDCOM ROX II will send keepalive messages to the other endpoint and wait for a response. If a response is not received before the next message is scheduled to be sent, it begins to count the number of consecutive messages sent that did not receive a reply. After so many failures to reply, the other endpoint is considered unreachable and a *Link Down* alarm is raised. This is the cue to the network administrator to bring down the GRE tunnel and investigate.

By default, keepalive messages are sent every 10 seconds and the remote endpoint has three opportunities to reply. These thresholds are user configurable.

To enable or disable keepalive messages for a GRE tunnel, do the following:

1. Navigate to the **GRE** tab under **Tunnel » GRE**.
2. Select the desired GRE tunnel
3. Select the check box under **Enable Keepalive Messages** to enable keep alive messages, or clear the check box to disable the feature.
4. If keepalive messages are enabled, configure the following parameters:

Parameter	Description
Interval	<p><b>Synopsis:</b> An integer between 1 and 32767</p> <p><b>Default:</b> 10</p> <p>The interval in second(s) at which keepalive messages are sent to the remote endpoint.</p>

Parameter	Description
Retries	<p><b>Synopsis:</b> An integer between 1 and 255</p> <p><b>Default:</b> 3</p> <p>The number of keepalive message the remote endpoint can ignore before it is considered unreachable.</p>
Failover	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enable this tunnel to support failover.</p>

5. Commit the changes.

## 11.7.6 Deleting a GRE Tunnel

To delete a GRE tunnel, do the following:

1. Navigate to the **GRE** tab under **Tunnel » GRE**.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.7.7 Example: Configuring a GRE Tunnel with IPsec

This example describes one method to configure a GRE tunnel with IPsec on RUGGEDCOM ROX II devices.

For more information about IPsec tunnels, refer to "Managing IPsec Tunnels" (Page 415).

### NOTICE

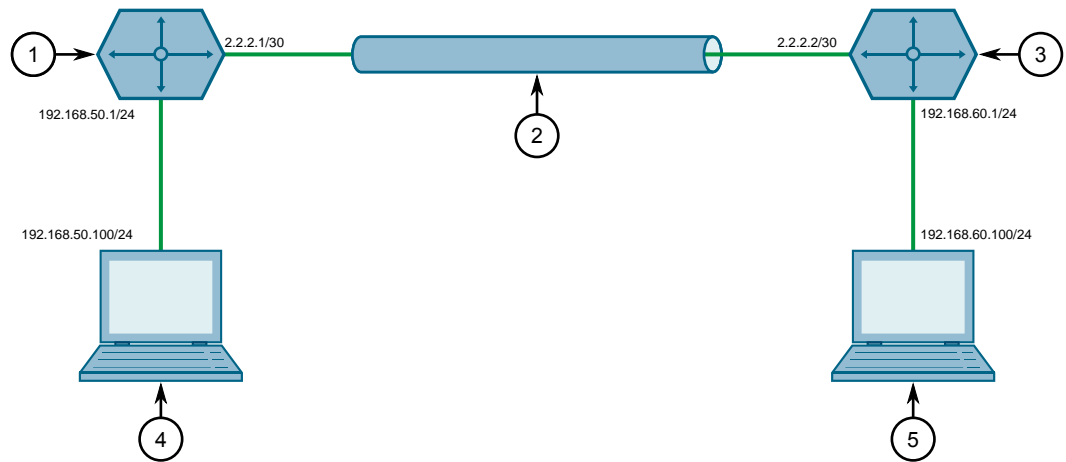
To ensure IPsec connections are independently managed when configuring GRE/IPsec, the following conditions must be met:

- The IPsec connection name must match the GRE tunnel interface name.
- Remote subnets defined under IPsec left/right sections are aware of each other only through the GRE tunnel. As the default value of the nexthop under left/right sections is *right side public-ip*, the nexthop value to the GRE tunnel IP must be configured to allow subnet traffic through the GRE tunnel.

### Note

When the IPsec connection name matches the GRE tunnel interface name, the left/right public IP(s) of the IPsec connection are ignored, and the GRE tunnel's local/remote IP is used to establish IPsec tunnel.

**NOTICE**  
 The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① Device A
- ② GRE/IPsec Tunnel
- ③ Device B
- ④ Client 1
- ⑤ Client 2

Figure 11.7 Topology – Site-to-Site Encrypted VPN Tunnel with a Pre-Shared Key

To configure a GRE tunnel with IPsec, do the following:

1. Configure Device A:
  - a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 105).
  - b. Add a GRE tunnel and configure the following parameters:

Parameter	Value
Local IP	2.2.2.1
Remote IP	2.2.2.2

For more information, refer to "Adding a GRE Tunnel" (Page 405).

- c. Enable Keepalive messages for GRE tunnel. For more information, refer to "Enabling/Disabling Keepalive Messages" (Page 408).
  - d. Assign IP address 172.16.1.1/24 to the gre tunnel interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
  - e. Add a unique pre-shared key and configure the following parameters:

Parameter	Value
Local Address	2.2.2.1
Remote Address	2.2.2.2

For more information, refer to "Adding a Pre-Shared Key" (Page 420).

- f. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret
Connection Type	tunnel

For more information about IPsec connections, refer to "Adding a Connection" (Page 421).

- g. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 426).
- h. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 428).
- i. Configure the left connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- j. Configure the left connection end for the IPsec tunnel with the following nexthop address parameters:

Parameter	Value
Type	address
Value	172.16.1.2

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- k. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).
- l. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.2

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- m. Configure the right connection end for the IPsec tunnel with the following nexthop address parameters:

Parameter	Value
Type	address
Value	172.16.1.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- n. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).

2. Configure Device B:

- a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 105).

- b. Add a GRE tunnel and configure the following parameters:

Parameter	Value
Local IP	2.2.2.2
Remote IP	2.2.2.1

For more information, refer to "Adding a GRE Tunnel" (Page 405).

- c. Enable Keepalive messages for GRE tunnel. For more information, refer to "Enabling/Disabling Keepalive Messages" (Page 408).

- d. Assign IP address *172.16.1.2/24* to the gre tunnel interface. For more information, refer to "Adding an IPv4 Address" (Page 225).

- e. Add a unique pre-shared key and configure the following parameters:

Parameter	Value
Local Address	2.2.2.2
Remote Address	2.2.2.1

For more information, refer to "Adding a Pre-Shared Key" (Page 420).

- f. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret
Connection Type	tunnel

For more information about IPsec connections, refer to "Adding a Connection" (Page 421).

- g. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 426).

- h. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 428).

- i. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- j. Configure the right connection end for the IPsec tunnel with the following nexthop address parameters:

Parameter	Value
Type	address
Value	172.16.1.2

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- k. Add subnet *192.168.50.0/24* for the right connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).
- l. Configure the left connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.2

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- m. Configure the left connection end for the IPsec tunnel with the following nexthop address parameters:

Parameter	Value
Type	address
Value	172.16.1.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- n. Add subnet *192.168.60.0/24* for the left connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).
3. Enable the IPsec tunnel. For more information, refer to "Configuring IPsec Tunnels" (Page 418).
4. Verify the tunnel status and make sure the traffic between the two sites is encrypted:
- View the IPsec tunnel status and look for a message that includes the connection name and the words *erouted*; *eroute owner*:. For example:

```
000 "gre-r1-r2":
192.168.50.0/24===2.2.2.1<2.2.2.1>;47/0---172.16.1.2...2.2.2.2<2.2.2.2>;47/0===192.168.60.0/24;
```



```
erouted; eroute owner: #10
```

This indicates the IPsec tunnel is active.

For more information, refer to "Viewing the IPsec Tunnel Status" (Page 420).

## Final Configuration Example

The following configuration reflects the topology:

### Device A

```
# show full-configuration
tunnel
gre r1-r2
  local-ip 2.2.2.1
  remote-ip 2.2.2.2
  gre-keepalives enabled
  gre-keepalives interval 10
  gre-keepalives retries 3
!
ipsec
enabled
no nat-traversal
preshared-key 2.2.2.2 2.2.2.1
  key $4$wocla9wLwmdwhYYI0d4IDw==
!
connection gre-r1-r2
  startup start
  authenticate secret
  connection-type tunnel
  dead-peer-detect enabled
  no l2tp
  ike algorithm aes256 sha1 modp1536
  !
  esp modpgroup modp1536
  esp algorithm aes256 sha1
  !
  left
  public-ip type address
  public-ip value 2.2.2.1
  nexthop type address
  nexthop value 172.16.1.2
  subnet 192.168.50.0/24
  !
  !
  right
  public-ip type address
  public-ip value 2.2.2.2
  nexthop type address
  nexthop value 172.16.1.1
  subnet 192.168.60.0/24
  !
  !
!
ip gre-r1-r2
no bandwidth
ipv4
address 172.16.1.1/24
no peer
!
```

### Device B

```
# show full-configuration
tunnel
gre r1-r2
  local-ip 2.2.2.2
  remote-ip 2.2.2.1
  gre-keepalives enabled
  gre-keepalives interval 10
  gre-keepalives retries 3
!
ipsec
  enabled
  no nat-traversal
  keep-alive 10
  preshared-key 2.2.2.1 2.2.2.2
  key $4$wocla9wLwmdwhYYI0d4IDw==
!
connection gre-r1-r2
  startup start
  authenticate secret
  connection-type tunnel
  dead-peer-detect enabled
  no l2tp
  ike algorithm aes256 sha1 modp1536
!
  esp modpgroup modp1536
  esp algorithm aes256 sha1
!
  left
  public-ip type address
  public-ip value 2.2.2.2
  nexthop type address
  nexthop value 172.16.1.1
  subnet 192.168.60.0/24
!
  right
  public-ip type address
  public-ip value 2.2.2.1
  nexthop type address
  nexthop value 172.16.1.2
  subnet 192.168.50.0/24
!
!
ip gre-r1-r2
  no bandwidth
  ipv4
  address 172.16.1.2/24
  no peer
!
!
```

## 11.8 Managing IPsec Tunnels

IPsec (Internet Protocol SECURITY) uses strong cryptography to provide authentication and encryption services. Authentication ensures that packets are from the right sender and have not been altered in transit. Encryption prevents unauthorized reading of packet contents.

These services allow secure tunnels to be built through untrusted networks. Everything passing through the untrusted network is encrypted by the IPsec gateway

and decrypted by the gateway at the other end. The result is a Virtual Private Network (VPN), a network which is effectively private even though it includes machines at several different sites connected by the insecure Internet.

For more information about IPsec tunnels, refer to "IPsec Tunneling Concepts" (Page 416).

**⚠ NOTICE**

IPsec is time-sensitive. To make sure proper re-keying between network peers, the time on both peers must be synchronized. It is strongly recommended that NTP (Network Time Protocol) be used on both IPsec peers to synchronize their clocks. For more information about configuring NTP, refer to "Managing NTP Servers" (Page 768).

## 11.8.1 IPsec Tunneling Concepts

The IPsec suite of protocols were developed by the Internet Engineering Task Force (IETF) and are required as part of IP version 6. Libreswan is the open source implementation of IPsec used by RUGGEDCOM ROX II.

The protocols used by IPsec are the Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) protocols. ESP provides encryption and authentication (ensuring that a message originated from the expected sender and has not been altered on route). IKE negotiates connection parameters, including keys, for ESP. IKE is based on the Diffie-Hellman key exchange protocol, which allows two parties without any initial shared secret to create one in a manner immune to eavesdropping.

### 11.8.1.1 IPsec Modes

IPsec has two basic modes of operation:

- **Transport Mode**  
In *transport* mode, IPsec headers are added as the original IP datagram is created. The resultant packet is composed of an IP header, IPsec headers and IP payload (including a transport header). Transport mode is most commonly used between IPsec end-stations, or between an end-station and a gateway.
- **Tunnel Mode**  
In *tunnel* mode, the original IP datagram is created normally and then encapsulated into a new IP datagram. The resultant packet is composed of a new IP header, IPsec headers, old IP header and IP payload. Tunnel mode is most commonly used between gateways, the gateway acting as a proxy for the hosts behind it.

### 11.8.1.2 Supported Encryption Protocols

Libreswan supports the following standard encryption protocols:

- **3DES (Triple DES)**

Uses three Data Encryption Standard (DES) encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. 3DES is the most CPU intensive cipher.

- **AES**

The Advanced Encryption Standard (AES) protocol cipher uses a 128-bit block and 128, 192 or 256-bit keys. This is the most secure protocol in use today, and is much preferred to 3DES due to its efficiency.

### 11.8.1.3 Public and Secret Key Cryptography

In *public key* cryptography, keys are created in matched pairs (called public and private keys). The public key is made public while the private key is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Only the owner of the private key can decrypt the message.

When this form of encryption is used, each router configures its VPN connection to use the RSA algorithm and includes the public signature of its peer.

In *secret key* cryptography, a single key known to both parties is used for both encryption and decryption.

When this form of encryption is used, each router configures its VPN connection to use a secret pre-shared key. For information about how to configure pre-shared keys, refer to "Managing Pre-Shared Keys" (Page 420).

### 11.8.1.4 X509 Certificates

In addition to pre-shared keys, IPsec also uses certificates to authenticate connections with hosts and routers. Certificates are digital signatures that are produced by a trusted source, namely a Certificate Authority (CA). For each host, the CA creates a certificate that contains CA and host information. The certificate is "signed" by creating a digest of all the fields in the certificate and then encrypting the hash value with its private key. The host's certificate and the CA public key are installed on all gateways that the host connects to.

When the gateway receives a connection request, it uses the CA public key to decrypt the signature back into the digest. It then recomputes its own digest from the plain text in the certificate and compares the two. If both digests match, the integrity of the certificate is verified (it was not tampered with), and the public key in the certificate is assumed to be the valid public key of the connecting host.

### 11.8.1.5 NAT Traversal

Historically, IPsec has presented problems when connections must traverse a firewall providing Network Address Translation (NAT). The Internet Key Exchange (IKE) used in IPsec is not NAT-translatable. When IPsec connections must traverse a firewall,

IKE messages and IPsec-protected packets must be encapsulated as User Datagram Protocol (UDP) messages. The encapsulation allows the original untranslated packet to be examined by IPsec.

Encapsulation is enabled during the IPsec configuration process. For more information, refer to "Configuring IPsec Tunnels" (Page 418).

#### 11.8.1.6 Remote IPsec Client Support

If the router is to support a remote IPsec client and the client will be assigned an address in a subnet of a local interface, a proxy ARP must be activated for that interface. This will cause the router to respond to ARP requests on behalf of the client and direct traffic to it over its connection.

IPsec relies upon the following protocols and ports:

- protocol 51, IPSEC-AH Authentication Header (RFC2402)
- protocol 50, IPSEC-ESP Encapsulating Security Payload (RFC2046)
- UDP port 500

The firewall must be configured to accept connections on these ports and protocols. For more information, refer to "Configuring the Firewall for a VPN" (Page 200).

#### 11.8.1.7 IPsec and Router Interfaces

If IPsec works on an interface which could disappear, such as a PPP connection, or if the IP address could change, the **Monitor Interface** option must be set for the IPsec connection. When this option is set, IPsec will restart when the interface disappears and reappears, or the IP address is changed.

The **Monitor Interface** option is set on the **Connection** form available for each connection. For more information about connections, refer to "Managing Connections" (Page 421).

### 11.8.2 Configuring IPsec Tunnels

To configure IPsec tunnels, do the following:

---

#### Note

RUGGEDCOM ROX II supports the creation of policy-based VPNs, which can be characterized as follows:

- No IPsec network interfaces have been created.
- The routing table is not involved in directing packets to IPsec.
- Only data traffic matching the tunnel's local and remote subnets is forwarded to the tunnel. Normal traffic is routed by one set of firewall rules and VPN traffic is routed based on separate rules.

- The firewall is configured with a VPN zone of type *ipsec*.
- As IPsec packets are received, they are decoded, flagged as IPsec-encoded, and presented as having arrived directly from the same network interface on which they were originally received.
- Firewall rules are written to allow traffic to and from VPN tunnels. These are based on the normal form of source/destination IP addresses, and IP protocol and port numbers. These rules, by virtue of the zones they match, use the policy flags inserted by the netkey to route matching data traffic to the proper interface.

For more information about configuring a policy-based VPN, refer to "Managing Firewalls" (Page 195).

1. Navigate to the **Parameters** tab under **Tunnel » IPsec**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enable IPsec	Enables IPsec.
NAT Traversal	This parameter is not supported and any value is ignored by the system. nat-traversal is always enabled in the IPsec VPN system.
Keep Alive	<b>Synopsis:</b> An integer between 1 and 86400 <b>Default:</b> 20  The delay (in seconds) for sending keepalive packets to prevent a NAT router from closing its port when there is not enough traffic on the IPsec connection.

3. Configure one or more pre-shared keys. For more information, refer to "Adding a Pre-Shared Key" (Page 420).
4. Configure one or more encrypted connections. For more information, refer to "Adding a Connection" (Page 421).
5. Commit the changes.

### 11.8.3 Configuring Certificates and Keys

To configure certificates and keys for IPsec Tunnels, do the following:

1. Add a CA certificate and Certificate Revocation List (CRL). For more information, refer to "Adding a CA Certificate and CRL" (Page 179).
2. Add a private key. For more information, refer to "Adding a Private Key" (Page 180).
3. Add a certificate. For more information, refer to "Adding a Certificate" (Page 184).
4. Add a public key. For more information, refer to "Adding a Public Key" (Page 182).
5. Navigate to the **Connection** tab under **Tunnel » IPsec**.

6. Select a connection, and then click **Left and Right**.
7. Under **System Public Key Type**, select **certificate** from the list. The **Certificate** parameter appears.
8. Under **Certificate**, select the appropriate certificate from the list.
9. Under **System Identifier Type**, select **from-certificate** from the list.
10. Commit the changes.

## 11.8.4 Viewing the IPsec Tunnel Status

To view the status of the IPsec tunnel, navigate to the **Parameters** tab under **Tunnel » IPsec**.

A detailed log of all IPsec activity is provided.

## 11.8.5 Managing Pre-Shared Keys

Pre-shared keys are used in *secret key* cryptography. For more information about *secret key* cryptography and pre-shared keys, refer to "Public and Secret Key Cryptography" (Page 417).

### 11.8.5.1 Viewing a List of Pre-Shared Keys

To view a list of pre-shared keys, navigate to the **Preshared Key** tab under **Tunnel » IPsec**.

If no pre-shared keys have been configured, add pre-shared keys as needed. For more information, refer to "Adding a Pre-Shared Key" (Page 420).

### 11.8.5.2 Adding a Pre-Shared Key

To add a pre-shared key, do the following:

1. Navigate to the **Preshared Key** tab under **Tunnel » IPsec**.
2. Configure the following parameters as required:

Parameter	Description
Remote Address	<b>Synopsis:</b> [ any ] or A string between 7 and 15 characters long or A string up to 1024 characters long  The remote address.
Local Address	<b>Synopsis:</b> [ any ] or A string between 7 and 15 characters long or A string up to 1024 characters long  The local address.

3. Click **OK** to create the new pre-shared key.
4. Configure the following parameter as required:

Parameter	Description
Key	<b>Synopsis:</b> A string between 1 and 8192 characters long The pre-shared key.

5. Commit the change.

### 11.8.5.3 Deleting a Pre-Shared Key

To delete a pre-shared key, do the following:

1. Navigate to the **Preshared Key** tab under **Tunnel » IPSec**.
2. Select the pre-shared key to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.8.6 Managing Connections

An IPsec connection is an encrypted connection between two devices who share the same pre-authorized authentication key.

### 11.8.6.1 Viewing a List of Connections

To view a list of connections configured for a VPN, navigate to the **Connection** tab under **Tunnel » IPSec**. If connections have been configured, a list appears.

If no connections have been configured, add connections as needed. For more information, refer to "Adding a Connection" (Page 421).

### 11.8.6.2 Adding a Connection

To add a new connection for a VPN, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPSec**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> [ default ] or A string between 1 and 30 characters long The connection name. Must start with a letter. If the name is 'default', all settings are considered the default for all other



Parameter	Description
	connections. If this connection is to be used with NHRP, the name given here must exactly match the interface name of the corresponding GRE tunnel interface.

4. Click **OK** to create the new connection.
5. Configure the following parameter(s) as required:

Parameter	Description
Startup Operation	<p><b>Synopsis:</b> [ ignore   add   start   route   default ]</p> <p><b>Default:</b> default</p> <p>The action to take when IPsec is initialized. The default value is 'ignore' unless overwritten by the default connection setting.</p>
Authenticate By	<p><b>Synopsis:</b> [ default   rsasig   secret ]</p> <p><b>Default:</b> default</p> <p>The authentication method. The default value is 'rsasig' unless overwritten by the default connection setting.</p>
Connection Type	<p><b>Synopsis:</b> [ tunnel   transport   passthrough   default ]</p> <p><b>Default:</b> default</p> <p>The connection type/mode. Options include:</p> <ul style="list-style-type: none"> <li>• tunnel: Encrypts traffic on host-to-host, host-to-subnet or subnet-to-subnet tunnels. This is the default type/mode unless overwritten by the default connection setting.</li> <li>• transport: Encrypts traffic on a host-to-host tunnel.</li> <li>• passthrough: Traffic is not encrypted.</li> </ul>
Address Family	<p><b>Synopsis:</b> [ ipv4   ipv6 ]</p> <p><b>Default:</b> ipv4</p> <p>The address-family to run for the connection. Accepted values include 'ipv4' (default) and 'ipv6'. All addresses used in the connection must have the same address family.</p>
IKE Version	<p><b>Synopsis:</b> [ v1   v2 ]</p> <p><b>Default:</b> v2</p> <p>Option to determine which Internet Key Exchange (IKE) version to use. Options include:</p> <ul style="list-style-type: none"> <li>• v1: Use IKEv1.</li> <li>• v2: Use IKEv2.</li> </ul>

6. If **Authenticate By** is set to **rsasig**, configure the following parameters:

Parameter	Description
Perfect Forward Secrecy	<p><b>Synopsis:</b> [ default   yes   no ]</p> <p><b>Default:</b> default</p> <p>Enables/disables Perfect Forwarding Secrecy (PFS). When enabled, IPsec negotiates new keys for each session. If an attacker compromises a key, only the session protected by the key is revealed. Not all clients support PFS. The default value is 'yes' unless overwritten by the default connection setting.</p>
SA Lifetime	<p><b>Synopsis:</b> [ default ] or An integer between 1081 and 86400</p> <p><b>Default:</b> default</p> <p>The lifetime in seconds for the Security Association (SA) key. This determines how long a particular instance of a connection should last, from successful negotiation to expiry. Normally, the connection is renegotiated before it expires. The default value is 28800 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the SA lifetime is longer.</p>
IKE Lifetime	<p><b>Synopsis:</b> [ default ] or An integer between 60 and 86400</p> <p><b>Default:</b> default</p> <p>The lifetime in seconds for for the IKE protocol. This determines how long the IKE keying channel of a connection should last before being renegotiated. The default value is 3600 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the IKE lifetime is longer.</p>
Keying Tries	<p><b>Synopsis:</b> [ default ] or An integer equal to or greater than 1</p> <p><b>Default:</b> default</p> <p>The maximum number of attempts to negotiate or replace a connection before aborting. When set to the default value '%forever', the device attempts to connect an unlimited number of times. This parameter is independent of the other endpoint's configuration.</p>
L2TP	Enables/disables L2TP for this connection.
Connection Alarms	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables or disables connection up and down alarms. Disabling connection alarms will prevent alarms from being sent for that connection. Connection alarms may also be controlled for the whole system under <b>admin &gt; alarm-cfg</b>.</p>
Monitor Interface	<p><b>Synopsis:</b> A string</p> <p>The interface to monitor. If the selected interface goes down and then up, this connection will be restarted.</p>

7. If required, enable and configure dead peer detection. For more information, refer to "Configuring Dead Peer Detection" (Page 424).
8. If required, configure the Internet Key Exchange (IKE) protocol by adding one or more algorithms. For more information, refer to "Adding an IKE Algorithm" (Page 426).
9. If required, configure Encapsulated Security Payload (ESP) encryption for the connection. For more information, refer to "Managing the Encapsulated Security Payload (ESP) Protocol" (Page 427).
10. If required, configure the left (local router) and right (remote router) ends of the connection. For more information, refer to "Managing Connection Ends" (Page 429).
11. If required, configure L2TP tunnels. For more information, refer to "Configuring L2TP Tunnels" (Page 365).
12. If certificates and keys are required, make sure they are configured on the device. For more information, refer to "Configuring Certificates and Keys" (Page 419).
13. Commit the changes.

### 11.8.6.3 Configuring Dead Peer Detection

Dead Peer Detection (DPD), as defined in [RFC 3706 \[http://tools.ietf.org/html/rfc3706\]](http://tools.ietf.org/html/rfc3706) is used to detect dead Internet Key Exchange (IKE) peers. In this method, peers exchange DPD Request (ISAKMP R-U-THERE) and DPD Response (ISAKMP R-U-THERE-ACK) messages. If a DPD Response is not received by a peer after a specified time and/or number of attempts, the other peer is considered *dead*. The remaining peer can either hold the connection until other peer responds, clear the connection, restart the connection and renegotiate the Security Association (SA), or restart all SA's to the dead peer.

In RUGGEDCOM ROX II, DPD Requests are sent when there is no traffic detected by the peer. How long to wait before sending a DPD Request and how long to wait for a DPD Response is user configurable.

It is generally recommended that DPD be configured to clear connections with any dead peers.

To configure dead peer detection for an IPsec connection, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection.
3. Configure the following parameter(s) as required:

---

**Note**

The timeout period must be two minutes longer than the interval period.

---

Parameter	Description
DPD Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables Dead Peer Detection (DPD) for this connection.</p>
DPD Interval	<p><b>Synopsis:</b> An integer between 1 and 3600</p> <p><b>Default:</b> 30</p> <p>The interval (in seconds) between Dead Peer Detection keepalive messages sent for this connection when no traffic (idle) appears to be sent by a DPD enabled peer.</p>
DPD Timeout	<p><b>Synopsis:</b> An integer between 1 and 28800</p> <p><b>Default:</b> 120</p> <p>The time in seconds to wait before a peer is declared dead.</p>
DPD Action	<p><b>Synopsis:</b> [ hold   clear   restart   restart-all-sa ]</p> <p><b>Default:</b> restart</p> <p>The action to be taken when a DPD enabled peer is declared dead. Options include:</p> <ul style="list-style-type: none"> <li>• hold: The route will be put on hold status.</li> <li>• clear: The route and Security Association (SA) will both be cleared</li> <li>• restart: The SA will immediately be renegotiated</li> <li>• restart-all-sa: All SA's to the dead peer will be renegotiated</li> </ul>

4. Commit the change.

#### 11.8.6.4 Deleting a Connection

To delete a connection for a VPN, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select the connection to be deleted, and then click **Delete Entry**.
3. Commit the change.

#### 11.8.6.5 Viewing the Status of a Connection

To view the status of an IPsec connection, navigate to the **Connection Status** tab under **Tunnel » IPsec**.

Possible values include:

- **dead peer detect disabled** – Dead Peer Detection (DPD) is disabled. DPD must be enabled to report the status of the connection.
- **inactive** – There are currently no established connections on the selected tunnel.

- **active** – There are established peer connections on the selected tunnel. The number of active peers is defined in brackets.
- **IPsec disabled** – IPsec is disabled.

## 11.8.7 Managing the Internet Key Exchange (IKE) Protocol

The Internet Key Exchange (IKE) protocol negotiates connection parameters, including keys, for the Encapsulated Security Payload (ESP) protocol employed by IPsec. IKE is based on the Diffie-Hellman key exchange protocol, which allows two parties without any initially shared secret to create one in a manner immune to eavesdropping.

### 11.8.7.1 Viewing a List of IKE Algorithms

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **IKE**. If algorithms have been configured, a list appears.

If no algorithms have been configured, add algorithms as needed. For more information, refer to "Adding an IKE Algorithm" (Page 426).

### 11.8.7.2 Adding an IKE Algorithm

To add a new algorithm for the Internet Key Exchange (IKE) protocol, do the following:

---

#### Note

#### Default Values

Default values for the cipher algorithm, method, or MODP group may change between RUGGEDCOM ROX II releases.

---

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **IKE**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Cipher	<p><b>Synopsis:</b> [ 3des   aes   aes256   aes192   aes128   any ]</p> <p>The cipher algorithm. The default value is 'aes' unless overwritten by the default connection setting. The value 'any' means to use the default value.</p>

## 11.8.8 Managing the Encapsulated Security Payload (ESP) Protocol

Parameter	Description
Hash	<p><b>Synopsis:</b> [ sha1   md5   sha2   any ]</p> <p>The hash method. The default value is 'sha2' unless overwritten by the default connection setting. The value 'any' means to use the default value.</p>
Modpgroup	<p><b>Synopsis:</b> [ modp1024   modp1536   modp2048   modp3072   modp4096   modp6144   modp8192   dh19   dh20   dh21   any ]</p> <p>The Modular Exponential (MODP) group. The default value is 'modp2048' unless overwritten by the default connection setting. The value 'any' means to use the default value.</p>

5. Click **Add** to create the new algorithm.
6. Click **OK** to create the new algorithm.
7. Commit the change.

### 11.8.7.3 Deleting an IKE Algorithm

To delete an algorithm for the Internet Key Exchange (IKE) protocol, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **IKE**.
3. Select the algorithm to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 11.8.8 Managing the Encapsulated Security Payload (ESP) Protocol

The Encapsulated Security Payload (ESP) employed by IPsec provides encryption and authentication, making sure that messages originated from the expected sender have not been altered in transit.

### 11.8.8.1 Configuring ESP Encryption

To configure the encryption algorithm for the Encapsulate Security Payload (ESP), do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **ESP**.
3. Configure the following parameter(s) as required:

Parameter	Description
Modpgroup	<p><b>Synopsis:</b> [ modp1024   modp1536   modp2048   modp3072   modp4096   modp6144   modp8192   dh19   dh20   dh21   any ]</p> <p><b>Default:</b> any</p> <p>The Modular Exponential (MODP) group. The default value is 'modp2048' unless overwritten by the default connection setting. The value 'any' means to use the default value.</p>

4. If required, add additional cipher algorithms. For more information on how to add algorithms, refer to "Adding an ESP Algorithm" (Page 428).
5. Commit the change.

### 11.8.8.2 Viewing a List of ESP Algorithms

1. Navigate to the **Connection** tab under *Tunnel » IPSec*.
2. Select a connection, and then click **ESP**. If algorithms have been configured, a list appears.

If no algorithms have been configured, add algorithms as needed. For more information, refer to "Adding an ESP Algorithm" (Page 428).

### 11.8.8.3 Adding an ESP Algorithm

To add a new algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

---

#### Note

#### Default Values

Default values for the cipher algorithm, method, or MODP group may change between RUGGEDCOM ROX II releases.

---

#### Note

If IKE v2 is selected, at least one ESP algorithm must be added.

---

1. Navigate to the **Connection** tab under *Tunnel » IPSec*.
2. Select a connection, and then click **ESP**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Cipher	<p><b>Synopsis:</b> [ 3des   aes   aes256   aes192   aes128   any ]</p> <p>The cipher algorithm. The default value is 'aes' unless overwritten by the default connection setting. The value 'any' means to use the default value.</p>
Hash	<p><b>Synopsis:</b> [ sha1   md5   sha2   any ]</p> <p>The hash method. The default value for IKEv1 is 'sha1' unless overwritten by the default connection setting. The value 'any' means to use the default value. There is no default value for IKEv2.</p>

5. Click **OK** to create the new algorithm.
6. Commit the change.

#### 11.8.8.4 Deleting an ESP Algorithm

To delete an algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **ESP**.
3. Select the algorithm to be deleted, and then click **Delete Entry**.
4. Commit the change.

### 11.8.9 Managing Connection Ends

Each IPsec tunnel has two ends: the local router and the remote router. These are otherwise referred to as the left and right connections, respectively. Both ends can have the same configuration or a unique configuration.

For each connection end, make sure to configure settings for the public IP address, system public key, system identifier, next hop, and the NAT traversal negotiation method.

#### 11.8.9.1 Configuring the Public IP Address for a Connection End

To configure the public IP address for a connection end, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **Left and Right**.
3. Configure the following parameters for the left (local router) or right (remote router) connection end:



<b>⚠ NOTICE</b>
Do not use a Virtual IP Address (VRIP) as the connection's public IP address if <b>Use Virtual MAC</b> is enabled under VRRP.

Parameter	Description
Public Address Type	<b>Synopsis:</b> [ none   default-route   any   address   hostname ] <b>Default:</b> none The public IP address type.
Public Hostname or IP Address	<b>Synopsis:</b> A string up to 1024 characters long The public hostname or IP address.

- Commit the changes.

### 11.8.9.2 Configuring the System Public Key for a Connection End

To configure the system public key for a connection end, do the following:

- Navigate to the **Connection** tab under **Tunnel » IPsec**.
- Select a connection, and then click **Left and Right**.
- Configure the following parameter for the left (local router) or right (remote router) connection end:

Parameter	Description
System Public Key Type	<b>Synopsis:</b> [ none   rsasig   certificate-any   certificate   ca-certificate ] <b>Default:</b> none Key type.

- If **rsasig** is the selected key type, configure the following parameters:

Parameter	Description
RSA Signature	<b>Synopsis:</b> A string between 1 and 255 characters long The RSA signature key name.
RSA Signature in ipsec format	<b>Synopsis:</b> A string between 1 and 8192 characters long The RSA signature in IPsec format.

- If **certificate** is the selected key type, configure the following parameters:

Parameter	Description
Certificate	<b>Synopsis:</b> A string between 1 and 255 characters long The selected certificate.

6. If **ca-certificate** is the selected key type, configure the following parameters:

Parameter	Description
CA certificate	<b>Synopsis:</b> A string between 1 and 255 characters long The selected CA certificate.

7. Commit the changes.

### 11.8.9.3 Configuring the System Identifier for a Connection End

To configure the system identifier for a connection end, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPSec**.
2. Select a connection, and then click **Left and Right**.
3. Configure the following parameters for the left (local router) or right (remote router) connection end:

Parameter	Description
System Identifier Type	<b>Synopsis:</b> [ default   none   from-certificate   address   hostname   der-asn1-dn   user-fqdn ] <b>Default:</b> default The system identifier type. The default value is 'left side public-ip' unless overwritten by the default connection setting.
Hostname, IP Address or Distinguished Name in Certificate	<b>Synopsis:</b> A string up to 1024 characters long The hostname, IP address or the Distinguished Name in the certificate.

4. Commit the changes.

### 11.8.9.4 Configuring the Next Hop for a Connection End

To configure the next hop to the other system for a connection end, do the following:

1. Navigate to the **Connection** tab under **Tunnel » IPSec**.
2. Select a connection, and then click **Left and Right**.
3. Configure the following parameters for the left (local router) or right (remote router) connection end:

Parameter	Description
Nexthop to Other System Type	<b>Synopsis:</b> [ default   default-route   address ] <b>Default:</b> default The next hop type. The default value is 'right side public-ip' unless overwritten by the default connection setting.

Parameter	Description
Nexthop to Other System IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long  The IP address of the next hop that can be used to reach the destination network.

4. Commit the changes.

### 11.8.9.5 Configuring the NAT Traversal Negotiation Method for a Connection End

To configure the Network Address Translation (NAT) traversal negotiation method for a connection end, do the following:

#### Note

Using the RFC 3947 negotiation method over draft-ietf-ipsec-nat-t-ike-02 may cause issues when connecting to the IPsec server, as RFC 3947 uses different identifiers when NAT is involved. For example, when a Windows XP/2003 client connects, Libreswan reports the main mode peer ID as `ID_FQDN: '@example.com'`. However, when a Vista, Windows 7 or other RFC 3947 compliant client connects, Libreswan reports the main mode peer ID as `ID_IPV4_ADDR: '192.168.1.1'`. If possible, use the draft-ietf-ipsec-nat-t-ike-02 method to avoid this issue.

1. Navigate to the **Connection** tab under **Tunnel » IPsec**.
2. Select a connection, and then click **Left and Right**.
3. Configure the following parameters for the left (local router) or right (remote router) connection end:

Parameter	Description
NAT Traversal Negotiation Method	<b>Synopsis:</b> [ default   draft-ietf-ipsec-nat-t-ike-02   rfc-3947 ] <b>Default:</b> default  The NAT traversal negotiation method. Some IPsec endpoints prefer RFC 3947 over draft-ietf-ipsec-nat-t-ike-02 when connecting with Libreswan, as these implementations use different identifiers when NAT is involved. For example, when a Windows XP/2003 client connects, Libreswan reports the main mode peer ID is <code>ID_FQDN: '@example.com'</code> , but when a Vista, Windows 7 or other RFC 3947 compliant client connects, Libreswan reports the main mode peer ID is <code>ID_IPV4_ADDR: '192.168.1.1'</code> . This will cause issues connecting to the IPsec server. In such cases, setting this option to draft-ietf-ipsec-nat-t-ike-02 will solve this problem. The default value is 'rfc-3947' unless overwritten by the default connection setting.

4. Commit the changes.

## 11.8.10 Managing Private Subnets

If the device is connected to an internal, private subnet, access to the subnet can be granted to the device at the other end of the IPsec tunnel. Only the IP address and mask of the private subnet is required.

### 11.8.10.1 Viewing a List of Addresses for Private Subnets

1. Navigate to the **Connection** tab under *Tunnel » IPsec*.
2. Select a connection, and then click **Left and Right Subnet**. If IP addresses have been configured, a list appears.

If no IP addresses have been configured, add addresses as needed. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).

### 11.8.10.2 Adding an Address for a Private Subnet

To add an IP address for a private subnet, do the following:

1. Navigate to the **Connection** tab under *Tunnel » IPsec*.
2. Select a connection, and then click **Left and Right Subnet**.
3. Click **Add Entry**, and then type the IPv4 address and prefix. Click **OK**.
4. Commit the change.

### 11.8.10.3 Deleting an Address for a Private Subnet

To delete an IP address for a private subnet, do the following:

1. Navigate to the **Connection** tab under *Tunnel » IPsec*.
2. Select a connection, and then click **Left and Right Subnet**.
3. Select the IP address to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 11.8.11 Example: Configuring an Encrypted VPN Tunnel

This example describes how to configure an encrypted VPN tunnel over a public network using Layer 3 RUGGEDCOM ROX II devices.

### NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

11.8.11 Example: Configuring an Encrypted VPN Tunnel

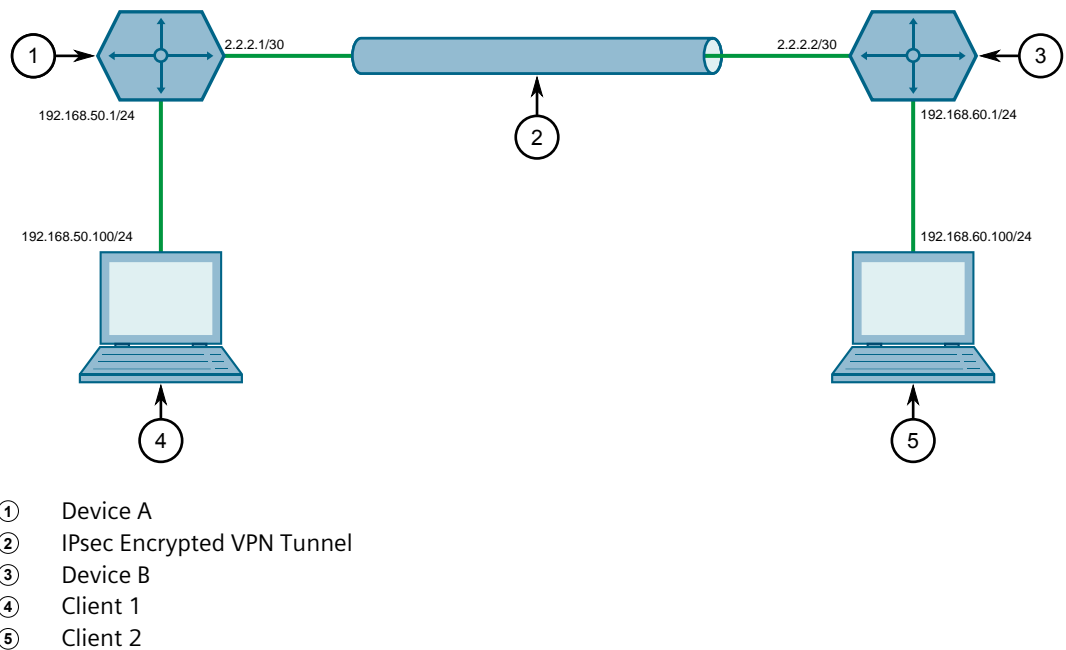


Figure 11.8 Topology – Site-to-Site Encrypted VPN Tunnel with a Pre-Shared Key

To configure a VPN tunnel, do the following:

1. Configure a connection name for the VPN. For more information, refer to "Adding a Connection" (Page 421).
2. Configure Device A:
  - a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 105).
  - b. Add a unique pre-shared key and configure the following parameters:

Parameter	Value
Local Address	2.2.2.1/30
Remote Address	2.2.2.2/30

For more information, refer to "Adding a Pre-Shared Key" (Page 420).

- c. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret
Connection Type	tunnel

For more information about IPsec connections, refer to "Adding a Connection" (Page 421).

- d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 426).

## 11.8.11 Example: Configuring an Encrypted VPN Tunnel

- e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 428).
- f. Configure the left connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- g. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).
- h. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.2

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- i. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).

### 3. Configure Device B:

- a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 105).
- b. Add a unique pre-shared key and configure the following parameters:

Parameter	Value
Local Address	2.2.2.2/30
Remote Address	2.2.2.1/30

For more information, refer to "Adding a Pre-Shared Key" (Page 420).

- c. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret
Connection Type	tunnel

For more information about IPsec connections, refer to "Adding a Connection" (Page 421).

- d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 426).

## 11.8.11 Example: Configuring an Encrypted VPN Tunnel

- e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 428).
- f. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.2

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- g. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).
- h. Configure the left connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 429).

- i. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to "Adding an Address for a Private Subnet" (Page 433).
4. Enable the IPsec tunnel. For more information, refer to "Configuring IPsec Tunnels" (Page 418).
  5. Verify the tunnel status and make sure the traffic between the two sites is encrypted:
    - a. View the IPsec tunnel status and look for a message that includes the connection name and the words *erouted; eroute owner*:. For example:

```
000 "ipsec-12": 192.168.22.0/24===192.168.12.2<192.168.12.2>[C=CA,
  ST=Ontario, O=RuggedCom, CN=router2, E=router2@exam
  ple.com,+S=C]...192.168.12.1<192.168.12.1>[C=CA, ST=Ontari o, O=Rugged
  Com, CN=router1, E=router1@example.com,+S=C]===192.168.11.0/24; erouted;
eroute owner: #2
```

This indicates the IPsec tunnel is active.

For more information, refer to "Viewing the IPsec Tunnel Status" (Page 420).

- b. Capture the packets using Tcpcmdump on one of the tunnel interfaces. Encrypted traffic will display an *ESP* header. For more information about using the Tcpcmdump utility, refer to "Capturing Packets from a Network Interface" (Page 43).

## Final Configuration Example

The following configuration reflects the topology:

### Device A

```
# show full-configuration
tunnel
ipsec
  enabled
  preshared-key 2.2.2.2 2.2.2.1
    key SiEm3nsRu993dc@m
  !
  connection test
    startup          start
    authenticate     secret
    connection-type  tunnel
    ike algorithm    any any any
  !
  esp algorithm      any any
  !
  left
    public-ip type  address
    public-ip value 2.2.2.1
    subnet 192.168.50.0/24
  !
  right
    public-ip type  address
    public-ip value 2.2.2.2
    subnet 192.168.60.0/24
```

### Device B

```
# show full-configuration
tunnel
ipsec
  enabled
  preshared-key 2.2.2.1 2.2.2.2
    key SiEm3nsRu993dc@m
  !
  connection test
    startup          start
    authenticate     secret
    connection-type  tunnel
    ike algorithm    any any any
  !
  esp algorithm      any any
  !
  left
    public-ip type  address
    public-ip value 2.2.2.1
    subnet 192.168.50.0/24
  !
  right
    public-ip type  address
    public-ip value 2.2.2.2
    subnet 192.168.60.0/24
```

## 11.9 Managing 6in4 and 4in6 Tunnels

In networks where IPv4 and IPv6 operate simultaneously, 6in4 and 4in6 tunnels can be used to enable IPv6/IPv4 hosts to reach services using the opposite protocol. IPv6/



IPv4 hosts and networks isolated from one another can also use these tunnels to access one another.

In a 6in4 tunnel, IPv6 traffic is encapsulated over configured IPv4 links, and vice versa for 4in6 tunnels.

---

**Note**

For information about how to monitor traffic through the tunnel, refer to "Viewing Statistics for Routable Interfaces" (Page 223).

---

### 11.9.1 Enabling/Disabling 6in4 or 4in6 Tunnels

To enable or disable all 6in4 or 4in6 tunnels, do the following:

1. Navigate to the **IP6in4 | IP4in6** tab under **Tunnel » IP2IP Tunnel**.
2. Under **IPv6 in IPv4 Tunnel Service**, select **Enabled** to enable 6in4 tunnels, or under **IP4v4 in IPv Tunnel Service** select **Enabled** to enable 4in6 tunnels, or clear **Enabled** to disable 6in4 or 4in6 tunnels.
3. Commit the change.

### 11.9.2 Viewing a List of 6in4 or 4in6 Tunnels

To view a list of 6in4 or 4in6 tunnels configured on the device, navigate to the **IP6in4 | IP4in6** tab under **Tunnel » IP2IP Tunnel**. If 6in4 or 4in6 tunnels have been configured, a list appears.

### 11.9.3 Viewing the Status of 6in4/4in6 Tunnels

To view the status of a 6in4 or 4in6 tunnel, navigate to the **IP6in4 | IP4in6** tab under **Tunnel » IP2IP Tunnel**.

### 11.9.4 Adding a 6in4 or 4in6 Tunnel

To add a 6in4 or 4in6 tunnel, do the following:

1. Navigate to the **IP6in4 | IP4in6** tab under **Tunnel » IP2IP Tunnel**.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string between 1 and 11 characters long</p> <p>The tunnel name. May contain any lower case letter or numerical digit. The prefix 't46-' is added automatically to create the iptunnel system interface name (ie. t46-1)</p>

- Click **OK** to create the new tunnel.
- Configure the following parameters as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables/disables the tunnel</p>
Local IP	<p><b>Synopsis:</b> A string between 6 and 40 characters long</p> <p>The IP address of the local tunnel endpoint</p>
Remote IP	<p><b>Synopsis:</b> A string between 6 and 40 characters long</p> <p>The IP address of the remote tunnel endpoint</p>
MTU	<p><b>Synopsis:</b> An integer between 68 and 1452</p> <p><b>Default:</b> 1452</p> <p>The Maximum Transmission Unit (MTU) of the network interface</p>

- Commit the change.

## 11.9.5 Deleting a 6in4 or 4in6 Tunnel

To delete a 6in4 or 4in6 tunnel, do the following:

- Navigate to the **IP6in4 | IP4in6** tab under **Tunnel » IP2IP Tunnel**.
- Select the tunnel to be deleted, and then click **Delete Entry**.
- Commit the change.

## 11.10 Managing DMVPN

This section describes how to configure the device as a spoke in a Dynamic Multipoint Virtual Private Network (DMVPN) hub-and-spoke network.

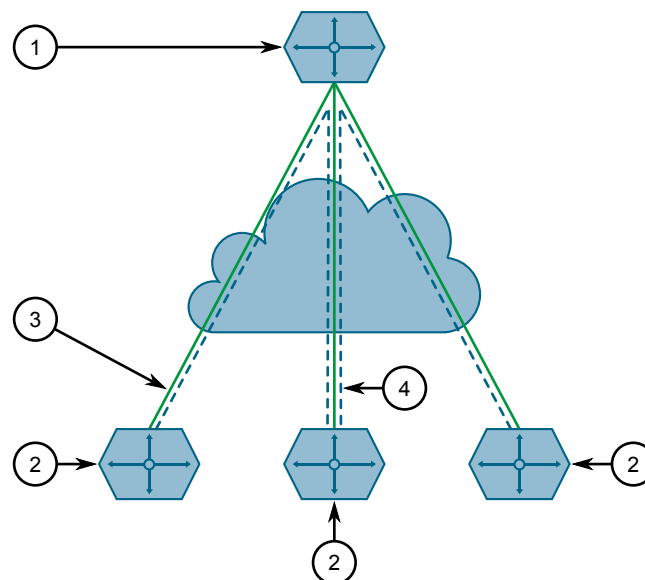
### 11.10.1 Understanding DMVPN

Dynamic Multipoint Virtual Private Network (DMVPN) is a routing solution for building scalable and secure VPN networks. It allows network designers to rapidly deploy routers for medium to large enterprises without having to configure static connections between all devices.

DMVPN can be deployed in one of two ways.

- Hub-and-Spoke
- Spoke-to-Spoke

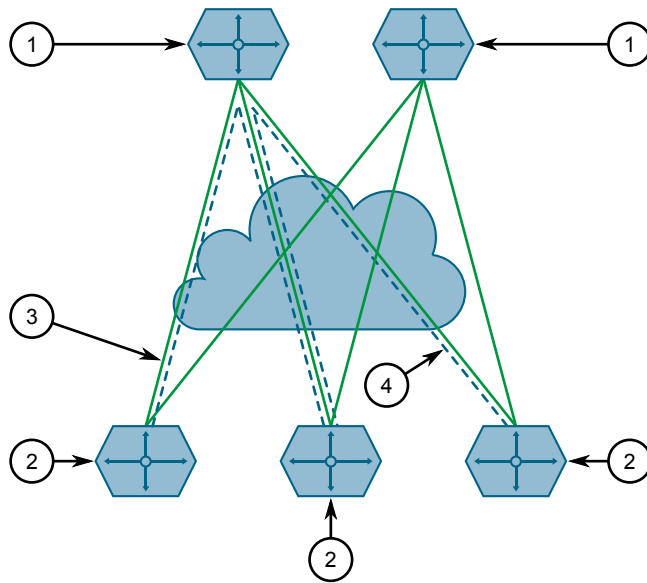
RUGGEDCOM ROX II supports hub-and-spoke deployments where a central router (the hub) uses Multipoint Generic Routing Encapsulation (mGRE) to establish GRE tunnels with one or more routers (the spokes). When spokes need to send traffic to one another, they send it to the hub first and the hub directs the data packets to the appropriate destination. This method allows network designers to avoid the complex task of defining static GRE tunnels for each possible connection.



- ① Hub (Static IP Address)
- ② Spoke (Static IP Address)
- ③ Hub-to-Spoke GRE/IPsec Tunnel

Figure 11.9 Hub-and-Spoke Topology – Single Hub

Spokes can also be connected to a secondary hub when redundancy is required.



- ① Hub (Static IP Address)
- ② Spoke (Static IP Address)
- ③ Hub-to-Spoke GRE/IPsec Tunnel

Figure 11.10 Hub-and-Spoke Topology – Dual Hub

## 11.10.2 Configuring DMVPN

To configure the device to act as a spoke in a hub-and-spoke network, do the following:

### Note

RUGGEDCOM ROX II supports connections with up to two hubs.

1. Determine the static IP address of the hub router.
2. Configure a GRE tunnel to the hub. For more information, refer to "Adding a GRE Tunnel" (Page 405).
3. Configure IPsec for the GRE tunnel, making sure the connection name matches the name of the GRE interface (e.g. gre-t1). For more information, refer to "Configuring IPsec Tunnels" (Page 418).
4. Configure a BGP route for the GRE tunnel. For more information, refer to "Configuring BGP" (Page 484).
5. Navigate to the **NHRP Parameters** tab under **Layer 3 » NHRP**.
6. Under **Enable NHRP**, click **Enabled** to enable the DMVPN service.

**Note**

RUGGEDCOM ROX II supports up to two DMVPN interfaces, each of which can be assigned to different GRE tunnels.

**11.10.3 Managing DMVPN Interfaces**

Configure a DMVPN interface to connect with a host. Up to two interfaces can be configured, allowing the device to connect with two hubs.

**11.10.3.1 Viewing a List of DMVPN Interfaces**

To view a list of DMVPN interfaces, navigate to the **NHRP Parameters** tab under **Layer 3 » NHRP**.

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a DMVPN Interface" (Page 442).

**11.10.3.2 Adding a DMVPN Interface**

To add a DMVPN interface, do the following:

1. Navigate to the **NHRP Parameters** tab under **Layer 3 » NHRP**.
2. Click **Add Entry**.
3. Configure the following parameter:

Parameter	Description
Interface Name	<p><b>Synopsis:</b> A string</p> <p>Interface name for the Generic Routing Encapsulation (GRE) tunnel to be used for NHRP: Note that the ipsec connection to be used for this interface must be configured with the same name as this interface. Maximum number of interfaces is 2.</p>

4. Click **OK** to add the interface.
5. Configure the following parameter(s) as required:

**⚠ NOTICE****Security hazard – risk of unauthorized access and/or exploitation**

For increased security, Siemens recommends configuring a key to authenticate the NHRP interface.

Parameter	Description
Enabled	A boolean flag to indicate Next Hop Resolution Protocol (NHRP) is enabled on this interface.
Address	<b>Synopsis:</b> A string between 9 and 18 characters long IPv4 address of remote GRE interface to be used for this NHRP session.
Hold Time	<b>Synopsis:</b> An integer <b>Default:</b> 7200 The time (in seconds) that Non-Broadcast Multi-Access (NBMA) addresses are advertised as valid in authoritative NHRP responses. Default is 7200 seconds.
Authentication	<b>Synopsis:</b> [ none   cisco ] The authentication string to allow intercommunication between source and destination NHRP nodes. Maximum length is 8 characters. Currently, only CISCO authentication is supported.
Key	<b>Synopsis:</b> A string The authentication key to allow intercommunication between source and destination NHRP nodes. Maximum length is 8 characters.

6. Commit the change.

### 11.10.3.3 Deleting a DMVPN Interface

To delete a DMVPN interface, do the following:

1. Navigate to the **NHRP Parameters** tab under **Layer 3 » NHRP**.
2. Select the interface to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 11.10.4 Viewing the Status of DMVPN

To view the status of the DMVPN service, navigate to the **Status** tab under **Layer 3 » NHRP**.

Information provided is taken directly from NHRP. The following are some of the fields that may be displayed:

---

### Note

Some fields only display when applicable.

---

Field	Description	Example
Status	The status of the interface.	Status: ok
Interface	The name of the interface.	Interface: gre-t1
Type	The NHRP peer type. Possible values: <ul style="list-style-type: none"> <li>• <code>shortcut-route</code> – Received or relayed resolution for the route</li> <li>• <code>incomplete</code> – Resolution request sent but no response received yet</li> <li>• <code>negative</code> – Negative cached</li> <li>• <code>cached</code> – Received or relayed resolution</li> <li>• <code>dynamic</code> – NHC registration</li> <li>• <code>dynamic-nhs</code> – Dynamic NHS from DNS map</li> <li>• <code>static</code> – Static map from the configuration file</li> <li>• <code>static-dns</code> – Static DNS map from the configuration file</li> <li>• <code>local-route</code> – Non-local destination, with local route</li> <li>• <code>local</code> – Local destination, IP or off-NBMA subnet</li> </ul>	Type: local
Protocol-Address	The interface's IP address.	Protocol-Address: 172.30.168.2/32
Flags	The flag(s) assigned to the last NHRP registration request packet. Possible values: <ul style="list-style-type: none"> <li>• <code>unique</code> – The NHRP peer is unique. Its NHRP mapping entry cannot be overwritten by a mapping entry with the same IP address, even if the associated peer has a different NBMA address.</li> <li>• <code>used</code> – The NHRP peer is in the kernel ARP table.</li> <li>• <code>up</code> – A connection with the NHRP peer has been established and the link is up.</li> <li>• <code>lower-up</code> – A connection with the NHRP peer has been established.</li> </ul>	Flags: up
NBMA-Address	The interface's NBMA address.	NBMA-Address: 172.19.20.21
NBMA-NAT_OA-Address	The interface's external IP address and mask. Displays only when the hub is behind a NAT-enabled router.	NBMA-NAT_OA-Address: 172.16.0.0/12
Expires-in	The time in seconds before the NBMA information of the responder is considered invalid and discarded. Displays only when the <b>Hold Time</b> is configured.	Expires-in: 120
Hostname	The host name of the NBMA responder, when available.	Hostname: ruggedcom

## Unicast and Multicast Routing

This chapter describes how to configure, monitor and manage static and dynamic routes unicast and multicast traffic.

### 12.1 Viewing the Status of IPv4 Routes

To view the status of the IPv4 routes configured on the device, navigate to the **IPv4 Routes** tab under **Layer 3 » Routing » Status » Routing Table**. If IPv4 routes have been configured, a list appears.

---

#### Note

It is possible to create a route on a locally connected broadcast network (i.e. without a gateway) without also bringing up a corresponding IP address on that interface. For example, it would be possible to add 192.168.1.0/24 to switch.0001, which has an IP address of 10.0.1.1 but no corresponding alias address on the 192.168.1.0/24 subnet.

---

The following information is provided:

Parameter	Description
Subnet	<b>Synopsis:</b> A string The network/prefix.
Gateway Address	<b>Synopsis:</b> A string The gateway address.
Interface Name	<b>Synopsis:</b> A string The interface name.
Route Type	<b>Synopsis:</b> A string The route type.
Route Weight	<b>Synopsis:</b> A string The route weight.
Metric	<b>Synopsis:</b> A string The route metric value.

If no IPv4 routes have been configured, add routes as needed. For more information, refer to "Adding an IPv4 Address" (Page 225).



## 12.2 Viewing the Status of IPv6 Routes

To view the status of the IPv6 routes configured on the device, navigate to the **IPv6 Routes** tab under **Layer 3 » Routing » Status » Routing Table**. If IPv6 routes have been configured, a list appears.

The following information is provided:

Parameter	Description
Subnet	<b>Synopsis:</b> A string The network/prefix.
Gateway Address	<b>Synopsis:</b> A string The gateway address.
Interface Name	<b>Synopsis:</b> A string The interface name.
Route Type	<b>Synopsis:</b> A string The route type.
Route Weight	<b>Synopsis:</b> A string The route weight.
Metric	<b>Synopsis:</b> A string The metric value.

If no IPv6 routes have been configured, add routes as needed. For more information, refer to "Adding an IPv6 Static Route" (Page 586).

## 12.3 Viewing the Memory Statistics

To view statistics related to the Core, RIP, OSPF and BGP daemons, navigate to **Layer 3 » Routing » Status**.

The following information is provided:

Parameter	Description
Total	<b>Synopsis:</b> An integer The total heap allocated (in bytes).
Used	<b>Synopsis:</b> An integer The number of used ordinary blocks (in bytes).
Free	<b>Synopsis:</b> An integer The number of free ordinary blocks (in bytes).

## 12.4 Configuring ICMP

To configure how RUGGEDCOM ROX II manages ICMP redirect messages, do the following:

1. Navigate to **Administration » ICMP**.
2. Configure the following parameter(s) as required:

---

### Note

ICMP redirect messages are sent by routers to hosts to inform them when a better route is available for a particular destination. However, before enabling RUGGEDCOM ROX II to send ICMP messages, be aware that ICMP redirects are simple to forge, allowing attackers to control the path by which packets are forwarded, and are sometimes considered a security risk. Send ICMP redirect messages only when appropriate.

Parameter	Description
Ignore ICMP ALL	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Ignores all ICMP echo requests sent to it.
Ignore ICMP Broadcast	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Ignores all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast.
Send ICMP Redirect	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Sends the ICMP redirect.

3. Commit the changes.

## 12.5 Managing Event Trackers

Trackers monitor the availability of hosts or devices by periodically transmitting ICMP messages (or pings). Based on the ICMP results, the tracker updates operational data with the status of the host or device as it changes (i.e. between "up" and "down" states). Other parts of the system can then subscribe to the operational data to be notified when changes take place.

Where available, a tracker can allow a user greater flexibility when configuring a feature. For example, advertised or received routes can be filtered or blocked entirely, based on the status of the tracker.

**Note**

Trackers only use ICMP messages to ping an IP target. Therefore, it can only provide availability for an IP device, and only up to the IP layer.

**12.5.1 Viewing a List of Event Trackers**

To view a list of event trackers, navigate to the **Events** tab under **Layer 3 » Tracking**. If event trackers have been configured, a list appears.

If no event trackers have been configured, add event trackers as needed. For more information, refer to "Adding an Event Tracker" (Page 449).

**12.5.2 Viewing Event Tracker Statistics**

RUGGEDCOM ROX II records statistics for each event tracker.

1. To view the statistics for an event tracker, navigate to the **Events** tab under **Layer 3 » Tracking**.
2. Select an event, and then select **Statistics**. If event trackers have been configured, a list appears.

This form provides the following information:

Parameter	Description
Echo Attempts	<b>Synopsis:</b> An integer The number of echo attempts.
Echo Replies	<b>Synopsis:</b> An integer The number of echo replies.
Min RTT	<b>Synopsis:</b> A string The minimum of the round trip time (in milliseconds).
Average RTT	<b>Synopsis:</b> A string The average of the round trip time (in milliseconds).
Max RTT	<b>Synopsis:</b> A string The maximum of the round trip time (in milliseconds).
Standard Deviation RTT	<b>Synopsis:</b> A string The standard deviation of the round trip time (in milliseconds).

### 12.5.3 Adding an Event Tracker

To add an event tracker, do the following:

1. Navigate to the **Events** tab under **Layer 3 » Tracking**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string up to 64 characters long The name of the event.

4. Click **OK** to add the tracker.
5. Configure the following parameter(s) as required:

Parameter	Description
Target	<b>Synopsis:</b> A string between 1 and 253 characters long Configures the ping target as an IPv4 address or hostname.domain.
Source IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long Sets the source address to a specified IPv4 address.
Source Interface	<b>Synopsis:</b> A string Forces a ping on a selected interface.
Timeout (ms)	<b>Synopsis:</b> An integer Determines how many milliseconds to wait for the ICMP response.
Interval (ms)	<b>Synopsis:</b> An integer equal to or greater than 100 Determines how many milliseconds to wait before sending another ICMP request.
Fall	<b>Synopsis:</b> An integer equal to or greater than 1 The number of times a failure occurs before changing the tracking state from up to down.
Rise	<b>Synopsis:</b> An integer equal to or greater than 1 The number of times success occurs before changing the tracking state from down to up.
State	<b>Synopsis:</b> [ up   down ] <b>Default:</b> up The state of the event.

6. Commit the changes.

## 12.5.4 Deleting an Event Tracker

To delete an event tracker, do the following:

1. Navigate to the **Events** tab under **Layer 3 » Tracking**.
2. Select the event tracker to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.6 Managing IS-IS

Intermediate System - Intermediate System (IS-IS) is one of a suite of routing protocols tasked with sharing routing information between routers. The job of the router is to enable the efficient movement of data over sometimes complex networks. Routing protocols are designed to share routing information across these networks and use sophisticated algorithms to decide the shortest route for the information to travel from point A to point B. One of the first link-state routing protocols was IS-IS developed in 1986 and later published in 1987 by ISO as ISO/IEC 10589. It was later republished as an IETF standard ([RFC 1142 \[http://tools.ietf.org/html/rfc1142\]](http://tools.ietf.org/html/rfc1142)).

### 12.6.1 IS-IS Concepts

IS-IS is an Interior Gateway Protocol (IGP) meant to exchange information within Autonomous Systems (AS). It is designed to operate within an administrative domain or network using link-state information to decide optimal data packet routing, similar to OSPF. IS-IS floods the network with link-state information and builds a database of the network's topology. The protocol computes the best path through the network (using Dijkstra's algorithm) and then forwards packets to their destination along that path.

Although it was originally designed as an ISO Connectionless-mode Network Protocol (CLNP), it was later adapted for IP network use (Dual IS-IS) in [RFC 1195 \[http://tools.ietf.org/html/rfc1195\]](http://tools.ietf.org/html/rfc1195). IS-IS is used primarily in ISP environments and better suited to *stringy* networks as opposed to central core based networks.

---

#### Note

In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

---

#### 12.6.1.1 IS-IS Routers

IS-IS routers can be defined as Level-1, Level-2, or both. Level 1 routers form the area, while Level 2 routers form the backbone of the network. By default,

RUGGEDCOM ROX II configures areas to be both (or Level-1-2). This allows the device to inter-operate between different areas with minimal configuration.

- **Level-1** routers are intra-area routers. They maintain a single Link-State Database (LSD) that only contains information about the Level-1 and Level-2 neighbors in its area. To communicate with routers in another area, Level-1 routers forward traffic through their closest Level-2 router.
- **Level-2** routers are inter-area routers, meaning they can communicate with routers in other areas. They also maintain a single LSD, but it only contains information about other Level-2 routers from the router's area or other areas. The router knows nothing about the Level-1 routers in its area.
- **Level-1-2** routers are both inter- and intra-area routers, meaning they can communicate with Level-1 and Level-2 routers in any area. They maintain separate LSDs for Level-1 and Level-2 routers in and outside the router's area.

### 12.6.1.2 Network Entity Title (NET) Addresses

IS-IS routers are identified by their Network Entity Title (NET) address, which is in Network Service Access Point (NSAP) format ([RFC 1237 \[http://tools.ietf.org/html/rfc1237\]](http://tools.ietf.org/html/rfc1237)). NSAP addresses range from 8 to 20 octets and consist of the Authority and Format Identifier (1 byte), the Area ID (0 to 12 bytes), the System ID (6 bytes) and the selector (1 byte).

The following is an example of an NSAP address:

```
NSAP address: 49.0001.1921.6800.1001.00

AFI: 49 (typical for IS-IS NET addresses)
Area ID: 0001 (typically 4 bytes)
System ID: 1921.6800.1001 (equates to the IP address 192.168.1.1)
Selector: 00 (NET addresses always have a selector of 00)
```

### 12.6.1.3 Advantages and Disadvantages of Using IS-IS

The advantages and disadvantages of using IS-IS include the following:

#### Advantages

- runs natively on the OSI network layer
- can support both IPv4 and IPv6 networks due to its independence from IP addressing
- IS-IS concept of areas is simpler to understand and implement
- IS-IS updates grouped together and sent as one LSP, rather than several small LSAs as with OSPF

#### Disadvantages

- used mostly by service providers
- limited support by network stack vendors and equipment makers
- CLNP addressing can be new and confusing to many users

- better scalability than OSPF due to a leaner daemon with less overhead
- gaining popularity among service providers
- integrates with MPLS
- protects from *spoofing* and Denial of Service (DoS) attacks due to use of the data link layer

## 12.6.2 Configuring IS-IS

To configure dynamic routing with IS-IS, do the following:

1. Navigate to the **Router Parameters** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**.
2. Under **Enable IS-IS**, select the **Enabled** check box.
3. Associate the device with one or more areas in the IS-IS network by defining area tags. For more information, refer to "Managing Area Tags" (Page 454).
4. Configure one or more interfaces on which to perform IS-IS routing. For more information, refer to "Managing Interfaces" (Page 456).

### Example

The following illustrates how to configure an IS-IS network that includes all circuit types. In this example, R1 is a Level-1 router that needs to forward traffic to Level-2 routers. R2 and R3 are configured to be Level-1-2 routers to facilitate the connection with routers R4 and R5, which are Level-2-only routers. Each router is configured to have a non-passive interface, use point-to-point network communication, and be in the same area.

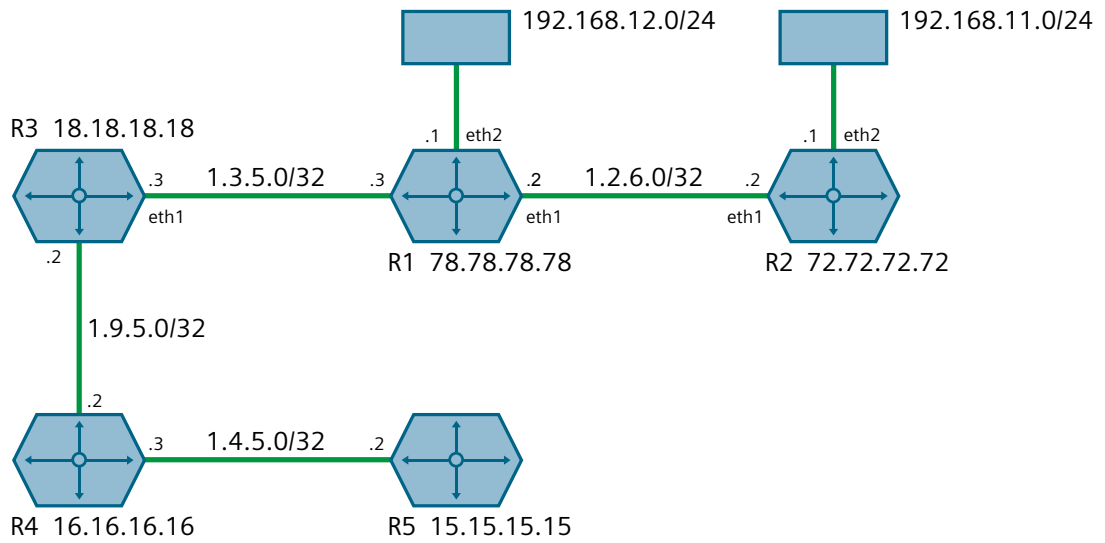


Figure 12.1 Multi-Level IS-IS Configuration

### 12.6.3 Viewing the Status of Neighbors

To view the status of neighboring devices on an IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to "Configuring IS-IS" (Page 452).
2. Navigate to **Layer 3 » Routing » Status » Dynamic Routing » IS-IS**.
3. Under **View ISIS Neighbors Status**, click **Perform**.

The following information is displayed:

Parameter	Description
System ID	The system ID.
Interface	The name of the interface.
L	The level. Possible levels are 1, 2 and 3, where 3 represents levels 1 and 2.
State	Adjacency state.
Holdtime	The remaining hold time in seconds.
SNPA	The MAC address of the Sub-Network Point of Attachment (SNPA).



## 12.6.4 Viewing the Status of the Link-State Database

To view the basic status of the link-state database for the IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to "Configuring IS-IS" (Page 452).
2. Navigate to **Layer 3 » Routing » Status » Dynamic Routing » IS-IS**.
3. Under **View ISIS Database Status**, click **Perform** for a basic view, or under **View ISIS Database Detail Status**, click **Perform** for a more detailed view.

The following information is displayed:

Parameter	Description
LSP-ID	Link-state PDU identifier.
Pdulength	Size of the PDU packet.
SeqNumber	Sequence number of the link-state PDU.
ChkSum	The checksum value of the link-state PDU.
Holdtime	The age of the link-state PDU in seconds.
ATT	Attach bit indicating the router is attached to another area.
P	Partition bit, set only if LSP supports partition repair.
OL	Overload, set only if the originator's LSP database is overloaded.

## 12.6.5 Managing Area Tags

An IS-IS area is a grouping of inter-connected (or neighboring) IS-IS configured routers. As opposed to OSPF, where an Area Border Router (ABR) can exist in two areas at once, IS-IS routers reside only in one area. It is the link between routers in two different areas that forms the border. This is because an IS-IS router has only one Network Service Access Point (NSAP) address.

A single router can be configured to act as a Level-1, Level-2 or Level-1-2 router in one or more areas.

Routers are associated with areas by area tags, which define the routing type, metric, and authentication/authorization rules.

### 12.6.5.1 Viewing a List of Area Tags

To view a list of area tags configured for dynamic IS-IS routes, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**. If area tags have been configured, a list appears.

If no area tags have been configured, add area tags as needed. For more information, refer to "Adding an Area Tag" (Page 455).

### 12.6.5.2 Adding an Area Tag

To add an area tag for dynamic IS-IS routes, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Area Tag	<b>Synopsis:</b> A string up to 64 characters long  Name for a routing process, must be unique among router processes for a given router. Mandatory field.

4. Click **OK** to create the new area tag.
5. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ]  The IS type for this area: level-1-only, level-2-only or level-1-2. Level-1 routers have neighbors only on the same area. Level-2-only (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
Metric Style	<b>Synopsis:</b> [ narrow   transition   wide ] <b>Default:</b> wide  The metric style Type Length Value (TLV) for this area: narrow, transition or wide. Default is wide.
Area Authorization	<b>Synopsis:</b> [ clear   md5 ] <b>Default:</b> clear  The authorization type for the area password. Default is clear.
Area Password	<b>Synopsis:</b> A string up to 254 characters long  The area password to be used for transmission of level-1 LSPs.
Area Authentication	<b>Synopsis:</b> [ send-only   validate ] <b>Default:</b> send-only  The authentication option to be used with the area password on SNP PDUs. Default is send-only.
Domain Authorization	<b>Synopsis:</b> [ clear   md5 ] <b>Default:</b> clear  The authorization type for the domain password. Default is clear.
Domain Password	<b>Synopsis:</b> A string up to 254 characters long  The domain password to be used for transmission of level-2 LSPs.

Parameter	Description
Domain Authentication	<p><b>Synopsis:</b> [ send-only   validate ]</p> <p><b>Default:</b> send-only</p> <p>The authentication option to be used with the domain password on SNP PDUs. Default is send-only.</p>

6. Add one or more Network Entity Titles (NETs). For more information, refer to "Managing Network Entity Titles (NETs)" (Page 464).
7. If necessary, configure intervals for the generation of Link-State Packets (LSPs). The default is 30 seconds. For more information, refer to "Managing LSP Generation" (Page 458).
8. If necessary, configure refresh intervals for Link-State Packets (LSPs). The default is 900 seconds. For more information, refer to "Managing LSP Refresh Intervals" (Page 462).
9. If necessary, configure the minimum interval between consecutive SPF calculations. The default is 1 second. For more information, refer to "Managing SPF Calculations" (Page 459).
10. If necessary, configure how long LSPs can reside in the device's Link State Database (LSDB) before they are refreshed. The default is 1200 seconds. For more information, refer to "Managing the Lifetime of LSPs" (Page 461).
11. If necessary, define rules for redistributing static, RIP, BGP or OSPF routes. For more information, refer to "Managing Redistribution Metrics" (Page 465).
12. Commit the changes.

### 12.6.5.3 Deleting an Area Tag

To delete an area tag for dynamic IS-IS routes, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**.
2. Select the area tag to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.6.6 Managing Interfaces

IS-IS transmits hello packets and Link-State Packets (LSPs) through IS-IS enabled interfaces.

---

### Note

IS-IS is only supported on Ethernet and WAN (HDLC-ETH) interfaces.

---

### 12.6.6.1 Viewing a List of Interfaces

To view a list of interfaces for dynamic IS-IS routes, navigate to the **Interface** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**. If interfaces have been configured, a list appears.

Interfaces are added automatically when a VLAN is created. For more information about creating a VLAN, refer to "Managing VLANs" (Page 311).

### 12.6.6.2 Configuring an Interface

When IS-IS is enabled, two interfaces are already configured: *fe-cm-01* and *switch.0001*.

To configure optional parameters for these and any other interfaces that have been added for IS-IS, do the following:

1. Navigate to the **Interface** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**.
2. Select an interface, and then configure the following parameter(s) as required:

Parameter	Description
IPv4 Area Tag	<b>Synopsis:</b> A string up to 64 characters long Name of Area Tag to be used for IS-IS over IPv4.
Circuit Routing Type	<b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ] The IS-IS Circuit Type. Level-1 routers have neighbors only on the same area. Level-2 (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
Point-to-Point	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Enable or disable point-to-point network communication
Passive	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Whether an interface is active or passive. Passive interfaces do not send packets to other routers and are not part of an IS-IS area.
Circuit Password	<b>Synopsis:</b> A string up to 254 characters long The value to be used as a transmit password in IIH PDUs transmitted by this Intermediate System.
Circuit Authorization	<b>Synopsis:</b> [ clear   md5 ] <b>Default:</b> clear The authorization type to be associated with the transmit password in IIH PDUs transmitted by this Intermediate System.

Parameter	Description
Metric	<p><b>Synopsis:</b> An integer between 1 and 16777214</p> <p><b>Default:</b> 10</p> <p>Metric assigned to the link, used to calculate the cost of the route. Value ranges from 1 to 16777214. Default is 10.</p>
CSNP Interval	<p><b>Synopsis:</b> An integer between 1 and 600</p> <p><b>Default:</b> 10</p> <p>CSNP interval in seconds, ranging from 1 to 600. Default is 10.</p>
Hello Interval	<p><b>Synopsis:</b> An integer between 1 and 600</p> <p><b>Default:</b> 3</p> <p>Hello interval in seconds, ranging from 1 to 600. Default is 3.</p>
Hello Multiplier	<p><b>Synopsis:</b> An integer between 2 and 100</p> <p><b>Default:</b> 10</p> <p>Multiplier for Hello holding time. Value ranges from 2 to 100. Default is 10.</p>
PSNP Interval	<p><b>Synopsis:</b> An integer between 1 and 120</p> <p><b>Default:</b> 2</p> <p>PSNP interval in seconds, ranging from 1 to 120. Default is 2.</p>

3. Commit the changes.

## 12.6.7 Managing LSP Generation

IS-IS generates new Link-State Packets (LSPs) every 30 seconds by default. However, the interval can be configured anywhere between 1 and 120 seconds.

Since the introduction of a new LSP causes other routers in the area to recalculate routes, it is recommended to increase the interval to decrease flooding during periods of network instability, so as to reduce the load on other routers in the area.

### 12.6.7.1 Viewing a List of LSP Generation Intervals

1. To view a list of LSP generation intervals configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **LSP Gen Interval** tab. If intervals have been configured, a list appears. If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an LSP Generation Interval" (Page 459).

### 12.6.7.2 Adding an LSP Generation Interval

To add an LSP generation interval to an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **LSP Gen Interval** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<p><b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ]</p> <p>The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.</p>

5. Click **OK** to create the new interval.
6. Configure the following parameter(s) as required:

Parameter	Description
Interval	<p><b>Synopsis:</b> An integer between 1 and 120</p> <p>Minimum interval in seconds, ranging from 1 to 120. Default is 30.</p>

7. Commit the changes.

### 12.6.7.3 Deleting an LSP Generation Interval

To delete an LSP generation interval for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **LSP Gen Interval** tab.
3. Select the interval to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.6.8 Managing SPF Calculations

IS-IS uses the Shortest Path First (SPF) algorithm to determine the best routes to every known destination in the network. When the network topology (not external links) changes, a partial recalculation is required.

IS-IS can be configured to perform the SPF calculation every 1 to 120 seconds. By default, IS-IS performs the SPF calculation every second, which could potentially be processor intensive, depending on the size of the area and how often the topology changes.

### 12.6.8.1 Viewing a List of SPF Calculation Intervals

1. To view a list of SPF calculation intervals configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **SPF Interval** tab. If intervals have been configured, a list appears.

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an SPF Calculation Interval" (Page 460).

### 12.6.8.2 Adding an SPF Calculation Interval

To add an SPF calculation interval to an IS-IS area, do the following:

1. To view a list of SPF calculation intervals configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **SPF Interval** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ] The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.

5. Click **OK** to create the new interval.
6. Configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 1 and 120 Minimum interval in seconds, ranging from from 1 to 120. Default is 1.

7. Commit the changes.

### 12.6.8.3 Deleting an SPF Calculation Interval

To delete an SPF calculation interval for an IS-IS area, do the following:

1. To view a list of SPF calculation intervals configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **SPF Interval** tab.
3. Select the interval to be deleted, and then click **Delete Entry**.

4. Commit the change.

## 12.6.9 Managing the Lifetime of LSPs

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, the maximum time limit is 1200 seconds. However, this interval can be customized for different routing types within the range of 350 to 65535 seconds if needed.

The lifetime interval is configurable for each area and routing type in the IS-IS network.

---

### Note

For information about configuring the refresh interval for an LSP, refer to "Managing LSP Refresh Intervals" (Page 462).

---

### 12.6.9.1 Viewing a List of LSP Lifetime Intervals

1. To view a list of LSP lifetime intervals configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **Max LSP Lifetime** tab. If intervals have been configured, a list appears.

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an LSP Lifetime Interval" (Page 461).

### 12.6.9.2 Adding an LSP Lifetime Interval

To add an LSP lifetime interval to an IS-IS area, do the following:

 <b>NOTICE</b>
The LSP lifetime interval must be 300 seconds higher than the LSP refresh interval. For more information about LSP refresh intervals, refer to "Managing LSP Refresh Intervals" (Page 462).

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **Max LSP Lifetime** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:



Parameter	Description
Routing Type	<b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ] The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.

5. Click **OK** to create the new limit.
6. Configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 1 and 65535 Minimum interval in seconds, ranging from 350 to 65535 seconds. Default is 1200.

7. Commit the changes.

### 12.6.9.3 Deleting an LSP Lifetime Interval

To delete an LSP lifetime interval for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **Max LSP Lifetime** tab.
3. Select the interval to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.6.10 Managing LSP Refresh Intervals

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, LSPs are retained in the LSDB for 1200 seconds (this is referred to as the *lifetime* of the LSP) and are refreshed every 900 seconds.

The refresh interval is configurable for each area and routing type in the IS-IS network.

---

### Note

For information about configuring the lifetime of an LSP, refer to "Managing the Lifetime of LSPs" (Page 461).

---

### 12.6.10.1 Viewing a List of LSP Refresh Intervals

1. To view a list of LSP refresh intervals configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **LSP Refresh Interval** tab. If intervals have been configured, a list appears.

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an LSP Refresh Interval" (Page 463).

### 12.6.10.2 Adding an LSP Refresh Interval

To add an LSP refresh interval to an IS-IS area, do the following:

**⚠ NOTICE**

The LSP refresh interval must be 300 seconds less than the LSP lifetime interval. For more information about LSP refresh intervals, refer to "Managing the Lifetime of LSPs" (Page 461).

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **LSP Refresh Interval** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<p><b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ]</p> <p>The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.</p>

5. Click **OK** to create the new interval.
6. Configure the following parameter(s) as required:

Parameter	Description
Interval	<p><b>Synopsis:</b> An integer between 1 and 65235</p> <p>Minimum interval in seconds, ranging from LSP generating interval to Maximum LSP lifetime less 300 seconds. Default is 900.</p>

7. Commit the changes.

### 12.6.10.3 Deleting an LSP Refresh Interval

To delete an LSP refresh interval for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **LSP Refresh Interval** tab.
3. Select the interval to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.6.11 Managing Network Entity Titles (NETs)

Network Entity Titles (NETs) define the area address and system ID for the router. Traffic received from another router that shares the same area address and system ID will be forwarded to this router.

RUGGEDCOM ROX II supports IS-IS multi-homing, which allows for multiple NETs to be defined for a single router and increases the list of possible traffic sources.

Each NET has a hexadecimal value, which can be between 8 and 20 octets long, although 10 octets is most common. The value includes an Authority and Format Identifier (AFI), an area ID, a system identifier, and a selector. The following is an example of an NET address:

```
49.0001.1921.6800.1001.00
```

- **49** is the AFI. Use **49** for private addressing.
- **0001** is the area ID. In this example, the area is **1**.
- **1921.6800.1001** is the system identifier. Any number can be used, but typically the system identifier is a modified form of the router's IP address. For example, the system identifier in this example translates to **192.168.1.1**. To convert the address in the opposite direction, pad the IP address with zeros (0) and rearrange the decimal points to form to make three two-byte numbers.
- **00** is the selector.

#### NOTICE

The system identifier must be unique to the network.

### 12.6.11.1 Viewing a List of NETs

1. To view a list of NETs configured for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **NET** tab. If NETs have been configured, a list appears.

If no NETs have been configured, add NETs as needed. For more information, refer to "Adding a NET" (Page 465).

### 12.6.11.2 Adding a NET

To add a Network Entity Title (NET) for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **NET** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Title	<p><b>Synopsis:</b> A string between 20 and 50 characters long</p> <p>The Network Entity Title (NET) for the device. The title must consist of an Authority and Format Identifier (AFI), a two-octet area ID, a six-octet system ID and a one-octet selector. For example: 49.0001.1921.68590.1001.00. The selector must be unique to the network.</p>

5. Click **OK** to create the new NET.
6. Commit the changes.

### 12.6.11.3 Deleting a NET

To delete a Network Entity Title (NET) for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **NET** tab.
3. Select the NET to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.6.12 Managing Redistribution Metrics

Redistribution in general is the advertisement of routes by one protocol that have been learned via another dynamic routing protocol, a static route, or a directly connected router. It is deployed to promote interoperability between networks running different routing protocols.

The redistribution of a route is achieved by defining a metric for the source routing protocol. As each routing protocol calculates routes differently, care must be taken to define a metric that is understood by the protocol.

There are two types of metrics: internal and external. Both types can be assigned a value between 0 and 63. However, to prevent external metrics from competing with internal metrics, 64 is automatically added to any external metric. This puts external metrics in the range of 64 to 128, even though the metric value defined is only in the range of 0 to 63.

There is no default metric for IS-IS. A metric should be defined for each routing protocol, otherwise a metric value of zero (0) is automatically applied.

### 12.6.12.1 Viewing a List of Redistribution Metrics

1. To view a list of redistribution metrics defined for an IS-IS area, navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **Redistribute** tab. If redistribution metrics have been configured, a list appears.

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 466).

### 12.6.12.2 Adding a Redistribution Metric

To add a redistribution metric for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **Redistribute** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Source	<b>Synopsis:</b> [ bgp   connected   kernel   ospf   rip   static ] Protocol that is source of IS-IS information.

5. Click **OK** to create the new metric.
6. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> [ level-1-only   level-2-only   level-1-2 ] IS type of the IS-IS information, specified as level-1-only, level-2-only or level-1-2. If not provided, uses IS type from area.
Metric Type	<b>Synopsis:</b> [ internal   external ] <b>Default:</b> external The IS-IS metric type for redistributed routes. Default is external
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric for redistributed routes.

7. Commit the changes.

### 12.6.12.3 Deleting a Redistribution Metric

To delete a redistribution metric for an IS-IS area, do the following:

1. Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » IS-IS**, and select an area tag.
2. Select the **Redistribute** tab.
3. Select the metric to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.7 Managing RIP

The Routing Information Protocol (RIP) determines the best path for routing IP traffic over a TCP/IP network based on the number of hops between any two routers. It uses the shortest route available to a given network as the route to use for sending packets to that network.

The RUGGEDCOM ROX II RIP daemon is an [RFC 1058](http://tools.ietf.org/rfc/rfc1058.txt) [http://tools.ietf.org/rfc/rfc1058.txt] compliant implementation of RIP that supports RIP version 1 and 2. RIP version 1 is limited to obsolete class-based networks, while RIP version 2 supports subnet masks, as well as simple authentication for controlling which routers to accept route exchanges with.

RIP uses network and neighbor entries to control which routers it will exchange routes with. A network is either a subnet or a physical (broadcast-capable) network interface. Any router that is part of that subnet or connected to that interface may exchange routes. A neighbor is a specific router, specified by its IP address, to exchange routes with. For point to point links (i.e. T1/E1 links), neighbor entries must be used to add other routers to exchange routes with. The maximum number of hops between two points on a RIP network is 15, placing a limit on network size.

Link failures will eventually be noticed when using RIP, although it is not unusual for RIP to take many minutes for a dead route to disappear from the whole network. Large RIP networks could take over an hour to converge when link or route changes occur. For fast convergence and recovery, OSPF is recommended. For more information about OSPF, refer to "Managing OSPF" (Page 522).

RIP is a legacy routing protocol that has mostly been superseded by OSPF.

---

### Note

In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

---

## 12.7.1 Configuring RIP

To configure dynamic routing using the Routing Information Protocol (RIP) daemon, do the following:

1. Navigate to the **Router Parameters** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Under **Timers**, configure the following parameters:

Parameter	Description
Update Timer	<b>Synopsis:</b> An integer between 5 and 2147483647 <b>Default:</b> 30 The routing table update timer (in seconds).
Timeout Timer	<b>Synopsis:</b> An integer between 5 and 2147483647 <b>Default:</b> 180 The routing information timeout timer (in seconds).
Garbage Collection Timer	<b>Synopsis:</b> An integer between 5 and 2147483647 <b>Default:</b> 120 The garbage collection timer (in seconds).

3. Under **Configurations**, configure the following parameters:

Parameter	Description
Enable RIP	Enables the RIP dynamic routing protocol.
Default Information Originate	The route element makes a static route only inside RIP. This element should be used only by advanced users who are particularly knowledgeable about the RIP protocol. In most cases, we recommend creating a static route and redistributing it in RIP using the redistribute element with static type.
Default Metric	<b>Synopsis:</b> An integer between 1 and 16 <b>Default:</b> 1 Sets the default metric. With the exception of connected route types, the default metric is advertised when a metric has not been configured for a redistributed route. For connected route types, the default metric is 1 despite the value of this parameter.
Distance Default	<b>Synopsis:</b> An integer between 1 and 255 Sets the default RIP distance.
Version	<b>Synopsis:</b> An integer between 1 and 2 Set the RIP version to accept for reads and send. The version can be either 1 or 2. Disabling RIPv1 by specifying version 2 is STRONGLY encouraged.

4. Configure prefix lists. For more information, refer to "Adding a Prefix List" (Page 472).

5. Configure a network. For more information, refer to "Configuring a Network" (Page 474).
6. Configure the prefix list distribution. For more information, refer to "Adding a Prefix List Distribution Path" (Page 478).
7. Configure key chains. For more information, refer to "Adding a Key Chain" (Page 479).
8. Configure redistribution metrics. For more information, refer to "Adding a Redistribution Metric" (Page 482).
9. Configure interfaces. For more information, refer to "Configuring a Routing Interface" (Page 482).
10. Commit the changes.

## 12.7.2 Viewing the Status of Dynamic RIP Routes

To view the status of the dynamic RIP routes configured on the device, navigate to the **Routes** tab under **Layer 3 » Routing » Status » Dynamic Routing » RIP**. If RIP routes have been configured, a list appears.

The following information is provided:

Parameter	Description
Network	<b>Synopsis:</b> A string The network.
Type	<b>Synopsis:</b> A string The route type.
Sub Type	<b>Synopsis:</b> A string The route sub type.
Next Hop	<b>Synopsis:</b> A string The next hop.
Metric	<b>Synopsis:</b> A string The metric value.
From	<b>Synopsis:</b> A string Where this route comes from.
Tag	<b>Synopsis:</b> A string Tag.
Time	<b>Synopsis:</b> A string The route update time.



To view the name of the interface associated with the route, navigate to the **Interface** tab under **Layer 3 » Routing » Status » Dynamic Routing » RIP**.

The following information is provided:

Parameter	Description
Name	<b>Synopsis:</b> A string The name of the interface.
Network	<b>Synopsis:</b> A string The network.
Type	<b>Synopsis:</b> A string The route type.
Sub Type	<b>Synopsis:</b> A string The route sub type.
Next Hop	<b>Synopsis:</b> A string Next hop.
Metric	<b>Synopsis:</b> A string The metric value.
From	<b>Synopsis:</b> A string Where this route comes from.
Tag	<b>Synopsis:</b> A string Tag.
Time	<b>Synopsis:</b> A string The route update time.

To view the routing information advertised to the network, navigate the **Interface** tab under **Layer 3 » Routing » Status » Dynamic Routing » RIP**. Select an interface, and then click **Advertised Route**.

The following information is provided:

Parameter	Description
Network	<b>Synopsis:</b> A string The network.
Type	<b>Synopsis:</b> A string The route type.
Sub Type	<b>Synopsis:</b> A string The route sub type.

Parameter	Description
Next Hop	<b>Synopsis:</b> A string Next hop.
Metric	<b>Synopsis:</b> A string The metric value.
From	<b>Synopsis:</b> A string Where this route comes from.
Tag	<b>Synopsis:</b> A string Tag.
Time	<b>Synopsis:</b> A string The route update time.

If no dynamic RIP routes have been configured, configure RIP and add routes as needed. For more information about configuring RIP, refer to "Configuring RIP" (Page 468).

## 12.7.3 Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the RIPs daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

### 12.7.3.1 Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic RIP routes, navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » RIP**. If prefix lists have been configured, a list appears.

If no prefix lists have been configured, add lists as needed. For more information, refer to "Adding a Prefix List" (Page 472).

### 12.7.3.2 Viewing a List of Prefix Entries

1. To view a list of entries for dynamic RIP prefix lists, navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » RIP**, and then select **Prefix List**.
2. Select a prefix list, and then click **Entry**. If entries have been configured, a list appears.

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 472).

**12.7.3.3 Adding a Prefix List**

To add a prefix list for dynamic RIP routes, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 1024 characters long The name of the prefix list.

4. Click **OK** to create the new prefix-list.
5. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string up to 1024 characters long The description of the prefix list.

6. Add prefix entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 472).
7. Commit the changes.

**12.7.3.4 Adding a Prefix Entry**

To add an entry for a dynamic RIP prefix list, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » RIP**, and then select **Prefix List**.
2. Select a prefix list, and then click **Entry**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Sequence	<b>Synopsis:</b> An integer between 1 and 4294967295 The sequence number of the entry.

5. Click **OK** to create the new entry.
6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ deny   permit ] <b>Default:</b> permit The action that will be performed.

Parameter	Description
Network	<b>Synopsis:</b> A string between 9 and 18 characters long The IPv4 network address and prefix.
Less Than or Equal To	<b>Synopsis:</b> An integer between 1 and 32 The maximum prefix length to be matched.
Greater Than or Equal To	<b>Synopsis:</b> An integer between 1 and 32 The minimum prefix length to be matched.

7. Commit the changes.

### 12.7.3.5 Deleting a Prefix List

To delete a prefix list for dynamic RIP routes, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.

---

#### Note

Deleting a prefix list removes all associated prefix entries as well.

---

2. Select the prefix list to be deleted, and then click **Delete Entry**.
3. Commit the changes.

### 12.7.3.6 Deleting a Prefix Entry

To delete an entry for a dynamic RIP prefix list, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » RIP**, and then select **Prefix List**.
2. Select a prefix list, and then click **Entry**.
3. Select the entry to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.7.4 Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

---

**Note**

For point to point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to "Adding a Neighbor" (Page 477).

---

**Note**

RIP v1 does not send subnet mask information in its updates. Any networks defined are restricted to the classic (i.e. Class A, B and C) networks.

---

**Note**

If neighbors are specified but no networks are specified, the router will receive routing information from its neighbors but will not advertise any routes to them. For more information about neighbors, refer to "Managing Neighbors" (Page 477).

---

#### 12.7.4.1 Configuring a Network

To configure a network for the RIP protocol, do the following:

1. Add one or more network IP addresses. For more information, refer to "Adding a Network IP Address" (Page 475).
2. Add one or more network interfaces. For more information, refer to "Adding a Network Interface" (Page 476).
3. Add one or more neighbors. For more information, refer to "Adding a Neighbor" (Page 477).

#### 12.7.4.2 Tracking Commands

Network commands can be tracked using event trackers configured under **Layer 3 » Tracking**. For more information about event trackers, refer to "Managing Event Trackers" (Page 447).

A network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's RIP peers) when the tracked target is unavailable.

To track a command for a RIP network, do the following:

1. Make sure a prefix list distribution path has been configured. For more information, refer to "Managing the Prefix List Distribution" (Page 477).
2. Navigate to the **Distribute Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
3. Select an interface, and then click the check box under **Track**.
4. Configure the following parameter(s) as required:

Parameter	Description
Track Event	<b>Synopsis:</b> A string up to 64 characters long  Selects an event to track. The distribute-prefix-list is applied only when the tracked event is in the UP state.
Apply When	<b>Synopsis:</b> [ up   down ] <b>Default:</b> up  Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

5. Commit the changes.

## 12.7.5 Managing Network IP Addresses

This section describes how to manage IP addresses for RIP networks.

### 12.7.5.1 Viewing a List of Network IP Addresses

To view a list of IP addresses configured for a RIP network, navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**, and then click **IP**. If addresses have been configured, a list appears.

If no IP addresses have been configured, add addresses as needed. For more information, refer to "Adding a Network IP Address" (Page 475).

### 12.7.5.2 Adding a Network IP Address

To add an IP address for a RIP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **IP**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address/Prefix	<b>Synopsis:</b> A string between 9 and 18 characters long  The IPv4 network address and prefix.

4. Click **OK** to add the IP address.
5. Commit the change.

### 12.7.5.3 Deleting a Network IP Address

To delete an IP address from a RIP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **IP**.
3. Select the IP address to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.7.6 Managing Network Interfaces

This section describes how to manage interfaces used by RIP networks.

### 12.7.6.1 Viewing a List of Network Interfaces

To view a list of interfaces configured for a RIP network, navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**. If interfaces have been configured, a list appears under **Interface**.

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Network Interface" (Page 476).

### 12.7.6.2 Adding a Network Interface

To add an interface for a RIP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Under **Interface**, select one or more interface(s) from the drop down list.
3. Commit the change.

### 12.7.6.3 Deleting a Network Interface

To delete an interface from a RIP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Under **Interface**, deselect one or more interface(s) from the drop down list.
3. Commit the change.

## 12.7.7 Managing Neighbors

Neighbors are other routers with which to exchange routes.

### 12.7.7.1 Viewing a List of Neighbors

To view a list of neighbors configured for a RIP network, navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**, and then click **Neighbor**. If neighbors have been configured, a list appears.

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 477).

### 12.7.7.2 Adding a Neighbor

To add a neighbor for a RIP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **Neighbor**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The IP address of the neighbor.

4. Click **OK** to add the address.
5. Commit the change.

### 12.7.7.3 Deleting a Neighbor

To delete a neighbor from a RIP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **Neighbor**.
3. Select the neighbor to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.7.8 Managing the Prefix List Distribution

This section describes how to manage the distribution of prefix lists.



### 12.7.8.1 Viewing a List of Prefix List Distribution Paths

To view a list of prefix list distribution paths for dynamic RIP routes, navigate to the **Distribute Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » RIP**. If distribution paths have been configured, a list appears.

If no prefix list distribution paths have been configured, add distribution paths as needed. For more information, refer to "Adding a Prefix List Distribution Path" (Page 478).

### 12.7.8.2 Adding a Prefix List Distribution Path

To add a prefix list distribution path for dynamic RIP routes, do the following:

1. Navigate to the **Distribute Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Direction	<b>Synopsis:</b> [ in   out ] Filters incoming or outgoing routing updates.
Interface Name	<b>Synopsis:</b> A string up to 15 characters long The name of the interface.

4. Click **OK** to add the path.
5. Configure the following parameter(s) as required:

Parameter	Description
Prefix List	<b>Synopsis:</b> A string between 1 and 1024 characters long The name of the prefix list.

6. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands" (Page 474).
7. Commit the changes.

### 12.7.8.3 Deleting a Prefix List Distribution Path

To delete a prefix list distribution path for dynamic RIP routes, do the following:

1. Navigate to the **Distribute Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select the path to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.7.9 Managing Key Chains and Keys

Key chains are collections of keys (or shared secrets), which are used to authenticate communications over a dynamic RIP network. Only routers with the same key are able to send and receive advertisements.

Multiple key chains can be configured for different groups of interfaces and the lifetime for each key within a chain can be separately configured.

### 12.7.9.1 Viewing a List of Key Chains

To view a list of key chains for dynamic RIP routes, navigate to the **Key Chain** tab under **Layer 3 » Routing » Dynamic Routing » RIP**. If key chains have been configured, a list appears.

If no key chains have been configured, add key chains as needed. For more information, refer to "Adding a Key Chain" (Page 479).

### 12.7.9.2 Viewing a List of Keys

1. To view a list of keys in a key chain, navigate to the **Key Chain** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select a key chain, and then click **Key**. If keys have been configured, a list appears.

If no keys have been configured, add keys as needed. For more information, refer to "Adding a Key" (Page 480).

### 12.7.9.3 Adding a Key Chain

To add a key chain for dynamic RIP routes, do the following:

1. Navigate to the **Key Chain** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Key Chain Name	<b>Synopsis:</b> A string between 1 and 1024 characters long The name of the key chain.

4. Click **OK** to add the key chain.
5. Configure one or more keys for the key chain. For more information, refer to "Adding a Key" (Page 480).

6. Configure a routing interface to use the key chain for authentication purposes. For more information, refer to "Configuring a Routing Interface" (Page 482).
7. Commit the changes.

#### 12.7.9.4 Adding a Key

Keys (or shared secrets) are used to authenticate communications over a RIP network. To maintain network stability, each key is assigned an accept and send lifetime.

The *accept* lifetime is the time period in which the key is accepted by the device.

The *send* lifetime is the time period in which the key can be sent to other devices.

This is referred to as hitless authentication key rollover, a method for seamlessly updating authentication keys without having to reset network sessions.

To add a key to a key chain, do the following:

1. Navigate to the **Key Chain** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select a key chain, and then click **Key**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Key ID	<b>Synopsis:</b> An integer The key identifier number.

5. Click **OK** to add the key.
6. Configure the following parameter(s) as required:

Parameter	Description
Key Configuration	<b>Synopsis:</b> A string Sets the key string.
Accept Life Time (Start)	<b>Synopsis:</b> A string The beginning time in which the key is considered valid.
Accept Life Time (Expire)	<b>Synopsis:</b> A string or [ infinite ] Expire time.
Send Life Time (Start)	<b>Synopsis:</b> A string Sets the time period in which the key on the key chain is considered valid.

Parameter	Description
Send Life Time (Expire)	<b>Synopsis:</b> A string or [ infinite ] The time at which the key expires.

7. Commit the changes.

### 12.7.9.5 Deleting a Key Chain

To delete a key chain for dynamic RIP routes, do the following:

1. Navigate to the **Key Chain** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select the key chain to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.7.9.6 Deleting a Key

To delete a key from a key chain, do the following:

1. Navigate to the **Key Chain** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select a key chain, and then click **Key**.
3. Select the key to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.7.10 Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the RIP networks, can also be advertised.

### 12.7.10.1 Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic RIP routes, navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » RIP**. If metrics have been configured, a list appears.

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 482).

**12.7.10.2 Adding a Redistribution Metric**

To add a redistribution metric for dynamic RIP routes, do the following:

1. Navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Metric	<b>Synopsis:</b> An integer between 0 and 16 The metric for redistributed routes.

4. Click **OK** to add the metric.
5. Commit the change.

**12.7.10.3 Deleting a Redistribution Metric**

To delete a redistribution metric for dynamic RIP routes, do the following:

1. Navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select the metric to be deleted, and then click **Delete Entry**.
3. Commit the change.

**12.7.11 Managing Routing Interfaces**

This section describes how to manage interfaces for RIP routes.

**12.7.11.1 Viewing a List of Routing Interfaces**

To view a list of routing interfaces for a RIP network, navigate to the **Interface** tab under **Layer 3 » Routing » Dynamic Routing » RIP**. A list appears.

**12.7.11.2 Configuring a Routing Interface**

To configure a routing interface for a RIP network, do the following:

---

**Note**

OSPF regards router interfaces as either passive or active, sending OSPF messages on active interfaces and ignoring passive interfaces.

---

1. Navigate to the **Interface** tab under **Layer 3 » Routing » Dynamic Routing » RIP**.
2. Select an interface, and then configure the following parameter(s) as required:

Parameter	Description
Mode	<b>Synopsis:</b> [ md5-rfc   md5-old-ripd   text   none ] The authentication mode.
Key Chain	<b>Synopsis:</b> A string between 1 and 1024 characters long The authentication key chain.
Authentication String	<b>Synopsis:</b> A string up to 16 characters long The authentication string.
Passive Interface	The specified interface is set to passive mode. In passive mode, all received packets are processed normally and RIPd sends neither multicast nor unicast RIP packets except to RIP neighbors specified with a neighbor element.
Receive Version	<b>Synopsis:</b> [ 1   2   1,2   2,1 ] The version of RIP packets that will be accepted on this interface. By default, version 1 and version 2 packets will be accepted.
Send Version	<b>Synopsis:</b> [ 1   2   1,2   2,1 ] The version of RIP to send packets with. By default, version 2 packets will be sent.
Split Horizon	<b>Synopsis:</b> [ yes   no   poisoned-reverse ] <b>Default:</b> yes A split horizon.

3. Commit the changes.

## 12.8 Managing BGP

The Border Gateway Protocol (BGP) as defined by [RFC 4271](http://tools.ietf.org/rfc/rfc4271.txt) [http://tools.ietf.org/rfc/rfc4271.txt] is a robust and scalable routing protocol. BGP is designed to manage a routing table of up to 90000 routes. Therefore, it is used in large networks or among groups of networks which have common administrative and routing policies. External BGP (eBGP) is used to exchange routes between different Autonomous Systems (AS). Interior BGP (iBGP) is used to exchange routes within autonomous system (AS).

BGP is used by the bgpd daemon to handle communications with other routers. The daemon also determines which routers it prefers to forward traffic to for each known network route.

**Note**

In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

**12.8.1 Configuring BGP**

To configure dynamic routing with BGP, do the following:

1. Navigate to the **Router Parameters** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Under **Distance**, configure the following parameters:

Parameter	Description
External Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 Distance value for external routes.
Internal Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 Distance value for internal routes.
Local Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 Distance value for local routes.

3. Under **BGP Configuration**, configure the following parameters:

Parameter	Description
Enable BGP	Enables BGP.
Autonomous System ID	<b>Synopsis:</b> An integer between 1 and 4294967295 Autonomous System (AS) ID, which can be a 2- or 4-byte AS number.
Always Compare MED	Always comparing MED from different neighbors.
Reachability Check	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Enables or disables the reachability check for advertised routes. When enabled, before advertising a self-generated BGP route to other BGP peers, the BGP daemon checks if the advertised route is reachable locally by default before advertising it to other BGP peers. The route is only advertised if it exists in the kernel routing table.
Default Local Preference	<b>Synopsis:</b> An integer <b>Default:</b> 100 Default local preference value.

Parameter	Description
Deterministic MED	Pick the best-MED path among paths advertised from neighboring AS.
Router ID	<b>Synopsis:</b> A string between 7 and 15 characters long Router ID for BGP.

4. Commit the changes.

---

**Note**

Following a change in the routing policy due to a configuration change, the BGP session must be reset for the new policy to take effect.

---

## 12.8.2 Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

### 12.8.2.1 Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic BGP, navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If filters have been configured, a list appears.

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 495).

### 12.8.2.2 Viewing a List of Route Map Filter Entries

1. To view a list of entries for a route map filter for either BGP, navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**. If entries have been configured, a list appears.

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 495).



### 12.8.2.3 Adding a Route Map Filter

To add a route map filter for dynamic BGP routes, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Under **Route Map Tag**, click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Route Map Tag	<b>Synopsis:</b> A string between 1 and 1024 characters long Route map tag.

4. Click **Add** to create the new filter.
5. Add one or more entries. For more information, refer to "Adding a Route Map Filter Entry" (Page 486).
6. Click **OK** to create the new filter.
7. Add one or more entries. For more information, refer to "Adding a Route Map Filter Entry" (Page 486).
8. Commit the change.

### 12.8.2.4 Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 65535 The sequence number of the route-map entry.

5. Click **OK** to create the new entry.
6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ deny   permit ] <b>Default:</b> permit Action.

Parameter	Description
Call Route Map	<b>Synopsis:</b> A string between 1 and 1024 characters long Jump to another route-map after match+set.
On Match Goto	<b>Synopsis:</b> An integer between 1 and 65535 Go to this entry on match.

7. Configure the match rules for the route map filter. For more information, refer to "Configuring Match Rules" (Page 487).
8. Configure a set for the route map filter. For more information, refer to "Configuring a Set" (Page 488).
9. Commit the change.

### 12.8.2.5 Deleting a Route Map Filter

To delete a route map filter for dynamic BGP routes, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Under **Route Map Tag**, select the filter to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.8.2.6 Deleting a Route Map Filter Entry

To delete an entry for a route map filter, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select the entry to be deleted, and then click **Delete Entry**.
4. Commit the change.

### 12.8.2.7 Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Under **Entry - { number }**, where { number } is the sequence number for the entry, configure the following parameters as required:

Parameter	Description
Match Address of Route	<b>Synopsis:</b> A string between 1 and 1024 characters long The prefix list name.
Match Nexthop of Route	<b>Synopsis:</b> A string between 1 and 1024 characters long The prefix list name.
Match Advertising Source Address	<b>Synopsis:</b> A string between 1 and 1024 characters long The prefix list name.
Match AS Path Filter	<b>Synopsis:</b> A string between 1 and 1024 characters long Match the BGP AS path filter.
Match Metric	<b>Synopsis:</b> An integer Match the route metric.
Match Peer	<b>Synopsis:</b> A string between 7 and 15 characters long This parameter is not supported and any value is ignored by the system.s
Match Origin	<b>Synopsis:</b> [ egp   igp   incomplete ] Match the BGP origin code.

4. Commit the change.

### 12.8.2.8 Configuring a Set

To configure a set for a route map filter entry, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Under **Entry - { number }**, where { number } is the sequence number for the entry, configure the following parameters as required:

Parameter	Description
Set Aggregator AS Number	<b>Synopsis:</b> An integer between 1 and 4294967295 AS number.
Set Aggregator IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long IP address of aggregator.
Set Metric Operation	<b>Synopsis:</b> [ set   add   sub ] Set , add or subtract the metric value.

## 12.8.3 Managing Prepended and Excluded Autonomous System Path Filters

Parameter	Description
Set Metric Value	<b>Synopsis:</b> An integer Value.
Local Preference	<b>Synopsis:</b> An integer Local preference.
Next Hop	<b>Synopsis:</b> A string between 7 and 15 characters long or [ peer ] The next hop address (xxx.xxx.xxx.xxx/xx or peer to use peer address).
Origin	<b>Synopsis:</b> [ egp   igp   incomplete ] The origin code.
Originator ID	<b>Synopsis:</b> A string between 7 and 15 characters long This parameter is not supported and any value is ignored by the system.
Weight	<b>Synopsis:</b> An integer Weight.

4. Add pre-pended and/or excluded autonomous system paths. For more information, refer to "Adding a Prepended Autonomous System Path Filter" (Page 490) and/or "Adding an Excluded Autonomous System Path filter" (Page 491).
5. Commit the change.

## 12.8.3 Managing Prepended and Excluded Autonomous System Path Filters

This section describes how to configure and manage prependded and excluded autonomous system path filters.

### 12.8.3.1 Viewing a List of Prepended Autonomous System Path Filters

1. To view a list of prependded autonomous system path filters configured for a BGP route map entry, navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select an entry, and then click **Set AS Path to Prepend**. If filters have been configured, a list appears.

If no prependded autonomous system path filters have been configured, add filters as needed. For more information, refer to "Adding a Prepended Autonomous System Path Filter" (Page 490).

### 12.8.3.2 Viewing a List of Excluded Autonomous System Paths

1. To view a list of excluded autonomous system path filters configured for a BGP route map entry, navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select an entry, and then click **Set AS Path Exclude**. If filters have been configured, a list appears.

If no excluded autonomous system path filters have been configured, add filters as needed. For more information, refer to "Adding an Excluded Autonomous System Path filter" (Page 491).

### 12.8.3.3 Adding a Prepended Autonomous System Path Filter

To add a prepended autonomous system path filter to a BGP route map entry, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select an entry, and then click **Set AS Path to Prepend**.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
AS Number	<b>Synopsis:</b> An integer between 1 and 4294967295 AS number.

6. Click **OK** to add the filter.
7. Configure the following parameter(s) as required:

Parameter	Description
Repeat Count	<b>Synopsis:</b> An integer between 1 and 9 <b>Default:</b> 1 Repeat count for AS number.

8. Commit the changes.

#### 12.8.3.4 Adding an Excluded Autonomous System Path filter

To add an excluded autonomous system path filter to a BGP route map entry, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select an entry, and then click **Set AS Path Exclude**.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
AS Number	<b>Synopsis:</b> An integer between 1 and 4294967295 AS number.

6. Click **OK** to add the filter.
7. Commit the change.

#### 12.8.3.5 Deleting a Prepended Autonomous System Path Filter

To delete a prependded autonomous system path filter from a BGP route map entry, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select an entry, and then click **Set AS Path to Prepend**.
4. Select the filter to be deleted, and then click **Delete Entry**.
5. Commit the change.

#### 12.8.3.6 Deleting an Excluded Autonomous System Path Filter

To delete an excluded autonomous system path filter from a BGP route map entry, do the following:

1. Navigate to the **Route Map** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a route map tag, and then click **Entry**.
3. Select an entry, and then click **Set AS Path Exclude**.
4. Select the filter to be deleted, and then click **Delete Entry**.
5. Commit the change.

## 12.8.4 Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the BGP daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

### 12.8.4.1 Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic BGP routes, navigate to the **Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If prefix lists have been configured, a list appears.

If no prefix lists have been configured, add lists as needed. For more information, refer to "Adding a Prefix List" (Page 492).

### 12.8.4.2 Viewing a List of Prefix Entries

1. To view a list of entries for dynamic BGP prefix lists, navigate to the **Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a prefix list, and then click **Entry**. If entries have been configured, a list appears.

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 493).

### 12.8.4.3 Adding a Prefix List

To add a prefix list for dynamic BGP routes, do the following:

1. Navigate to the **Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 1024 characters long The name of the prefix list.

4. Click **OK** to create the new prefix list.
5. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string up to 1024 characters long The description of the prefix list.

6. Add prefix entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 493).
7. Commit the changes.

#### 12.8.4.4 Adding a Prefix Entry

To add an entry for a dynamic BGP prefix list, do the following:

1. Navigate to the **Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a prefix list, and then click **Entry**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 4294967295 Sequence number of the entry.

5. Click **OK** to create the new entry.
6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ deny   permit ] <b>Default:</b> permit Action.
Network	<b>Synopsis:</b> A string between 9 and 18 characters long Network (xxx.xxx.xxx.xxx/xx).
Maximum Prefix to Mask for Subnet	<b>Synopsis:</b> An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
Minimum Prefix to Mask for Subnet	<b>Synopsis:</b> An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

7. Commit the change.

#### 12.8.4.5 Deleting a Prefix List

To delete a prefix list for dynamic BGP routes, do the following:

1. Navigate to the **Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.



---

**Note**

Deleting a prefix list removes all associated prefix entries as well.

---

2. Select the prefix list to be deleted, and then click **Delete Entry**.
3. Commit the change.

#### 12.8.4.6 Deleting a Prefix Entry

To delete an entry for a dynamic BGP prefix list, do the following:

1. Navigate to the **Prefix List** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a prefix list, and then click **Entry**.
3. Select the entry to be deleted, and then click **Delete Entry**.
4. Commit the change.

### 12.8.5 Managing Autonomous System Paths and Entries

This section describes how to configure autonomous system paths and entries for dynamic BGP routes.

#### 12.8.5.1 Viewing a List of Autonomous System Paths

To view a list of autonomous system path filters for dynamic BGP routes, navigate to the **AS Path** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If filters have been configured, a list appears.

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 495).

#### 12.8.5.2 Viewing a List of Autonomous System Path Entries

1. To view a list of entries for an autonomous system path filter, navigate to the **AS Path** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select an autonomous system path filter, and then click **Entry**. If entries have been configured, a list appears.

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 495).

### 12.8.5.3 Adding an Autonomous System Path Filter

To add an autonomous system path filter for dynamic BGP routes, do the following:

1. Navigate to the **AS Path** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 1024 characters long Name of the AS-path filter.

4. Click **Add** to create the new filter.
5. Add one or more entries. For more information, refer to "Adding an Autonomous System Path Filter Entry" (Page 495).
6. Click **OK** to create the new filter.
7. Add one or more entries. For more information, refer to "Adding an Autonomous System Path Filter Entry" (Page 495).
8. Commit the change.

### 12.8.5.4 Adding an Autonomous System Path Filter Entry

Create an entry for an autonomous system path filter to match a string or integer value in AS path and then perform an action. The match criteria is defined using regular expressions. The following lists special characters that can be used in a regular expression:

Character	Description	Example
.	Matches any single character (e.g. .100, 100., .100.)	.100 100. .100.
*	Matches zero (0) or more occurrences of a pattern	100*
+	Matches 1 or more occurrences of a pattern	100+
?	Match 0 or 1 occurrences of a pattern	100?
^	Matches the beginning of the line	^100
\$	Matches the end of the line	100\$
()	Matches only the characters specified	(38a)
[]	Matches any character other than those specified	[^abc]
_ (underscore)	The underscore character has special meanings in an autonomous system path. It matches to: <ul style="list-style-type: none"> <li>• Each space ( ) and comma (,)</li> <li>• Each AS set delimiter (e.g. { and })</li> <li>• Each AS confederation delimiter (e.g. ( and ))</li> <li>• The beginning and end of the line</li> </ul>	_100,100_ _100_

Character	Description	Example
	Therefore, the underscore can be used to match AS values.	

To add an entry for an autonomous system path filter, do the following:

1. Navigate to the **AS Path** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select an autonomous system path filter, and then click **Entry**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ deny   permit ] Action.
Match	<b>Synopsis:</b> A string up to 1024 characters long The regular expression to match the BGP AS paths - for more information about regular expressions, refer to the User Guide.

5. Click **Add** to create the new entry.
6. Click **OK** to create the new entry..
7. Commit the change.

### 12.8.5.5 Deleting an Autonomous System Path

To delete an autonomous system path filter for dynamic BGP routes, do the following:

1. Navigate to the **AS Path** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select the filter to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.8.5.6 Deleting an Autonomous System Path Filter Entry

To delete an entry for an autonomous system path filter, do the following:

1. Navigate to the **AS Path** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select an autonomous system path filter, and then click **Entry**.
3. Select the entry to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.8.6 Managing Neighbors

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for BGP to operate.

### Note

If neighbors are specified but no networks are specified, the router will receive BGP routing information from its neighbors but will not advertise any routes to them. For more information about networks, refer to "Managing Networks" (Page 500).

### 12.8.6.1 Viewing a List of Neighbors

To view a list of neighbors configured for a BGP network, navigate to the **Neighbor** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If neighbors have been configured, a list appears.

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 497).

### 12.8.6.2 Adding a Neighbor

To add a neighbor for a BGP network, do the following:

1. Navigate to the **Neighbor** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Under **Neighbor**, click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The neighbor IP address.

4. Click **OK** to add the address.
5. [Optional] Enable the neighbor as a route reflector client by configuring the following parameter:

Parameter	Description
Enable Reflector Client	If enabled and Route Reflector enabled, makes this neighbor a client for Route Reflector.

6. [Optional] Configure the following parameter(s) as required:

Parameter	Description
Route Map In	<b>Synopsis:</b> A string between 1 and 1024 characters long Apply route map to incoming routes.

Parameter	Description
Route Map Out	<b>Synopsis:</b> A string between 1 and 1024 characters long Apply route map to outbound routes.
Neighbor Autonomous System ID	<b>Synopsis:</b> An integer between 1 and 4294967295 A BGP neighbor.
EBGP Multihop Count	<b>Synopsis:</b> An integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
Maximum Prefix	<b>Synopsis:</b> An integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
Next Hop Itself	Disables the next hop calculation for this neighbor.
Password	<b>Synopsis:</b> A string Password.
Update Source	<b>Synopsis:</b> A string between 7 and 15 characters long Source IP address of routing updates.
Disable Connected Check	Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
Soft Reconfiguration	Per neighbor soft reconfiguration.
Weight	<b>Synopsis:</b> An integer The default weight for routes from this neighbor.

7. Commit the change.

### 12.8.6.3 Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in a BGP network, do the following:

1. Make sure the desired prefix list is configured for the BGP network. For more information, refer to "Adding a Prefix List" (Page 492).
2. Navigate to the **Neighbor** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
3. Select a neighbor, and then click **Distribute Prefix List**.
4. Select the **Enabled** check box under either **In** or **Out**, depending on the direction of the route (incoming or outbound).
5. Select the desired prefix list.
6. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands for BGP Neighbors" (Page 499).

- Commit the change.

#### 12.8.6.4 Tracking Commands for BGP Neighbors

Network commands can be tracked using event trackers configured under **Layer 3 » Tracking**. For more information about event trackers, refer to "Managing Event Trackers" (Page 447).

The network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's BGP peers) when the tracked target is unavailable.

To track a command for a BGP neighbor, do the following:

- Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
- Select a BGP network, and then click **Track**.
- Under **Track**, click the **Enabled** check box.
- Configure the following parameter(s) as required:

##### Note

For information about creating event trackers, refer to "Adding an Event Tracker" (Page 449).

Parameter	Description
Event	<b>Synopsis:</b> A string up to 64 characters long Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state.
Apply When	<b>Synopsis:</b> [ up   down ] <b>Default:</b> up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

- Click **Add** to create the tracker.
- Commit the change.

#### 12.8.6.5 Deleting a Neighbor

To delete a neighbor from a BGP network, do the following:

- Navigate to the **Neighbor** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
- Select the neighbor to be deleted, and then click **Delete Entry**.

3. Commit the change.

## 12.8.7 Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

---

### Note

For point-to-point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to "Adding a Neighbor" (Page 497).

---

### Note

Networks for the BGP protocol do not require a valid entry in the routing table. Since BGP is a broader gateway protocol, a more general network specification would typically be entered. For example, if a routed network inside the Autonomous System (AS) was comprised of many different Class C subnets (/24) of the 192.168.0.0/16 range, it is more efficient to advertise the one Class B network specification, 192.168.0.0/16, to its BGP neighbors.

---

### Note

If neighbors are specified but no networks are specified, the router will receive routing information from its neighbors but will not advertise any routes to them. For more information about neighbors, refer to "Managing Neighbors" (Page 497).

---

### 12.8.7.1 Viewing a List of Networks

To view a list of networks configured for the BGP protocol, navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If networks have been configured, a list appears.

If no networks have been configured, add networks as needed. For more information, refer to "Adding a Network" (Page 500).

### 12.8.7.2 Adding a Network

To add a network for the BGP protocol, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address/Prefix	<b>Synopsis:</b> A string between 9 and 18 characters long IP address/prefix.

4. Click **OK** to create the network.
5. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands for a BGP Network" (Page 501).
6. Commit the change.

### 12.8.7.3 Tracking Commands for a BGP Network

Network commands can be tracked using event trackers configured under **Layer 3 » Tracking**. For more information about event trackers, refer to "Managing Event Trackers" (Page 447).

The network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's BGP peers) when the tracked target is unavailable.

To track a command for a BGP network, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a BGP network, and then click **Track**.
3. Select the **Enabled** check box.
4. Configure the following parameter(s) as required:

#### Note

For information about creating event trackers, refer to "Adding an Event Tracker" (Page 449).

Parameter	Description
Event	<b>Synopsis:</b> A string up to 64 characters long Select an event.
Apply When	<b>Synopsis:</b> [ up   down ] <b>Default:</b> up Advertises the network when the tracked event state goes UP or stops advertising the network when the tracked event goes DOWN.

5. Commit the change.



#### 12.8.7.4 Deleting a Network

To delete a network configured for the BGP protocol, do the following:

1. Navigate to the **Network** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select the network to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.8.8 Managing Aggregate Addresses

This section describes how to aggregate multiple addresses into a single dynamic BGP route.

#### 12.8.8.1 Viewing a List of Aggregate Addresses

To view a list of aggregate addresses for dynamic BGP routes, navigate to the **Aggregate Address** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If addresses have been configured, a list appears.

If no aggregate addresses have been configured, add addresses as needed. For more information, refer to "Adding an Aggregate Address" (Page 502).

#### 12.8.8.2 Adding an Aggregate Address

To add an aggregate address for dynamic BGP routes, do the following:

1. Navigate to the **Aggregate Address** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Click **Add Entry**, and then configure the following parameter(s) as required:

Parameter	Description
Subnet	<b>Synopsis:</b> A string between 9 and 18 characters long subnet (xxx.xxx.xxx.xxx/xx).

3. Click **OK** to add the address.
4. If necessary, configure options for the address. For more information, refer to "Adding an Aggregate Address Option" (Page 503).
5. Commit the change.

### 12.8.8.3 Deleting an Aggregate Address

To delete an aggregate address for dynamic BGP routes, do the following:

1. Navigate to the **Aggregate Address** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select the address to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.8.9 Managing Aggregate Address Options

This section describes how to set the **as-set** and **summary-only** options for BGP aggregate addresses.

### 12.8.9.1 Viewing a List of Aggregate Address Options

1. To view a list of options for an aggregate address, navigate to the **Aggregate Address** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select an aggregate address, and then click **Options**. If options have been configured, a list appears.

If no options have been configured, add options as needed. For more information, refer to "Adding an Aggregate Address Option" (Page 503).

### 12.8.9.2 Adding an Aggregate Address Option

To add an option for an aggregate address, do the following:

1. Navigate to the **Aggregate Address** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select an aggregate address, and then click **Options**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Value	<b>Synopsis:</b> [ as-set   summary-only ] Aggregate address option.

5. Click **OK** to add the option.
6. Commit the change.

**12.8.9.3 Deleting an Aggregate Address Option**

To delete an option for an aggregate address, do the following:

1. Navigate to the **Aggregate Address** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select an aggregate address, and then click **Options**.
3. Select the option to be deleted, and then click **Delete Entry**.
4. Commit the change.

**12.8.10 Managing Redistribution Metrics**

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the BGP network, can also be advertised.

**12.8.10.1 Viewing a List of Redistribution Metrics**

To view a list of redistribution metrics for dynamic BGP routes, navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » BGP**. If metrics have been configured, a list appears.

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 504).

**12.8.10.2 Adding a Redistribution Metric**

To add a redistribution metric for dynamic BGP routes, do the following:

1. Navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Click **Add Entry**, and then configure the following parameter(s) as required:

Parameter	Description
Metric	<b>Synopsis:</b> An integer Metric value for redistributed routes.

3. Click **OK** to add the metric.
4. Configure the following parameter(s) as required:

Parameter	Description
Metric	<b>Synopsis:</b> An integer Metric value for redistributed routes.

5. Commit the change.

### 12.8.10.3 Deleting a Redistribution Metric

To delete a redistribution metric for dynamic BGP routes, do the following:

1. Navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select the metric to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.8.11 Managing Route Reflector Options

This section describes how to configure the device as a route reflector for BGP networks.

### 12.8.11.1 Understanding Route Reflectors

Route reflectors offer a method for simplifying BGP network topologies and improving scalability.

#### The Full-Mesh Requirement

Due to BGP route advertisement rules, BGP requires a logical full-mesh topology, wherein each router advertises and forwards its routes to each of its neighbors. This requirement is easily met by external BGP (eBGP) networks, where connections are established between Autonomous Systems (AS). Routers can easily avoid loops by dropping any routes that share the same AS numeric identifier. However, in internal BGP (iBGP), each router shares the same AS numeric identifier, so all routes received by a router would be dropped.

One method for solving this problem is to have each iBGP router establish neighborship with its peers, but that would result in a significant number of BGP sessions and unnecessary traffic on large networks. The formula for determining the number of BGP sessions for X number of routers is  $X*(X-1)/2$ . Therefore, 20 iBGP routers would generate 190 BGP sessions ( $20*[20-1]/2 = 190$ ).

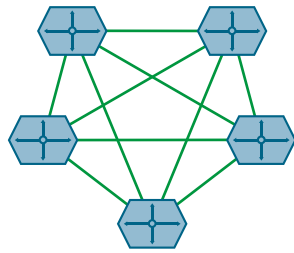


Figure 12.2 A Simple BGP Topology Without a Route Reflector

### The Route Reflector Solution

Route reflectors simplify the topology by grouping routers into a cluster. In the cluster, the route reflector establishes a BGP session with each client (BGP neighbor). The clients are not required to establish BGP sessions with each other, nor are they required to be fully-meshed. All routes are advertised to the route reflector, who in turn reflects the routes to its clients, thus meeting the logical full-mesh requirement. RUGGEDCOM ROX II does not use BGP routes to resolve BGP next-hop values.

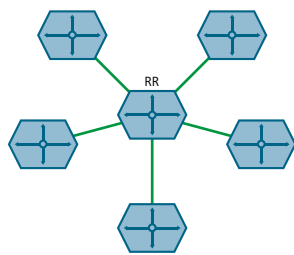
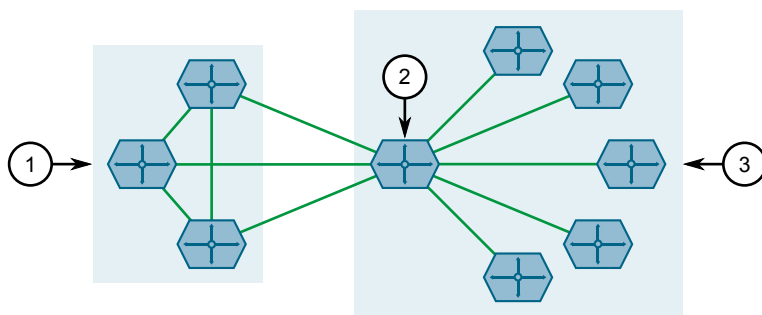


Figure 12.3 A Simple BGP Topology With a Route Reflector

Route reflectors can also share routes with routers outside of their clusters. These are referred to as *non-clients*. Non-clients are required to be fully-meshed.



- ① Fully Meshed iBGP Peers (Non-Clients)
- ② Route Reflector
- ③ Cluster (Clients)

Figure 12.4 A Complex BGP Topology

### Combining Clusters for Scalability

Multiple clusters can be linked together via their route reflectors to form a full-mesh topology of internal peers. In this configuration, routes advertised to a route reflector are not only re-advertised to its clients, but also with the other route reflectors who in turn advertise the routes to their clients. This allows routes to propagate through the entire AS without the scaling problems associated with the full-mesh requirement.

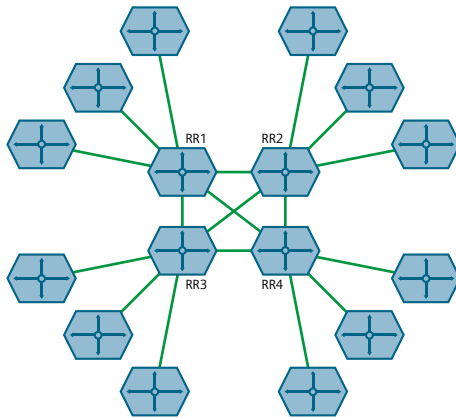


Figure 12.5 Multiple Clusters Fully-Meshed

Route reflectors can also be partially-meshed by combining them in a cluster of their own.

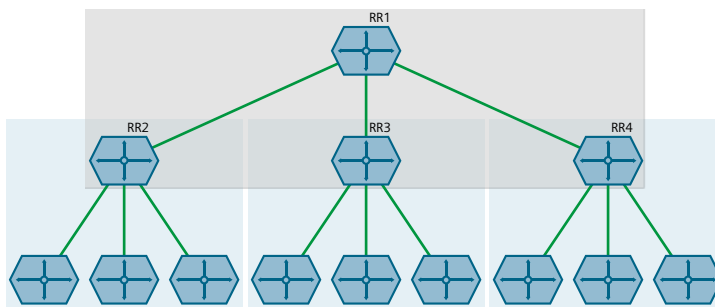
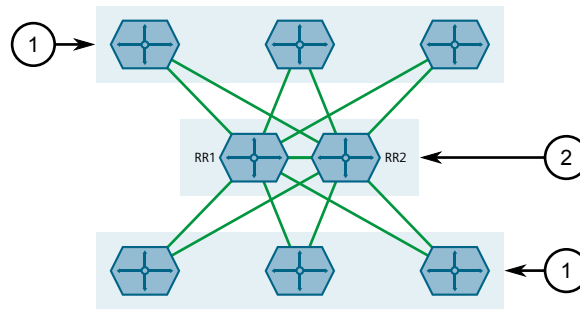


Figure 12.6 Multiple Clusters Partially-Meshed

### Redundant Route Reflectors

To avoid a single point of failure in the BGP network, each cluster should be served by more than one route reflector to provide redundancy in case of failure. In this arrangement, each route reflectors are configured to have the same BGP neighbors as clients.



- ① Cluster
- ② Route Reflector

Figure 12.7 Redundant Route Reflector Topology

### 12.8.11.2 Configuring the Device as a Route Reflector

To configure the device to be a route reflector for a specific cluster, do the following:

1. Navigate to the **Router Parameters** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Configure the following parameters as required:

Parameter	Description
Enable Route Reflector	When enabled, sets this router as a Route Reflector.
Cluster ID	<b>Synopsis:</b> A string between 7 and 15 characters long The ID of the BGP cluster to which the device belongs. The ID is expressed as an IPv4 address (e.g. 1.2.3.4).

3. Configure one or more BGP neighbors to be clients of the device. For more information, refer to "Configuring BGP Neighbors as Clients" (Page 508).
4. Commit the change.

### 12.8.11.3 Configuring BGP Neighbors as Clients

When the device is configured to be a route reflector, BGP neighbors can then be configured to be clients of the reflector.

#### BGP Neighbors

To configure a BGP neighbor to be a client of the device, do the following:

1. Make sure a BGP neighbor is defined. For more information, refer to "Adding a Neighbor" (Page 497).

2. Navigate to the **Neighbor** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
3. Select a neighbor.
4. Under **Enable Reflector Client**, select the check box.
5. Commit the change.

### BGP Neighbors In an IPv4 Address Family

To configure a BGP neighbor that belongs to an IPv4 address family to be a client of the device, do the following:

1. Make sure an IPv4 address family is defined. For more information, refer to "Adding an IPv4 Address Family" (Page 569).
2. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
3. Under **IPv4VRF**, select a VRF, and then click **Neighbor**.
4. Select a neighbor.
5. Under **Enable Reflector Client**, select the check box.
6. Commit the change.

### BGP Neighbors In a VPNv4 Address Family

To configure a BGP neighbor that belongs to a VPNv4 address family to be a client of the device, do the following:

1. Make sure a VPNv4 address family is defined. For more information, refer to "Adding a Neighbor" (Page 568).
2. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
3. Under **VPNv4**, select an address.
4. Under **Enable Route Reflector Client**, select the check box.
5. Commit the change.

#### 12.8.11.4 Example: Basic Route Reflection

This example demonstrates how to configure a partially-meshed Autonomous System (AS) where a route reflector advertises routes to clients and non-clients.

#### Overview

In the following topology, routes advertised by the external BGP (eBGP) router (labeled as R1) are forwarded to the route reflector (labeled as RR). The route reflector then in turn readvertises the routes to its BGP neighbors. Neighbors within



the route reflector's cluster are the clients (labeled C1, C2 and C3). Neighbors outside of the cluster are non-clients (labeled NC1, NC2 and NC3).

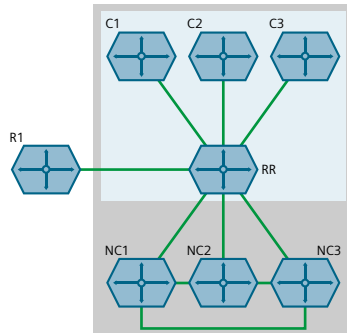


Figure 12.8 Basic Route Reflection Topology

Similarly, routes advertised by a non-client (NC1, NC2 or NC3) are forwarded to its BGP neighbors, including the route reflector. The route reflector in turn readvertises the routes to its BGP neighbors, which includes those in its cluster and the eBGP router (R1).

With the exception of the eBGP router (R1), all devices are within the same Autonomous System (AS).

## Configuration

To configure the device to act as the route reflector in this scenario, do the following:

1. Enable the route reflector feature and assign a cluster ID to the device. For more information, refer to "Configuring the Device as a Route Reflector" (Page 508).
2. For each router that advertises and forwards routes to the route reflector, define a BGP neighbor. Make sure each belongs to the same AS. For more information, refer to "Adding a Neighbor" (Page 497).
3. For each BGP neighbor that belongs to the route reflector's cluster, enable the neighbor as a route reflector client. For more information, refer to "Configuring BGP Neighbors as Clients" (Page 508).

## Final Configuration Example

```

routing bgp
  enabled
  as-id 100
  route-reflector enabled
  route-reflector cluster-id 10.11.12.13
  !
  neighbor 172.30.140.10 { Client }
  remote-as 100
  route-reflector-client enabled
  !
  neighbor 172.30.140.20 { Client }
  remote-as 100
  route-reflector-client enabled
  !
  neighbor 172.30.140.30 { Client }

```

```

remote-as 100
route-reflector-client enabled
!
neighbor 172.30.150.10          { Non-Client }
remote-as 100
no route-reflector-client enabled
!
neighbor 172.30.150.20        { Non-Client }
remote-as 100
no route-reflector-client enabled
!
neighbor 172.30.150.30        { Non-Client }
remote-as 100
no route-reflector-client enabled
!
!
!

```

### 12.8.11.5 Example: Linking Clusters

This example demonstrates how to link two multiple clusters together by connecting each route reflector in a full-mesh topology.

#### Overview

In the following topology, three route reflectors (RR1, RR2 and RR3) are internal peers of one another.

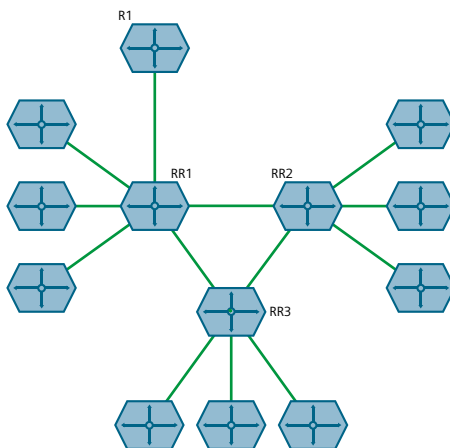


Figure 12.9 Linked Clusters

When an external BGP (eBGP) router (R1) advertises routes to RR1, RR1 readvertises the routes to RR2, RR3 and its clients. RR2 and RR3 then readvertise the routes again to their clients.

## Configuration

To configure this topology, do the following:

1. Configure the clusters for RR1, RR2, RR3. For more information, refer to "Configuring the Device as a Route Reflector" (Page 508).
2. For each route reflector, define the other route reflectors as BGP neighbors. For more information, refer to "Adding a Neighbor" (Page 497).

## Final Configuration Example

### RR1 (172.30.110.10)

```
routing bgp
enabled
as-id 100
route-reflector cluster-id 0.1.2.3
!
neighbor 172.30.110.20 { RR2 }
remote-as 100
no route-reflector-client enabled
!
neighbor 172.30.110.30 { RR3 }
remote-as 100
no route-reflector-client enabled
!
neighbor 172.30.140.10 { Client }
remote-as 100
route-reflector-client enabled
!
neighbor 172.30.140.20 { Client }
remote-as 100
route-reflector-client enabled
!
neighbor 172.30.140.30 { Client }
remote-as 100
route-reflector-client enabled
!
!
```

### RR2 (172.30.110.20)

```
routing bgp
enabled
as-id 100
route-reflector cluster-id 10.11.12.13
!
neighbor 172.30.110.10 { RR1 }
remote-as 100
no route-reflector-client enabled
!
neighbor 172.30.110.30 { RR3 }
remote-as 100
no route-reflector-client enabled
!
neighbor 172.30.150.10 { Client }
remote-as 100
route-reflector-client enabled
!
neighbor 172.30.150.30 { Client }
remote-as 100
route-reflector-client enabled
!
!
```

```
neighbor 172.30.150.20          { Client }
  remote-as 100
  route-reflector-client enabled
!
!
```

### RR3 (172.30.110.30)

```
routing bgp
  enabled
  as-id          100
  route-reflector cluster-id 20.21.22.23
  !
  neighbor 172.30.110.10      { RR1 }
    remote-as 100
    no route-reflector-client enabled
  !
  neighbor 172.30.110.20      { RR2 }
    remote-as 100
    no route-reflector-client enabled
  !
  neighbor 172.30.160.10      { Client }
    remote-as 100
    route-reflector-client enabled
  !
  neighbor 172.30.160.20      { Client }
    remote-as 100
    route-reflector-client enabled
  !
  !
```

#### 12.8.11.6 Example: Clusters in Clusters

This example demonstrates how to group clusters into a hierarchical structure (clusters of clusters).

#### Overview

In the following topology, a route reflector (RR1) forms a cluster with two other route reflectors (RR2 and RR3). RR2 and RR3 are also part of their own individual clusters, each of which consists of three clients.

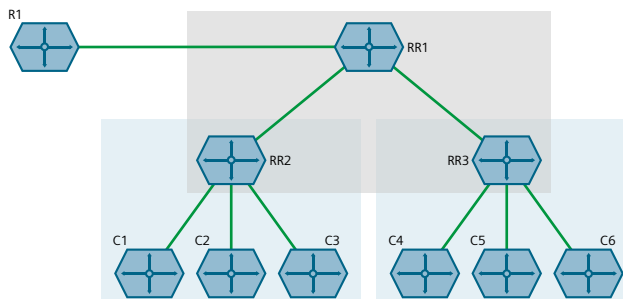


Figure 12.10 Hierarchical Clusters Topology

When an external BGP (eBGP) router (R1) advertises routes to RR1, RR1 readvertises the routes to RR2 and RR3. RR2 and RR3 then readvertise the routes again to their clients.

## Configuration

To configure this topology, do the following:

1. Configure the clusters for RR2 and RR3. For more information, refer to "Configuring the Device as a Route Reflector" (Page 508).
2. Configure RR1 as a route reflector and define RR2 and RR3 as its clients. For more information, refer to "Configuring the Device as a Route Reflector" (Page 508).

## Final Configuration Example

### RR1 (172.30.140.10)

```

routing bgp
  enabled
  as-id          100
  route-reflector enabled
  route-reflector cluster-id 0.1.2.3
  !
  neighbor 172.30.140.20          { RR2 }
    remote-as 100
    route-reflector-client enabled
  !
  neighbor 172.30.140.30          { RR3 }
    remote-as 100
    route-reflector-client enabled
  !

```

### RR2 (172.30.140.20)

```

routing bgp
  enabled
  as-id          100
  route-reflector enabled
  route-reflector cluster-id 10.11.12.13
  !
  neighbor 172.30.140.10          { RR1 }
    remote-as 100
    no route-reflector-client enabled
  !
  neighbor 172.30.150.10          { Client }
    remote-as 100
    route-reflector-client enabled
  !
  neighbor 172.30.150.20          { Client }
    remote-as 100
    route-reflector-client enabled
  !
  neighbor 172.30.150.30          { Client }
    remote-as 100
    route-reflector-client enabled
  !
  !

```

### RR3 (172.30.140.30)

```

routing bgp
  enabled
  as-id 100
  route-reflector enabled
  route-reflector cluster-id 20.21.22.23
  !
  neighbor 172.30.140.10 { RR1 }
    remote-as 100
    no route-reflector-client enabled
  !
  neighbor 172.30.160.10 { Client }
    remote-as 100
    route-reflector-client enabled
  !
  neighbor 172.30.160.20 { Client }
    remote-as 100
    route-reflector-client enabled
  !
  neighbor 172.30.160.30 { Client }
    remote-as 100
    route-reflector-client enabled
  !
  !

```

### 12.8.11.7 Example: Route Reflection in a VRF Instance

This example demonstrates how to configure BGP route reflection in a VRF instance.

#### Overview

In the following topology, router RR is a BGP route reflector configured with a VRF instance (VRF1). The VRF instance is configured with a single IPv4 address family consisting of routers R2 and R3. All three routers belong to the same autonomous system (AS1).

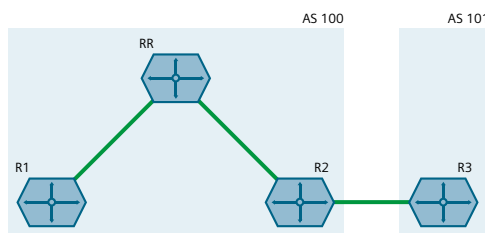


Figure 12.11 Route Reflection in a VRF Instance

RR receives BGP routing information from R2 via its VRF interface, 1.1.2.1. It then readvertises the information to its client, R1.

R2 receives BGP routing information from R3, an external BGP (eBGP) router.

## Configuration

To configure this topology, do the following:

### 1. Configure RR

- a. Configure a VRF definition for *VRF1* with a route distinguisher of **100:1**. For more information, refer to "Adding a VRF Definition" (Page 562).
- b. Define a route target for *VRF1* of type **both** with the export community set to **100:1**. For more information, refer to "Adding a Route Target" (Page 563).
- c. Make sure interfaces are configured with the IP addresses 1.1.12/24 and 1.1.2.1/24.
- d. Assign the interfaces in step 1c (Page 516) to forward traffic to *VRF1*. For more information, refer to "Configuring a VRF Interface" (Page 560).
- e. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	100
Router ID	5.5.5.5

- f. Enable the router as a BGP route reflector and set the cluster ID to **5.5.5.5**. For more information, refer to "Configuring the Device as a Route Reflector" (Page 508).
- g. Define an IPv4 address family for *VRF1* with the following neighbors:

- **Neighbor 1.1.1.1**

Parameter	Value
Neighbor IP Address	1.1.1.1
Autonomous System ID	100
Route Reflector Client	Enabled

- **Neighbor 1.1.2.2**

Parameter	Value
Neighbor IP Address	1.1.2.2
Autonomous System ID	100
Route Reflector Client	Enabled

For more information, refer to "Adding an IPv4 Address Family" (Page 569).

- h. Define a redistribution metric for IPv4 family of type **connected**. For more information, refer to "Adding a Redistribution" (Page 571).

### 2. Configure R1

- a. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	100
Router ID	5.5.5.1

For more information, refer to "Configuring BGP" (Page 484).

- b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.1.2
Autonomous System ID	100

For more information, refer to "Adding a Neighbor" (Page 497).

- c. Define a redistribution metric for BGP of type **connected**. For more information, refer to "Adding a Redistribution Metric" (Page 504).

### 3. Configure R2

- a. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	100
Router ID	5.5.5.2

For more information, refer to "Configuring BGP" (Page 484).

- b. Define the following BGP neighbors:

- **Neighbor 1.1.2.1**

Parameter	Value
Neighbor IP Address	1.1.2.1
Autonomous System ID	100

- **Neighbor 1.1.3.2**

Parameter	Value
Neighbor IP Address	1.1.3.2
Autonomous System ID	101

For more information, refer to "Adding a Neighbor" (Page 497).

- c. Define a redistribution metric for BGP of type **connected**. For more information, refer to "Adding a Redistribution Metric" (Page 504).

### 4. Configure R3

- a. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	101
Router ID	5.5.5.3

For more information, refer to "Configuring BGP" (Page 484).

- b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.3.1
Autonomous System ID	101



For more information, refer to "Adding a Neighbor" (Page 497).

- c. Define a redistribution metric for BGP of type **connected**. For more information, refer to "Adding a Redistribution Metric" (Page 504).

## Verification

Verify the configuration by navigating to **routing » status » bgp » route** on R1. The following routes should be displayed:

NETWORK	ADDRESS	SELECTED	INTERNAL	METRIC	LOCAL PREFERENCE	WEIGHT	AS PATH	ORIGIN
1.1.1.0/30	1.1.1.2	true	true	0	100	0		Unspecified
1.1.2.0/30	1.1.1.2	true	true	0	100	0		Unspecified
1.1.3.0/30	1.1.2.2	true	true	0	100	0		Unspecified

## Final Configuration Example

### RR Configuration

```
global
vrf
  definition vrf1
    rd 100:1
    route-target both 100:1
ip fe-1-1
vrf-forwarding vrf1
ipv4
  address 1.1.1.2/30
ip fe-1-2
vrf-forwarding vrf1
ipv4
  address 1.1.2.1/30
routing bgp
enabled
as-id 100
router-id 5.5.5.5
route-reflector enabled
route-reflector cluster-id 5.5.5.5
address-family ipv4
vrf vrf1
  redistribute connected
  neighbor 1.1.1.1
  remote-as 100
  route-reflector-client enabled
neighbor 1.1.2.2
  remote-as 100
  route-reflector-client enabled
```

### R1 Configuration

```
routing bgp
enabled
as-id 100
router-id 5.5.5.1
neighbor 1.1.1.2
  remote-as 100
redistribute connected
```

### R2 Configuration

```
routing bgp
enabled
as-id 100
router-id 5.5.5.2
neighbor 1.1.2.1
  remote-as 100
neighbor 1.1.3.2
  remote-as 101
redistribute connected
```

### R3 Configuration

```
routing bgp
enabled
as-id 100
router-id 5.5.5.3
neighbor 1.1.3.1
  remote-as 100
redistribute connected
```

### 12.8.11.8 Example: Route Reflection with VPNv4 Clients

BGP route reflection can be used to advertise VPNv4 routes between Provider Edge (PE) devices inside a provider network. This specific application is complicated by the fact that VPNv4 routes to the Customer Edge (CE) devices are within VRFs that are not known to the global VRF shared by each PE device.

For more information about configuring this type of topology, refer to the application description "[Using BGP Route Reflection with VPNv4 Clients \[https://support.industry.siemens.com/cs/ww/en/view/109757209\]](https://support.industry.siemens.com/cs/ww/en/view/109757209)".

## 12.8.12 Viewing the Status of Dynamic BGP Routes

To view the status of the dynamic BGP routes configured on the device, navigate to the **Route** tab under **Layer 3 » Routing » Status » Dynamic Routing » BGP**, and then click **Network**. If BGP routes have been configured, a list appears.

The following information is provided:

Parameter	Description
Network	<b>Synopsis:</b> A string Network.
Address	<b>Synopsis:</b> A string Next-hop address.
Selected	<b>Synopsis:</b> [ true   false ] Selected next-hop for this route.
Internal	<b>Synopsis:</b> [ true   false ] Internal route.
Metric	<b>Synopsis:</b> A string Metric.
Local Preference	<b>Synopsis:</b> A string Local preference.
Weight	<b>Synopsis:</b> An integer Weight.
AS Path	<b>Synopsis:</b> A string AS path.
Origin	<b>Synopsis:</b> A string Origin.

To view the routing information advertised to the network by a BGP neighbor, navigate to the **Neighbor** tab under **Layer 3 » Routing » Status » Dynamic Routing » BGP**. Select a configuration, and then click **Advertised Route**.

The following information is provided:

Parameter	Description
Network	<b>Synopsis:</b> A string Network.
Next Hop	<b>Synopsis:</b> A string Next-hop address.
Selected	<b>Synopsis:</b> [ true   false ] Selected next-hop for this route.
Internal	<b>Synopsis:</b> [ true   false ] Internal route.
Metric	<b>Synopsis:</b> An integer Metric value.
Local Preference	<b>Synopsis:</b> A string Local preference.
Weight	<b>Synopsis:</b> An integer Weight.
AS Path	<b>Synopsis:</b> A string Path.
Origin	<b>Synopsis:</b> A string Origin.

If no dynamic BGP routes have been configured, configure BGP and add routes as needed. For more information about configuring BGP, refer to "Configuring BGP" (Page 484).

### 12.8.13 Resetting a BGP Session

Whenever there is a change in the routing policy due to a configuration change, the BGP session must be reset for the new policy to take effect.

RUGGEDCOM ROX II allows users to perform either a hard or soft reset on both incoming and outbound sessions, as selected.

A BGP session can be reset for all routing tables, or for a specified neighbor.

## Resetting All BGP Sessions

To reset all BGP sessions, do the following:

1. Navigate to the **Router Parameters** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Under **Reset All Peer Sessions**, click **Perform** and then configure the following parameter(s) as required:

Parameter	Description
Reset Type	<p><b>Synopsis:</b> [ hard   soft-inbound   soft-outbound   soft ]</p> <p>The method for resetting all BGP peering sessions. Options include:</p> <ul style="list-style-type: none"> <li>• hard: Tears down and re-establishes all BGP sessions.</li> <li>• soft: The existing peering sessions continue to run while running both inbound and outbound actions.</li> <li>• soft-inbound: The existing peering sessions continue to run while generating inbound updates from all neighbors.</li> <li>• soft-outbound: The existing peering sessions continue to run while sending outbound updates to all neighbors.</li> </ul>

3. Click **OK** to reset all BGP sessions as configured.

## Resetting a BGP Session for a Specified Neighbor

To reset a BGP session for a specified neighbor, do the following:

1. Navigate to the **Neighbor** tab under **Layer 3 » Routing » Dynamic Routing » BGP**.
2. Select a neighbor.
3. Under **Peer Reset**, click **Perform** and then configure the following parameter(s) as required:

Parameter	Description
Reset Type	<p><b>Synopsis:</b> [ hard   soft-inbound   soft-outbound   soft ]</p> <p>The method for resetting the selected BGP peering session. Options include:</p> <ul style="list-style-type: none"> <li>• hard: Tears down the existing peering session then re-establishes it.</li> <li>• soft: The existing peering session continues to run while running both inbound and outbound actions.</li> <li>• soft-inbound: The existing peering session continues to run while generating inbound updates from its neighbor.</li> <li>• soft-outbound: The existing peering session continues to run while sending outbound updates to its neighbor.</li> </ul>

4. Click **OK** to reset the peer session for the selected neighbor.

## 12.9 Managing OSPF

The Open Shortest Path First (OSPF) protocol determines the best path for routing IP traffic over a TCP/IP network based on link cost and quality. Unlike static routing, OSPF takes link failures and other network topology changes into account. OSPF also differs from RIP in that it provides less router to router update traffic.

The RUGGEDCOM ROX II OSPF daemon (ospfd) is an [RFC 2178](http://tools.ietf.org/html/rfc2178) [http://tools.ietf.org/html/rfc2178] compliant implementation of OSPF version 2. The daemon also adheres to the Opaque LSA ([RFC 2370](http://tools.ietf.org/html/rfc2370) [http://tools.ietf.org/html/rfc2370]) and ABR-Types ([RFC 3509](http://tools.ietf.org/html/rfc3509) [http://tools.ietf.org/html/rfc3509]) extensions.

OSPF network design usually involves partitioning a network into a number of self-contained areas. The areas are chosen to minimize intra-area router traffic, making more manageable and reducing the number of advertised routes. Area numbers are assigned to each area. All routers in the area are known as Area routers. If traffic must flow between two areas a router with links in each area is selected to be an Area Border router, and serves as a gateway.

---

### Note

The **Router ID** parameter defines the ID of the router. By default this is the highest IP assigned to the router. It is recommended to configure this value manually to avoid the ID changing if interfaces are added or deleted from the router. During elections for the master router, the ID is one of the values used to pick the winner. Keeping the ID fixed will avoid any unexpected changes in the election of the master router.

---

### Note

In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

---

### Note

Specific routes for Virtual Routing and Forwarding (VRF) interfaces can be configured. For more information about VRF, refer to "Managing Virtual Routing and Forwarding (VRF)" (Page 558).

---

### 12.9.1 OSPF Concepts

When an OSPF configured router starts operating, it issues a *hello* packet. Routers having the same OSPF Area, hello-interval and dead-interval timers will communicate with each other and are said to be neighbors.

After discovering its neighbors, a router will exchange Link State Advertisements in order to determine the network topology.

Every 30 minutes (by default), the entire topology of the network must be sent to all routers in an area.

If the link speeds are too low, the links are too busy or there are too many routes, some routes may fail to get re-announced and will be aged out.

Splitting the network into smaller areas to reduce the number of routes within an area or reducing the number of routes to be advertised may help to avoid this problem.

In shared access networks (i.e. routers connected by switches or hubs) a designated router and a backup designated are elected to receive route changes from subnets in the area. Once a designated router is picked, all routing state changes are sent to the designated router, which then sends the resulting changes to all the routers.

The election is decided based on the priority assigned to the interface of each router. The highest priority wins. If the priority is tied, the highest router-id wins.

## 12.9.2 Configuring OSPF

To configure dynamic routing using the Open Shortest Path First (OSPF) daemon, do the following:

1. Navigate to the **Router Parameters** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**, and then select **Distance**.
2. Configure the following parameters:

Parameter	Description
External Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for external routes.
Inter Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for inter-area routes.
Intra Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for intra-area routes.

3. Select **Configurations**, and then configure the following parameters:

Parameter	Description
Enable OSPF	Enables the OSPF dynamic routing protocol.
ABR Type	<b>Synopsis:</b> [ cisco   ibm   shortcut   standard ] <b>Default:</b> cisco The OSPF ABR type.
Auto Cost Reference Bandwidth	<b>Synopsis:</b> An integer between 1 and 4294967 <b>Default:</b> 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
Compatible with RFC1583	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)

Parameter	Description
Default Information Originate	Advertises the default route.
Default Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The default metric of redistribute routes.
Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance.
Enable Opaque-LSA capability	Enables the Opaque-LSA capability (RFC2370).
Passive Default	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Default passive value for new interface.
Refresh Timer	<b>Synopsis:</b> An integer between 10 and 1800 <b>Default:</b> 10 The refresh timer.
Router ID	<b>Synopsis:</b> A string between 7 and 15 characters long The Router ID for OSPF.

4. If **Default Information Originate** was enabled on the **OSPF Configuration** form, select **Default Information Originate**.
5. Configure the following parameters:

Parameter	Description
Always Advertise Default Route	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Always advertise default route even when there is no default route present in routing table.
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric value for default route.
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 <b>Default:</b> 2 The metric type for default route.
Route Map	<b>Synopsis:</b> A string between 1 and 1024 characters long The route map name.

6. Configure prefix list filters. For more information, refer to "Adding a Prefix List" (Page 527).
7. Configure areas. For more information, refer to "Adding an Area" (Page 530).

8. Configure route map filters. For more information, refer to "Adding a Route Map Filter" (Page 532).
9. Configure redistribution metrics. For more information, refer to "Adding a Redistribution Metric" (Page 537).
10. Configure interfaces. For more information, refer to "Configuring a Routing Interface" (Page 539).
11. Commit the changes.

### 12.9.3 Viewing the Status of Dynamic OSPF Routes

1. To view the status of the dynamic OSPF routes configured on the device, navigate to the **Route** tab under **Layer 3 » Routing » Status » Dynamic Routing » OSPF**.
2. Click **Network**. If OSPF routes have been configured, a list appears.  
The following information is provided:

Parameter	Description
Destination	<b>Synopsis:</b> A string Destination (network or discard).
Path Type	<b>Synopsis:</b> A string Path type (inter-area or intra-area).
Cost	<b>Synopsis:</b> A string Cost.
Area	<b>Synopsis:</b> A string Area.

If no dynamic OSPF routes have been configured, configure OSPF and add routes as needed. For more information about configuring OSPF, refer to "Configuring OSPF" (Page 523).

### 12.9.4 Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the OSPF daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

#### 12.9.4.1 Viewing a List of Prefix Lists

Users can view a list of prefix lists for standard dynamic OSPF routes and VRF routes via OSPF.



### Standard Dynamic OSPF Routes

To view a list of prefix lists for Standard dynamic OSPF routes, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Click **Prefix list**. If prefix lists have been configured, a list appears.

### VRF Routes via OSPF

To view a list of prefix lists for VRF routes via OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
2. Select the **Filter** tab, and then click **Prefix list**. If prefix lists have been configured, a list appears.

If no prefix lists have been configured, add lists as needed. For more information, refer to "Adding a Prefix List" (Page 527).

#### 12.9.4.2 Viewing a List of Prefix Entries

Users can view a list of prefix entries for standard dynamic OSPF routes and VRF routes via OSPF.

### Standard Dynamic OSPF Routes

To view a list of prefix entries for Standard dynamic OSPF routes, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Click **Prefix list**.
3. Select a prefix, and then click **Entry**. If entries have been configured, a list appears.

### VRF Routes via OSPF

To view a list of prefix entries for VRF routes via OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
2. Select the **Filter** tab, and then click **Prefix list**.
3. Select a prefix, and then click **Entry**. If entries have been configured, a list appears.

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 527).

### 12.9.4.3 Adding a Prefix List

To add a prefix list for dynamic OSPF routes, do the following:

1. For prefix lists for Standard dynamic OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Select **Prefix list**.
2. For prefix lists for VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then select **Prefix list**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Prefix	<b>Synopsis:</b> A string between 1 and 1024 characters long The name of the prefix list.

5. Click **OK** to create the new prefix-list.
6. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string up to 1024 characters long The description of the prefix list.

7. Add prefix entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 527).
8. Commit the changes.

### 12.9.4.4 Adding a Prefix Entry

To add an entry for a dynamic OSPF prefix list, do the following:

1. For prefix lists for Standard dynamic OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Prefix list**.
  - c. Select a prefix, and then click **Entry**.
2. For prefix lists for VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Prefix list**.
  - c. Select a prefix, and then click **Entry**.

3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 4294967295 Sequence number of the entry.

5. Click **OK** to create the new entry.
6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ deny   permit ] <b>Default:</b> permit Action.
Subnet	<b>Synopsis:</b> A string between 9 and 18 characters long Network (xxx.xxx.xxx.xxx/xx).
Maximum Prefix to Mask for Subnet	<b>Synopsis:</b> An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
Minimum Prefix to Mask for Subnet	<b>Synopsis:</b> An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

7. Commit the changes.

#### 12.9.4.5 Deleting a Prefix List

To delete a prefix list for dynamic OSPF routes, do the following:

1. For prefix lists for Standard dynamic OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Prefix list**.
2. For prefix lists for VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Prefix list**.

---

#### Note

Deleting a prefix list removes all associate prefix entries as well.

---

3. Select the prefix list to be deleted, and then click **Delete Entry**.
4. Commit the change.

### 12.9.4.6 Deleting a Prefix Entry

To delete an entry for a dynamic OSPF prefix list, do the following:

1. For prefix lists for Standard dynamic OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Prefix list**.
  - c. Select a prefix, and then click **Entry**.
2. For prefix lists for VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Prefix list**.
  - c. Select a prefix, and then click **Entry**.
3. Select the entry to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.9.5 Managing Areas

Network areas determine the regions within which routes are distributed to other routers. The subnets at a particular router can be added to its OSPF Area. The router will advertise these subnets to all routers in its area.

OSPF areas must be designed such that no single link failure will cause the network to be split into two disjointed networks.

A router can be part of multiple areas and function as a gateway between areas. When multiple areas are used on a network, area zero (0) is the backbone area. All areas must have a router connecting them to area zero (0).

### 12.9.5.1 Viewing a List of Areas

To view a list of areas configured for dynamic Standard OSPF routes, navigate to the **Area** tab under **Layer 3 » Routing » VRF » Dynamic Routing » OSPF**.

To view a list of areas configured for dynamic VRF Routes via OSPF, navigate to the **VRF** tab under **Layer 3 » Routing » OSPF - VRF**, select a VRF, and then click the **Area** tab.

If areas have been configured, a list appears.

If no areas have been configured, add areas as needed. For more information, refer to "Adding an Area" (Page 530).

### 12.9.5.2 Adding an Area

To add an area for dynamic OSPF routes, do the following:

1. For Standard dynamic OSPF routes:  
Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. For VRF Routes via OSPF:
  - a. Navigate to the **Area** tab under **Layer 3 » Routing » VRF » Dynamic Routing » OSPF**.
  - b. Select a VRF, and then click the **Area** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Area	<b>Synopsis:</b> A string between 7 and 15 characters long The OSPF Area ID (format: A.B.C.D).
Network	<b>Synopsis:</b> A string between 9 and 18 characters long The OSPF area network/prefix.

5. Click **OK** to create the new area.

#### NOTICE

All areas within the same OSPF network must use the same shortcutting mode.

6. Configure the following parameter(s) as required:

Parameter	Description
Shortcut	<b>Synopsis:</b> [ default   disable   enable ] <b>Default:</b> default Sets the area's shortcutting mode. Options include: <ul style="list-style-type: none"> <li>• <b>Default:</b> If the Area Border Router (ABR) has an active backbone connection, the area is not used for shortcutting and a new bit (S-bit) is not set by the ABR in the router-LSA originated for the area. The opposite is true if the ABR does not have an active backbone connection.</li> <li>• <b>Enable:</b> If the ABR has an active backbone connection, it sets the new bit (S-bit) in the router-LSA originated for the area and uses it for shortcutting. Other ABRs in the area must also report the new bit. However, if the ABR does not have an active backbone connection, it uses the area unconditionally for shortcutting and sets the new bit in the router-LSA originated for the area.</li> <li>• <b>Disable:</b> The ABR does not use this area for shortcutting, or set the new bit (S-bit) in the router-LSA originated for it.</li> </ul>

7. Commit the change.

### 12.9.5.3 Deleting an Area

To delete an area for dynamic OSPF routes, do the following:

1. For Standard dynamic OSPF routes:  
Navigate to the **Area** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. For VRF Routes via OSPF:
  - a. Navigate to the **Area** tab under **Layer 3 » Routing » VRF » Dynamic Routing » OSPF**.
  - b. Select a VRF, and then click the **Area** tab.
3. Select the area to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.9.6 Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed. In RUGGEDCOM ROX II, route maps are configured to filter routes based on their metric value, which defines the cost of the route. Once a match is found, the assigned action is taken.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

### 12.9.6.1 Viewing a List of Route Map Filters

Users can view a list of route map filters for Standard dynamic OSPF routes and VRF routes via OSPF.

#### Standard Dynamic OSPF Routes

To view a list of route map filters for Standard dynamic OSPF routes, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Click **Route Map**. If filters have been configured, a list appears.

#### VRF Routes via OSPF

To view a list of route map filters for VRF routes via OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.

2. Select the **Filter** tab, and then click **Route Map**. If filters have been configured, a list appears.

If no filters have been configured, add filters as needed. For more information, refer to "Adding a Route Map Filter" (Page 532).

### 12.9.6.2 Viewing a List of Route Map Filter Entries

Users can view a list of entries for a route map filter for Standard dynamic OSPF routes and VRF routes via OSPF.

#### Standard Dynamic OSPF Routes

To view a list of entries for a route map filter for Standard dynamic OSPF routes, do the following:

1. Navigate to the **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Click **Route Map**.
3. Select a route map, and then click **Entry**. If entries have been configured, a list appears.

#### VRF Routes via OSPF

To view a list of entries for a route map filter for VRF Routes via OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
2. Select the **Filter** tab, and then click **Route Map**.
3. Select a route map, and then click **Entry**. If entries have been configured, a list appears.

If no filters have been configured, add filters as needed. For more information, refer to "Adding a Route Map Filter Entry" (Page 533).

### 12.9.6.3 Adding a Route Map Filter

To add a route map filter for dynamic OSPF routes, do the following:

1. For Standard OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Route Map**.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.

- b. Select the **Filter** tab, and then click **Route Map**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Route Map Tag	<b>Synopsis:</b> A string between 1 and 1024 characters long Route map tag.

5. Click **OK** to create the new filter.
6. Add one or more entries. For more information, refer to "Adding a Route Map Filter Entry" (Page 533).
7. Commit the change.

#### 12.9.6.4 Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

1. For Standard OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Route Map**.
  - c. Select a route map, and then click **Entry**.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Route Map**.
  - c. Select a route map, and then click **Entry**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 65535 The sequence number of the route-map entry.

5. Click **OK** to create the new entry.
6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> [ deny   permit ] <b>Default:</b> permit Action.



Parameter	Description
Call Route Map	<b>Synopsis:</b> A string between 1 and 1024 characters long Jump to another route-map after match+set.
On Match Goto	<b>Synopsis:</b> An integer between 1 and 65535 Go to this entry on match.
Metric	<b>Synopsis:</b> An integer Metric value.
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 External route type.

7. Configure the match rules for the route map filter. For more information, refer to "Configuring Match Rules" (Page 535).
8. Commit the changes.

#### 12.9.6.5 Deleting a Route Map Filter

To delete a route map filter for dynamic OSPF routes, do the following:

1. For Standard OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Route Map**.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Route Map**.
3. Select the filter to be deleted, and then click **Delete Entry**.
4. Commit the change.

#### 12.9.6.6 Deleting a Route Map Filter Entry

To delete an entry for a route map filter, do the following:

1. For Standard OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Route Map**.
  - c. Select a route map, and then click **Entry**.
2. For VRF Routes via OSPF, navigate to:

- a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Route Map**.
  - c. Select a route map, and then click **Entry**.
3. Select the entry to be deleted, and then click **Delete Entry**.
  4. Commit the change.

### 12.9.6.7 Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. For Standard OSPF routes, navigate to:
  - a. The **Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Click **Route Map**.
  - c. Select a route map, and then click **Entry**.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Filter** tab, and then click **Route Map**.
  - c. Select a route map, and then click **Entry**.
3. Configure the following parameters as required:

Parameter	Description
Match Address of Route	<b>Synopsis:</b> A string between 1 and 1024 characters long The prefix list name.
Match Nexthop of Route	<b>Synopsis:</b> A string between 1 and 1024 characters long The prefix list name.
Match Interface	<b>Synopsis:</b> A string between 1 and 32 characters long The interface name.

4. Commit the changes.

## 12.9.7 Managing Incoming Route Filters

Incoming route advertisements can be filtered by assigning one or route map filters. This can be useful for excluding specific OSPF routes from the routing table.

---

**Note**

For more information about route map filters, refer to "Managing Route Maps" (Page 531).

---

### 12.9.7.1 Viewing List of Incoming Route Filters

To view a list of route filters configured for Standard incoming advertised routes, navigate to the **Incoming Route Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.

To view a list of route filters configured for incoming advertised VRF Routes via OSPF, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Dynamic Routing » OSPF**, select a VRF, and then click **Incoming Route Filter**.

If route filters have been configured, a list appears.

If no route filters have been configured, add filters as needed. For more information, refer to "Adding an Incoming Route Filter" (Page 536).

### 12.9.7.2 Adding an Incoming Route Filter

To add a route filter for incoming advertised routes, do the following:

1. Make sure a route map has been configured. For more information, refer to "Managing Route Maps" (Page 531).
2. For Standard OSPF routes, navigate to:
  - The **Incoming Route Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
3. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Incoming Route Filter** tab, and then click **Route Map**.
4. Select the **Enabled** check box for the route map to be added.
5. Commit the changes.

### 12.9.7.3 Deleting an Incoming Route Filter

To delete a route filter configured for incoming advertised routes, do the following:

1. For Standard OSPF routes, navigate to:
  - The **Incoming Route Filter** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. For VRF Routes via OSPF, navigate to:

- a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
- b. Select the **Incoming Route Filter** tab, and then click **Route Map**.
3. Deselect the **Enabled** check box for the route map to be deleted.
4. Commit the changes.

## 12.9.8 Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the OSPF areas, can also be advertised.

### 12.9.8.1 Viewing a List of Redistribution Metrics

To view a list of redistribution metrics configured for Standard OSPF routes, navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.

To view a list of redistribution metrics configured for VRF Routes via OSPF, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF - VRF**, select a VRF, and then click **Redistribute**.

If metrics have been configured, a list appears.

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 537).

### 12.9.8.2 Adding a Redistribution Metric

To add a redistribution metric for dynamic OSPF routes, do the following:

1. For Standard OSPF routes, navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Redistribute** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Route From	<b>Synopsis:</b> [ kernel   static   connected   rip   bgp ] Redistributes the route type.

5. Click **OK** to add the metric.
6. Configure the following parameter(s) as required:

Parameter	Description
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 <b>Default:</b> 2 The OSPF exterior metric type for redistributed routes.
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric for redistributed routes.
Route Map	<b>Synopsis:</b> A string between 1 and 1024 characters long The route map name.

7. Commit the changes.

### 12.9.8.3 Deleting a Redistribution Metric

To delete a redistribution metric for dynamic OSPF routes, do the following:

1. For Standard OSPF routes, navigate to the **Redistribute** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Redistribute** tab.
3. Select the metric to be deleted, and then click **Delete Entry**.
4. Commit the changes.

## 12.9.9 Managing Routing Interfaces

This section describes how to manage interfaces for OSPF routes.

### 12.9.9.1 Viewing a List of Routing Interfaces

To view a list of routing interfaces for standard OSPF routes, navigate to the **Interface** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.

To view a list of routing interfaces configured for VRF Routes via OSPF, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF - VRF**, select a VRF, and then click **Interface**.

If interfaces have been configured, a list appears.

### 12.9.9.2 Configuring a Routing Interface

To configure a routing interface for an OSPF network, do the following:

1. For Standard OSPF routes, navigate to:
  - a. The **Interface** tab under *Layer 3 » Routing » Dynamic Routing » OSPF*.
  - b. Select an interface.
2. For VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under *Layer 3 » Routing » VRF » OSPF-VRF*, and then select a VRF.
  - b. Select the **Interface** tab, and then select an interface.
3. Under **Dead Interval**, configure the following parameter(s) as required:

---

#### Note

For reliable operation, it is recommended that the **Dead Interval** value be at least four times the number of Hellos per second.

---

#### Note

Lower values of **Dead Interval** and **Number of Hellos Per Second** will help speed up the change in network routes when the topology of the network changes. It will also increase the load on the router and the links, due to higher traffic caused by the increase in messages.

Lower values will also put limits on the number of routes that can be distributed within an OSPF network area, as will running over slower links.

---

 **NOTICE**

The **Dead Interval** and number of Hellos per second must be identical on every router in an OSPF network area.

Parameter	Description
Dead Interval	<p><b>Synopsis:</b> An integer between 1 and 65535</p> <p><b>Default:</b> 40</p> <p>The time before considering a router dead (in seconds).</p>
Number of Hellos Per Second	<p><b>Synopsis:</b> An integer between 1 and 10</p> <p>The number of times a hello message can be sent within one second.</p>

4. Configure the following parameter(s) as required:

---

#### Note

Link detection is enabled automatically for active network interfaces. It makes sure the appropriate routing daemon is notified when an interface goes down and stops advertising subnets associated with that interface. The routing daemon resumes advertising the subnet when the link is restored. This allows

routing daemons to detect link failures more rapidly, as the router does not have to wait for the **dead interval** to time out. Link detection also causes **redistributed** routes to start and stop being advertised based on the status of their interface links.

---

### Note

The link cost determines which route to use when multiple links can reach a given destination. By default, OSPF assigns the same cost to all links unless it is provided with extra information about the links. Each interface is assumed to be 10 Mbit, unless otherwise specified by the **Auto-Cost Bandwidth** parameter set for the interface. For more information about the **Auto-Cost Bandwidth**, refer to "Configuring Costing for Routable Interfaces" (Page 223).

The default OSPF reference bandwidth for link cost calculations is 100 Mbit. The reference bandwidth divided by the link bandwidth gives the default cost for a link, which by default is 10. If a specific bandwidth is assigned to each link, the costs take this into account.

Link costs can be assigned manually under OSPF to each routable interface. This should be done when the speed of the link should not be used as the method for choosing the best link.

Parameter	Description
Authentication Type	<b>Synopsis:</b> [ message-digest   null ] The authentication type on this interface.
Link Cost	<b>Synopsis:</b> An integer between 1 and 65535 The link cost. If not set, the cost is based on calculation of reference bandwidth divide by interface bandwidth.
Hello Interval	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 10 The time (in seconds) between sending hello packets.
Priority	<b>Synopsis:</b> An integer between 0 and 255 <b>Default:</b> 1 Priority of interface.
Passive Interface	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Whether an interface is active or passive. Passive interfaces do not send LSAs to other routers and are not part of an OSPF area.
Retransmit Interval	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 5 Time (in seconds) between retransmitting lost link state advertisements.

Parameter	Description
Transmit Delay	<p><b>Synopsis:</b> An integer between 1 and 65535</p> <p><b>Default:</b> 1</p> <p>The link state transmit delay (in seconds).</p>

5. Commit the changes.

## 12.9.10 Managing Message Digest Keys

Message digest keys use the MD5 algorithm to authenticate OSPF neighbors and prevent unauthorized routers from joining the OSPF network. By enabling authentication and configuring a shared key on all the routers, only routers which have the same authentication key will be able to send and receive advertisements within the OSPF network.

An ID for each key allows the router to use multiple passwords and prevent replay attacks where OSPF packets are captured, modified and transmitted to a router. To change passwords, simply create a new key and delete the old key.

### NOTICE

The router can only share routing information with neighbors that use the same authentication method and password.

### Note

Authentication adds a small overhead due to the encryption of messages. It is not recommended for completely private networks with controlled access.

### 12.9.10.1 Viewing a List of Message Digest Keys

Users can view a list of message digest keys for standard dynamic OSPF routes and VRF routes via OSPF.

#### Standard Dynamic OSPF Routes

To view a list of message digest keys for Standard dynamic OSPF routes, do the following:

1. Navigate to the **Interface** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Select an interface, and then click **Message Digest Key**. If keys have been configured, a list appears.



**VRF Routes via OSPF**

To view a list of message digest keys for VRF routes via OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
2. Select the **Interface** tab, and then select an interface.
3. Select the **Message Digest Key** tab. If keys have been configured, a list appears.

If no message digest keys have been configured, add keys as needed. For more information, refer to "Adding a Message Digest Key" (Page 542).

**12.9.10.2 Adding a Message Digest Key**

To add a message digest key to an OSPF routing interface, do the following:

1. For message digest keys for Standard dynamic OSPF routes, navigate to:
  - a. The **Interface** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Select an interface, and then click **Message Digest Key**.
2. For message digest keys for VRF Routes via OSPF, navigate to:
  - a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Interface** tab, and then select an interface.
  - c. Select the **Message Digest Key** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Key ID	<b>Synopsis:</b> An integer up to 255 The key ID.

5. Click **OK** to add the key.
6. Commit the changes.

**12.9.10.3 Deleting a Message Digest Key**

To delete a message digest key from an OSPF routing interface, do the following:

1. For message digest keys for Standard dynamic OSPF routes, navigate to:
  - a. The **Interface** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
  - b. Select an interface, and then click **Message Digest Key**.
2. For message digest keys for VRF Routes via OSPF, navigate to:

- a. The **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
  - b. Select the **Interface** tab, and then select an interface.
  - c. Select the **Message Digest Key** tab.
3. Select the key to be deleted, and then click **Delete Entry**.
  4. Commit the change.

## 12.9.11 Managing ABR Route Summarization

An inherent problem with OSPF is the number of Link-State Advertisements (LSAs) generated per area. When a route disappears in an area, the Link-State Database (LSDB) can be flooded with multiple advertisements from other areas describing individual routes. This not only creates large routing tables, it also consumes memory and increases CPU utilization.

This can be avoided by enabling an Area Border Router (ABR) to summarize all type-3 summary LSAs for its area into a single type-3 summary LSA.

This section describes ABR route summarization for OSPF and how to configure it.

### 12.9.11.1 Understanding ABR Route Summarization

ABR route summarization reduces the number of type-3 summary LSAs sent between OSPF areas. When ABR route summarization is enabled, type-3 summary LSAs within a specific subnet range(s) received by the ABR are summarized and forwarded to the next area as a single type-3 summary LSA. This significantly reduces traffic between areas and reduces CPU utilization.

ABR route summarization requires the configuration of one or more area ranges for an ABR. An area range defines a network prefix and area ID. An action type (advertise or not advertise) and cost can also be applied. Type-3 LSAs that fall within the specified range are collected by the ABR.

Choosing to not advertise LSAs within a specific area range helps filter LSAs, and prevents any route happening in one area from propagating from one area into others.

### 12.9.11.2 Viewing a List of Summary Routes

To view a list of summary routes configured on the device, navigate to the **Area Range** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.

If no summary routes have been configured, add routes as needed. For more information, refer to "Adding a Summary Route" (Page 544).

### 12.9.11.3 Adding a Summary Route

To add a summary route, do the following:

1. Navigate to the **Area Range** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Area ID	<b>Synopsis:</b> A string between 7 and 15 characters long The OSPF Area ID (format: A.B.C.D).
Area Range	<b>Synopsis:</b> A string between 9 and 18 characters long The OSPF area range network/prefix.

4. Click **OK** to add the area range.
5. Configure the following parameter(s) as required:

Parameter	Description
Advertisement Action	<b>Synopsis:</b> [ advertise   not-advertise ] <b>Default:</b> advertise The OSPF area range advertisement action types.
Area Range Cost	<b>Synopsis:</b> An integer between 1 and 65535 The cost of the summarized route used by OSPF.

6. Commit the changes.

### 12.9.11.4 Deleting a Summary Route

To delete a summary route, do the following:

1. Navigate to the **Area Range** tab under **Layer 3 » Routing » Dynamic Routing » OSPF**.
2. Select the area range to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.9.11.5 Example: Basic Route Summarization

The following demonstrates how to define a series of summary routes for an ABR in a simple OSPF network. In the following topology:

- R1 resides in area 0.0.0.0, the backbone of the OSPF network
- R2 acts as the ABR for areas 0.0.0.0 and 0.0.0.1

- R3 resides in area 0.0.0.1 and is connected to four stub networks (192.168.\*.0/24)

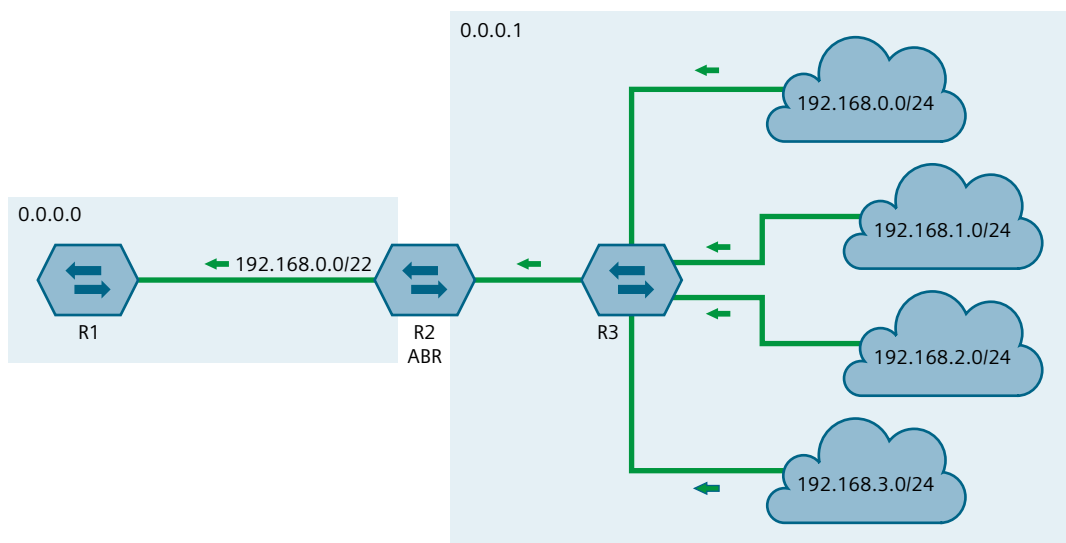


Figure 12.12 Basic ABR Router Summarization

### Configuring a Summary Route to Summarize LSAs

To configure a summary route for R2, do the following:

- Assign IP interfaces to interfaces.

Interface	IP Address/Prefix
fe-1	172.168.1.2/24
fe-2	192.168.10.2/24

- Configure OSPF.
  - Enable OSPF
  - Add the following areas:

Area ID	IP Address/Prefix
0.0.0.0	192.168.10.0/24
0.0.0.1	172.168.1.0/24

- Define fe-1 and fe-2 as routing interfaces.
- Configure a summary route to capture all LSAs advertised by area 0.0.0.1.

Area ID	0.0.0.1
IP Address/Prefix	192.168.0.0/22

- On R1, review the routing table and verify the only LSA received from the ABR is a type-3 summary LSA. For example:

Destination	Gateway	Interface	Type	Weight	Metric
172.168.1.0/24	192.168.10.2	fe-1-2	zebra		20
<b>192.168.0.0/22</b>	<b>192.168.10.2</b>	<b>fe-1-2</b>	<b>zebra</b>		<b>20</b>
192.168.10.0/24		fe-1-2	kernel		

### Configuring a Cost to a Summary Route

The default cost for each summary route is 20. To change the cost for the R2's area range, do the following:

- Navigate to area range 0.0.0.1 for IP address 192.168.0.0/22.
- Change **Cost** to any number between 1 and 65535.
- On R1, review the routing table and verify the cost assigned to the type-3 summary LSA forwarded by the ABR. For example:

Destination	Gateway	Interface	Type	Weight	Metric
172.168.1.0/24	192.168.10.2	fe-1-2	zebra		20
192.168.0.0/22	192.168.10.2	fe-1-2	zebra		<b>30</b>
192.168.10.0/24		fe-1-2	kernel		

### Configuring a Summary Route to Not Advertise Routes

By default, an ABR will advertise all summary LSAs. To configure R2 to summarize but not advertise the LSAs forward by R3, do the following:

- Navigate to area range 0.0.0.1 for IP address 192.168.0.0/22.
- Change **Action Type** from **Advertise** to **Not Advertise**.
- On R1, review the routing table and confirm the ABR is not forwarding any LSAs. For example:

Destination	Gateway	Interface	Type	Weight	Metric
172.168.1.0/24	192.168.10.2	fe-1-2	zebra		20
192.168.10.0/24		fe-1-2	kernel		

## 12.10 Managing MPLS

MPLS (Multi-Protocol Label Switching) operates between Layer 2 and Layer 3 of the OSI (Open Systems Interconnection) model and provides a mechanism to carry traffic for any network layer protocol. MPLS makes forwarding decisions based on labels where the labels are mapped to destination IP networks. MPLS traffic flows are connection-oriented, as they operate on pre-configured LSPs (Label Switch Paths) built based on the dynamic Label Distribution Protocol (LDP), or through static label bindings.

## 12.10.1 Viewing the Status of IP Binding

To view the status of the IP binding on the device, navigate to the **IP Binding** tab under **Layer 3 » MPLS » Status**. If IP binding has been configured, a list appears.

This table provides the following information:

Parameter	Description
Prefix	<b>Synopsis:</b> A string The destination address prefix.
Local Label	<b>Synopsis:</b> A string The incoming (local) label.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.
Remote Label	<b>Synopsis:</b> A string The remote label

## 12.10.2 Viewing the Status of the Forwarding Table

To view the status of the forwarding table on the device, navigate to the **Forwarding Table** tab under **Layer 3 » MPLS » Status**.

The following information is provided:

Parameter	Description
Local Label	<b>Synopsis:</b> A string The incoming (local) label
Outgoing Label	<b>Synopsis:</b> A string The outgoing (remote) label.
Prefix	<b>Synopsis:</b> A string The destination address prefix.
Outgoing Interface	<b>Synopsis:</b> A string The outgoing interface.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.
Up Time	<b>Synopsis:</b> A string The time this entry has been up.

### 12.10.3 Enabling/Disabling MPLS

To enable MPLS routing, do the following:

1. Navigate to **Layer 3 » MPLS**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enable MPLS	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>A boolean flag to indicate that MPLS forwarding of IP packets is enabled.</p>

3. Commit the change.

### 12.10.4 Managing the MPLS Interfaces

This section describes how to manage the MPLS interfaces.

#### 12.10.4.1 Viewing the Status of MPLS Interfaces

To view the status of the MPLS interfaces on the device, navigate to the **Interfaces** tab under **Layer 3 » MPLS » Status**. If MPLS interfaces have been configured, a list appears.

This table provides the following information:

Parameter	Description
Name	<p><b>Synopsis:</b> A string</p> <p>The interface that has been enabled for MPLS.</p>
Status	<p><b>Synopsis:</b> A string</p> <p>The operational status.</p>

If no MPLS interface has been enabled, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to "Enabling/Disabling an MPLS Interface" (Page 549).

#### 12.10.4.2 Viewing a List of MPLS Interfaces

To view a list of MPLS interfaces, navigate to **Layer 3 » MPLS » Interface MPLS**. A list appears. Configured MPLS interfaces are displayed with a check mark in the **Enabled** column.

If no MPLS interfaces have been configured, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to "Enabling/Disabling an MPLS Interface" (Page 549).

### 12.10.4.3 Enabling/Disabling an MPLS Interface

To enable or disable an MPLS interface, do the following:

1. Navigate to **Layer 3 » MPLS » Interface MPLS**, and then select an interface.
2. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>A boolean flag to indicate Multiprotocol Label Switching (MPLS) forwarding of IP packets is enabled on this interface.</p>

3. Commit the change.

## 12.10.5 Managing Static Label Binding

This section describes how to bind (or reserve) labels for IPv4 network prefixes.

### 12.10.5.1 Viewing the Status of Static Label Binding

To view the status of all configured static label binding, navigate to the **Static Binding** tab under **Layer 3 » MPLS » Status**. If static label binding has been configured, a list appears.

This table provides the following information:

Parameter	Description
IP Address	<p><b>Synopsis:</b> A string</p> <p>The destination address prefix.</p>
In Label	<p><b>Synopsis:</b> A string</p> <p>The incoming (local) label.</p>
Out Label	<p><b>Synopsis:</b> A string</p> <p>The outgoing (remote) label.</p>
Next Hop	<p><b>Synopsis:</b> A string</p> <p>The destination next hop router.</p>



If no static label binding has been configured, configure binding as needed. For more information about configuring static-binding, refer to "Adding a Static Label" (Page 550).

### 12.10.5.2 Viewing a List of Static Labels

To view a list of static labels, navigate to the { **Binding IPv4|Binding IPv6** } tab under **Layer 3 » MPLS » Static-MPLS**. If static labels have been configured, a list appears.

If no static labels have been configured, add labels as needed. For more information about adding static labels, refer to "Adding a Static Label" (Page 550).

### 12.10.5.3 Adding a Static Label

To add a static label, do the following:

1. Navigate to the { **Binding IPv4|Binding IPv6** } tab under **Layer 3 » MPLS » Static-MPLS**.
2. Click **Add Entry**.

---

#### Note

A route to the destination address must already be present in the routing table.

---

3. Configure the following parameter(s) as required:

Parameter	Description
Address	<b>Synopsis:</b> A string between 9 and 18 characters long The destination address/prefix.

4. Click **OK** to apply the static label to the destination address.
5. Configure the following parameter(s) as required:

Parameter	Description
In Label	<b>Synopsis:</b> An integer between 16 and 1048575 The incoming label: integer 16 -> 1048575.
Next Hop	<b>Synopsis:</b> A string between 7 and 15 characters long The IP address for the destination next-hop router.
Out Label	<b>Synopsis:</b> [ explicit-null   implicit-null ] or An integer between 16 and 1048575 The outgoing label: <ul style="list-style-type: none"> <li>• <b>implicit null</b> - The label has a value of 3, meaning the penultimate (next-to-last) router performs a pop operation and forwards the remainder of the packet to the egress router. Penultimate Hop Popping (PHP) reduces the number</li> </ul>

Parameter	Description
	<p>of label lookups that need to be performed by the egress router</p> <ul style="list-style-type: none"> <li><b>explicit null</b> - The label has a value of 0, meaning that, in place of a pop operation, the penultimate (next-to-last) router forwards an IPv4 packet with an outgoing MPLS label of 0 to the egress router</li> </ul>

6. Commit the changes.

#### 12.10.5.4 Deleting a Static Label

To delete a static label, do the following:

1. Navigate to the { **Binding IPv4|Binding IPv6** } tab under **Layer 3 » MPLS » Static-MPLS**.
2. Select the static label to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.10.6 Managing Static Cross-Connects

Configure MPLS static cross-connects when the device is the core MPLS router. Cross-connects build Label Switch Paths (LSPs) when neighboring routers do not deploy the Label Distribution Protocol (LDP). The entry for static cross-connects is added to the Label Forwarding Information Base (LFIB). And, as such, label binding is not required in the Label Information Base (LIB).

#### 12.10.6.1 Viewing the Status of Static Cross-Connects

To view the status of all configured static cross-connects, navigate to the **Static Cross Connect** tab under **Layer 3 » MPLS » Status**. If static cross-connects have been configured, a list appears.

This table provides the following information:

Parameter	Description
Local Label	<p><b>Synopsis:</b> A string</p> <p>The incoming (local) label.</p>
Outgoing Label	<p><b>Synopsis:</b> A string</p> <p>The outgoing (remote) label.</p>
Outgoing Interface	<p><b>Synopsis:</b> A string</p> <p>The outgoing interface.</p>

Parameter	Description
Next Hop	<b>Synopsis:</b> A string The destination next hop router.

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to "Adding a Static Cross-Connect" (Page 552).

### 12.10.6.2 Viewing a List of Static Cross-Connects

To view a list of configured static cross-connects, navigate to the **Cross Connect** tab under **Layer 3 » MPLS » Static-MPLS**. If cross-connect labels have been configured, a list appears.

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to "Adding a Static Cross-Connect" (Page 552).

### 12.10.6.3 Adding a Static Cross-Connect

To add a static cross-connect, do the following:

1. Navigate to the **Cross Connect** tab under **Layer 3 » MPLS » Static-MPLS**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Label	<b>Synopsis:</b> An integer between 16 and 1048575 The incoming label.

4. Click **OK** to add the cross-connect label.
5. Configure the following parameter(s) as required:

Parameter	Description
Out Interface	<b>Synopsis:</b> A string The outgoing interface.
Next Hop	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long The destination next-hop router (IPv4 or IPv6 format).
Out Label	<b>Synopsis:</b> [ explicit-null   implicit-null ] or An integer between 16 and 1048575 The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575.

6. Commit the changes.

#### 12.10.6.4 Deleting a Static Cross-Connect

To delete a static cross-connect, do the following:

1. Navigate to the **Cross Connect** tab under **Layer 3 » MPLS » Static-MPLS**.
2. Select the cross-connect label to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 12.10.7 Managing LDP

LDP (Label Distribution Protocol), defined by [RFC 5036 \[http://tools.ietf.org/html/rfc5036\]](http://tools.ietf.org/html/rfc5036), is a protocol that enables an MPLS capable router to exchange MPLS label information. The labels are distributed in both directions so that an LSP (Label Switched Path) can be established and managed within an MPLS network dynamically, as opposed to configuring static routes. LDP takes advantage of already established routing information (using OSPF or IS-IS) to distribute label information amongst the MPLS enabled routers).

LDP works by enabling Label Switch Routers (LSRs) to discover and bind labels to their neighbors within the MPLS network. The LSRs then identify their peers and exchange their label information with one another. Label information is stored in Label Information Base (LIB) and Label Forwarding Information Base (LFIB) tables.

#### 12.10.7.1 Viewing the Status of LDP Binding

To view the status of the LDP binding on the device, navigate to the **Binding** tab under **Layer 3 » MPLS » Status » LDP**. If LDP interfaces have been configured, a list appears.

This table provides the following information:

Parameter	Description
Prefix	<b>Synopsis:</b> A string The LDP transport prefix.
Local Label	<b>Synopsis:</b> A string The incoming (local) label.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.
Remote Label	<b>Synopsis:</b> A string The LDP remote label.

Parameter	Description
In Use	<b>Synopsis:</b> A string The LDP in-use flag.

### 12.10.7.2 Viewing the Status of the LDP Discovery Interfaces

To view the status of the LDP discovery interfaces on the device, navigate to the **Discovery** tab under *Layer 3 » MPLS » Status » LDP*. If LDP interfaces have been configured, a list appears.

This table provides the following information:

Parameter	Description
Interface	<b>Synopsis:</b> A string The LDP discovery interface.
Source IP Address	<b>Synopsis:</b> A string The LDP discovery source IP address.
Peer ID	<b>Synopsis:</b> A string The LDP discovery peer ID.
Peer IP	<b>Synopsis:</b> A string LDP discovery peer IP address
State	<b>Synopsis:</b> A string The LDP discovery interface state.

For more information about configuring LDP discovery interfaces, refer to "Enabling/Disabling an LDP Interface" (Page 557).

### 12.10.7.3 Viewing the Status of the LDP Neighbor Local Node Information

To view the status of the local node(s) for the LDP neighbor on the device, navigate to the **Neighbor** tab under *Layer 3 » MPLS » Status » LDP*, and then click **Local Node Information**.

The following information is provided:

Parameter	Description
LDP ID	<b>Synopsis:</b> A string The LDP ID of the neighbor local node.
Hello Hold Time	<b>Synopsis:</b> A string LDP hello holdtime of the neighbor local node.

Parameter	Description
Keepalive Interval	<b>Synopsis:</b> A string The LDP session holdtime of the neighbor local node.

#### 12.10.7.4 Viewing the Status of the LDP Neighbor Connection Information

To view the status of the LDP neighbor connection on the device, navigate to the **Neighbor** tab under **Layer 3 » MPLS » Status » LDP**, and then click **Connection Information**.

The following information is provided:

Parameter	Description
Peer ID	<b>Synopsis:</b> A string The peer ID of the LDP neighbor connection.
TCP Connection	<b>Synopsis:</b> A string The TCP connection of the LDP neighbor connection.
State	<b>Synopsis:</b> A string The state of the LDP neighbor connection.
Up Time	<b>Synopsis:</b> A string The up time of the LDP neighbor connection.

#### 12.10.7.5 Viewing the Status of the LDP Neighbor Discovery Information

To view the status of the LDP neighbor discovery information on the device, navigate to the **Neighbor** tab under **Layer 3 » MPLS » Status » LDP**, and then click **Discovery Information**.

The following information is provided:

Parameter	Description
Peer ID	<b>Synopsis:</b> A string The peer ID of the LDP neighbor discovery.
Peer IP	<b>Synopsis:</b> A string The peer ID of the LDP neighbor discovery.
Interface	<b>Synopsis:</b> A string The local IP address of the LDP neighbor discovery.
Local IP	<b>Synopsis:</b> A string LDP neighbor discovery state.

Parameter	Description
Peer Holdtime	<b>Synopsis:</b> A string The peer hello holdtime of the LDP neighbor discovery.
Agreed Hello Holdtime	<b>Synopsis:</b> A string The agreed upon hello holdtime (shorter holdtime of local/peer) of the LDP neighbor discovery.
Peer Session Holdtime	<b>Synopsis:</b> A string The peer session holdtime of the LDP neighbor discovery.

### 12.10.7.6 Configuring LDP

To configure the LDP, do the following:

1. Navigate to the **Configurations** tab under **Layer 3 » MPLS » LDP**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enable LDP	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false A boolean flag to indicate that Label Distribution Protocol (LDP) is enabled.
LDP Hold Time	<b>Synopsis:</b> An integer <b>Default:</b> 180 The session holdtime (in seconds), used as the keepalive timeout to maintain the Label Distribution Protocol (LDP) session in the absence of LDP messages from the session peer.

#### Note

MPLS must be enabled and MPLS label bindings must be removed before enabling LDP. Refer to "Enabling/Disabling MPLS" (Page 548) and "Deleting a Static Label" (Page 551) for further information.

3. Commit the changes.

### 12.10.7.7 Configuring Neighbor Discovery

To configure the LDP neighbor discovery, do the following:

1. Navigate to the **Discovery** tab under **Layer 3 » MPLS » LDP**.
2. Configure the following parameter(s) as required:

Parameter	Description
LDP Hello Interval	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 5</p> <p>The time (in seconds) between the sending of consecutive Hello messages.</p>
LDP Hello Hold Time	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 15</p> <p>The time (in seconds) that a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.</p>

3. Commit the changes.

### 12.10.7.8 Viewing a List of LDP Interfaces

To view a list of LDP interfaces, navigate to the **Interfaces** tab under **Layer 3 » MPLS » LDP**. If IP interfaces have been configured, a list appears.

For more information about enabling LDP interfaces, refer to "Enabling/Disabling an LDP Interface" (Page 557).

### 12.10.7.9 Enabling/Disabling an LDP Interface

To enable or disable an LDP interface, do the following:

1. Navigate to the **Interfaces** tab under **Layer 3 » MPLS » LDP**, and then select an interface.
2. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>A boolean flag to indicate a transport interface is LDP-enabled or not. Only LDP-enabled interfaces are used for LDP.</p>
IP Address	<p><b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long</p> <p>The transport IP address (IPv4 format). If not provided, <b>interface</b> is used as the transport address.</p>

3. Commit the changes.



## 12.11 Managing Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) allows multiple routing instances to exist at the same time on a network router without conflicting with one another or the global routing table. This feature is used typically by service providers to route different types of traffic emanating from the same router.

Each routing instance is completely isolated and has its own set of interfaces. Any traffic sent on those interfaces is considered to be part of that VRF only.

An MPLS label can be applied as well to traffic traversing the tunnel to improve security. This is considered full VRF, as compared to VRF-Lite (first introduced by Cisco).

RUGGEDCOM RX5000/MX5000/MX5000RE devices can be configured to act as a CE, PE or P (provider core) router.

### 12.11.1 VRF Concepts

This section describes some of the concepts important to the implementation of Virtual Routing and Forwarding (VRF) in RUGGEDCOM ROX II.

#### 12.11.1.1 VRF and VRF-Lite

Both full VRF and VRF-Lite employ the concept of VRFs to isolate interfaces, provide IP address reuse and manage routing tables. Both also provide a level of security for those interfaces forward to the VRFs. Under full VRF, MPLS is used in conjunction with IP/VPNs to provide a greater level of security than VRF-Lite.

RUGGEDCOM ROX II supports both VRF and VRF-Lite simultaneously. Use of full VRF interfaces and VRF-Lite interfaces can be mixed.

#### 12.11.1.2 Advantages and Disadvantages of Using VRF

The advantages and disadvantages of using VRF include the following:

##### Advantages

- Create multiple isolated network pipes for various data streams
- Provide individualized security for each VRF
- Manage each VRF separately for audit and billing purposes
- Create separate Intranets within one work environment

##### Disadvantages

- Greater memory consumption. Each VRF configured results in BGP route replication and requires new FIBs and IP routing tables
- Extra processing (overhead) and memory consumption due to namespace management

- Create VRFs based on differing services (e.g. Finance, engineering, HR, etc.)
- Reduce the size of routing tables
- Re-use of IP addresses or subnets
- MPLS IP VPNs can replace much more expensive, leased T1/E1 lines, while providing the same level of security

### 12.11.2 Viewing VRF Interface Statistics

To view statistics for interfaces associated with a VRF instance, do the following:


1. Navigate to the **Static Routing** tab under *Layer 3 » Routing » VRF » Status*.
2. Select the **VRF** tab, and then select a VRF instance.
3. Select the **IP** tab, and then select **VRF Routable Interface**.

The following information is provided:

Parameter	Description
Admin State	<b>Synopsis:</b> [ not set   up   down   testing   unknown   dormant   notPresent   lowerLayerDown ]  The port's administrative status.
State	<b>Synopsis:</b> [ not set   up   down   testing   unknown   dormant   notPresent   lowerLayerDown ]  Shows whether the link is up or down.
Point to Point	<b>Synopsis:</b> [ true   false ]  The point-to-point link.

### 12.11.3 Configuring VRF

To configure Virtual Routing and Forwarding (VRF), do the following:

 <b>NOTICE</b>
BGP routing must be enabled before VRF is configured.

#### Full VRF Configuration

1. Make sure BGP is enabled and configure the Autonomous System ID for the Border Gateway Protocol (BGP). For more information, refer to "Configuring BGP" (Page 484).

2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to "Adding a VRF Definition" (Page 562).
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to "Configuring a VRF Interface" (Page 560).
4. Enable OSPF. For more information, refer to "Configuring OSPF" (Page 523).
5. Configure one or more VRF instances for OSPF. For more information, refer to "Configuring OSPF" (Page 523).
6. Add one or more BGP neighbors. For more information, refer to "Adding a Neighbor" (Page 497).
7. Configure one or more IP/VPN tunnels for each interface. For more information, refer to "Adding an IP/VPN Tunnel" (Page 567).
8. Add one or more BGP neighbors to the VPNv4 address family. For more information, refer to "Adding a Neighbor" (Page 568).
9. Verify the network configuration.

### VRF-Lite Configuration

1. Make sure BGP is enabled and configure the Autonomous System ID for the Border Gateway Protocol (BGP). For more information, refer to "Configuring BGP" (Page 484).
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to "Adding a VRF Definition" (Page 562).
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to "Configuring a VRF Interface" (Page 560).
4. Enable OSPF. For more information, refer to "Configuring OSPF" (Page 523).
5. Configure one or more VRF instances for OSPF. For more information, refer to "Configuring OSPF" (Page 523).
6. Configure an IPv4 address family for each VRF instance. For more information, refer to "Adding an IPv4 Address Family" (Page 569).
7. Configure one or more static VRF routes. For more information, refer to "Adding a Static VRF Route" (Page 575).
8. Verify the network configuration.

### 12.11.4 Configuring a VRF Interface

Each VRF definition must be associated with at least one routable interface that has been assigned an IP address.

To configure a routable interface to forward VRF traffic for a specific VRF definition, do the following:

1. Navigate to the **Interface** tab under **Interface » { IP Interfaces }**, and then select an interface.

---

**Note**

The **VRF Forwarding** list is not available for the *dummy* interface.

---

2. Configure the following parameter(s) as required:

Parameter	Description
VRF Forwarding	<b>Synopsis:</b> A string  The VRF to which this interface is to be forwarded. When forwarded, this interface will be made available when that VRF is configured in the IS-IS and OSPF routing protocols. When forwarding is changed/removed for this interface, a validation error will be emitted if the interface is configured for use with that VRF in any of those protocols.

3. Configure an IPv4 or IPv6 address for the interface. For more information, refer to "Adding an IPv4 Address" (Page 225) or "Adding an IPv6 Address" (Page 226).
4. Commit the changes.

## 12.11.5 Managing VRF Definitions

VRF definitions represent individual Customer Edge (CE) routers in the VRF topology. RUGGEDCOM ROX II supports up to eight definitions in total, each composed of a unique VRF name, an optional description and a Route Distinguisher (RD). The Route Distinguisher is an 8 octet field typically made up of an AS number or IP address followed by a colon (:) and the site ID (e.g. 6500:20 or 172.20.120.12:10). When prefixed to the IPv4 address of the associated interface, it uniquely identifies each IP packet, allowing the Provider Edge (PE) to determine which VPN tunnel the packet belongs to.

Each VRF definition can also be associated with one or more route targets.

### 12.11.5.1 Viewing a List of VRF Definitions

To view a list of VRF definitions, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**, and then select **VRF**. If definitions have been configured, a list appears.

If no VRF definitions have been configured, add definitions as needed. For more information, refer to "Adding a VRF Definition" (Page 562).

### 12.11.5.2 Adding a VRF Definition

To add a VRF definition, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**, and then select **VRF**.

---

#### Note

Whenever possible, use meaningful names for each VRF definition, such as *Fin* for financial or *User* for user data.

Consider including numbers as well to further isolate separate streams of data (i.e. *PLCvrf1*, *PLCvrf2*, etc.).

---

2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>The name of the VRF, consisting of 1 to 32 alphanumeric characters. Spaces are not allowed. The 1st character must not be a special character, and following that the only permitted special characters are: -(hyphen), _(underscore), :(colon), and .(period). When created, this VRF name will be added to the list of VRF's available for BGP, IS-IS and OSPF routing protocols. If deleted, a validation error will be emitted if the VRF is configured for use in any of those protocols.</p>

4. Click **OK**.
5. Configure the following parameter(s) as required:

Parameter	Description
Description	<p><b>Synopsis:</b> A string between 0 and 256 characters long</p> <p>A string that can be used to describe the vrf. Maximum length 256 characters, including blanks.</p>
Route Distinguisher	<p><b>Synopsis:</b> A string between 0 and 32 characters long</p> <p>The VRF's route distinguisher: 8-byte value, typical format is (as-number:id   ip-address:id) (e.g. 6500:20). It will be prepended to the IPv4 prefix to create the VPN IPv4 prefix. Note that changing the route distinguisher will affect the route targets: it is recommended that you verify that the configured route targets used in your network will still be correct.</p>

6. Add one or more route targets. For more information, refer to "Adding a Route Target" (Page 563).
7. Configure a routable interface for the VRF instance. For more information, refer to "Configuring a VRF Interface" (Page 560).
8. Commit the changes.

### 12.11.5.3 Deleting a VRF Definition

To delete a VRF definition, do the following:

1. Set **VRF Forwarding** for the associated routable interface to another VRF definition or none at all.
2. Delete the associated VRF instance under OSPF. For more information, refer to "Deleting a VRF Instance" (Page 566).
3. Delete the associated IPv4 address family under BGP. For more information, refer to "Deleting an IPv4 Address Family" (Page 570).
4. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**, and then select **VRF**.
5. Select the definition to be deleted, and then click **Delete Entry**.
6. Commit the changes.

## 12.11.6 Managing Route Targets

Route targets identify those routes to import/export within the Multi-Protocol BGP (MBGP) network. Similar to the normal global routing instance, the route target sets the route import and export parameters for BGP. This parameter enables users to specify which prefixes they wish to import to other neighbors and which ones to export.

### 12.11.6.1 Viewing a List of Route Targets

1. To view a list of route targets for a VRF definition, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**, and then select **VRF**.
2. Select a VRF, and then select { **Export|Import|Both** }. If definitions have been configured, a list appears.

If no VRF definitions have been configured, add definitions as needed. For more information, refer to "Adding a VRF Definition" (Page 562).

### 12.11.6.2 Adding a Route Target

To add a route target, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**, and then select **VRF**.
2. Select a VRF, and then select { **Export|Import|Both** }.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Export Community	<b>Synopsis:</b> A string between 0 and 32 characters long Target VPN extended community to which routing information is exported.

5. Click **OK**.
6. Commit the changes.

### 12.11.6.3 Deleting a Route Target

To delete a route target, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » Static Routing**, and then select **VRF**.
2. Select a VRF, and then select { **Export|Import|Both** }.
3. Select the route target to be deleted, and then click **Delete Entry**.
4. Commit the changes.

## 12.11.7 Managing VRF Instances and OSPF

OSPF can be configured for one or more VRF definitions. This is done by by enabling OSPF for a VRF instance and then configuring the required OSPF parameters.

OSPF can be run on any physical or switched interface, as well as VRF-Lite interfaces (IPv4) and full VRF interfaces (IP/VPN using MPLS).

### 12.11.7.1 Viewing a List of VRF Instances

1. To view a list of VRF instances defined for OSPF, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
2. Select the **VRF Parameters** tab, and then **Configurations**.

If no VRF definitions have been configured, add definitions as needed. For more information, refer to "Adding a VRF Definition" (Page 562).

### 12.11.7.2 Adding a VRF Instance and Configuring OSPF

To add a VRF instance and configure OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**, and then select a VRF.
2. Select the **VRF Parameters** tab, and then select **Distance**.

3. Configure the following parameters:

Parameter	Description
External Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for external routes.
Inter Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for inter-area routes.
Intra Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for intra-area routes.

4. Select **Configurations**, and then configure the following parameters:

Parameter	Description
Enable OSPF	Enables the OSPF dynamic routing protocol.
ABR Type	<b>Synopsis:</b> [ cisco   ibm   shortcut   standard ] <b>Default:</b> cisco The OSPF ABR type.
Auto Cost Reference Bandwidth	<b>Synopsis:</b> An integer between 1 and 4294967 <b>Default:</b> 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
Compatible with RFC1583	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
Default Information Originate	Advertises the default route.
Default Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The default metric of redistribute routes.
Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance.
Enable Opaque-LSA capability	Enables the Opaque-LSA capability (RFC2370).
Passive Default	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true Default passive value for new interface.
Refresh Timer	<b>Synopsis:</b> An integer between 10 and 1800 <b>Default:</b> 10 The refresh timer.



Parameter	Description
Router ID	<b>Synopsis:</b> A string between 7 and 15 characters long The Router ID for OSPF.

5. If **Default Information Originate** is enabled, configure the following parameters:

Parameter	Description
Always Advertise Default Route	<b>Synopsis:</b> [ true   false ] <b>Default:</b> false Always advertise default route even when there is no default route present in routing table.
Default Information Originate Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric value for default route.
Default Information Originate Metric Type	<b>Synopsis:</b> An integer between 1 and 2 <b>Default:</b> 2 The metric type for default route.
Default Information Originate Route Map	<b>Synopsis:</b> A string between 1 and 1024 characters long The route map name.

6. Configure prefix list filters for the VRF instance. For more information, refer to "Adding a Prefix List" (Page 527).
7. Configure areas for the VRF instance. For more information, refer to "Adding an Area" (Page 530).
8. Configure route map filters for the VRF instance. For more information, refer to "Adding a Route Map Filter" (Page 532).
9. Configure redistribution metrics for the VRF instance. For more information, refer to "Adding a Redistribution Metric" (Page 537).
10. Configure interfaces for the VRF instance. For more information, refer to "Configuring a Routing Interface" (Page 539).
11. Commit the changes.

### 12.11.7.3 Deleting a VRF Instance

To delete a VRF instance under OSPF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » OSPF-VRF**.
2. Select the VRF instance to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.11.8 Managing IP/VPN Tunnels

IP/VPN tunnels use the VPNv4 protocol to exchange customer prefixes (i.e. route distributions and route targets) and labels between Provider Edge (PE) routers. IP/VPNs provide isolation of the interfaces connecting each end of the VPN.

---

### Note

VRF maintains a table listing each interface belonging to each IP/VPN tunnel.

---

### 12.11.8.1 Viewing a List of IP/VPN Tunnels

To view a list of IP/VPN tunnels configured for VRF, navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **VPNv4**.

### 12.11.8.2 Adding an IP/VPN Tunnel

To add a new IP/VPN tunnel for VRF, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **VPNv4**.
2. Click **Add Entry**.
3. Configure the following parameter as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The neighbor IP address.

4. Click **OK** to add the address.
5. [Optional] Set the send community by configuring the following parameter:

Parameter	Description
Send Community	<b>Synopsis:</b> [ standard   extended   both   none ] <b>Default:</b> both Identifies the send Community. Default is both.

6. [Optional] Enable the IP/VPN tunnel as a VPNv4 route reflector client by configuring the following parameter:

Parameter	Description
Enable Route Reflector Client	When enabled, the neighbor is a VPNv4 route reflector client.

7. Commit the changes.

**12.11.8.3 Deleting an IP/VPN Tunnels**

To delete an IP/VPN tunnel, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **VPNv4**.
2. Select the tunnel to be deleted, and then click **Delete Entry**.
3. Commit the change.

**12.11.9 Managing VPNv4 Neighbors**

VPNv4 neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for VRF-Lite to operate.

**12.11.9.1 Viewing a List of Neighbors**

To view a list of configured VPNv4 neighbors, navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **VPNv4**. If neighbors have been configured, a list appears.

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 572).

**12.11.9.2 Adding a Neighbor**

To add a new VPNv4 neighbor, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **VPNv4**.
2. Click **Add Entry**.
3. Configure the following parameter as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The neighbor IP address.

4. Click **OK** to add the address.
5. [Optional] Set the send community by configuring the following parameter:

Parameter	Description
Send Community	<b>Synopsis:</b> [ standard   extended   both   none ] <b>Default:</b> both Identifies the send Community. Default is both.

- [Optional] Enable the neighbor as a route reflector client by configuring the following parameter:

Parameter	Description
Enable Route Reflector Client	When enabled, the neighbor is a VPNv4 route reflector client.

- Commit the changes.

### 12.11.9.3 Deleting a Neighbor

To delete a VPNv4 neighbor, do the following:

- Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **VPNv4**.
- Select the neighbor to be deleted, and then click **Delete Entry**.
- Commit the change.

## 12.11.10 Managing IPv4 Address Families

IPv4 address families are configured when deploying VRF-Lite. Address families under BGP specify the neighbors with whom the router will share VRF routing information and what type of routing distribution method is permitted. One or more address families can be configured for each VRF instance.

Route distribution can be limited directly connected routes, static routes, or OSPF learned routes.

### 12.11.10.1 Viewing a List of IPv4 Address Families

To view a list of configured VPNv4 neighbors, navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **IPv4 VRF**. If IPv4 address families have been configured, a list appears.

If no IPv4 address families have been configured, add them as needed. For more information, refer to "Adding an IPv4 Address Family" (Page 569).

### 12.11.10.2 Adding an IPv4 Address Family

To add an IPv4 address family, do the following:

- Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **IPv4 VRF**.
- Click **Add Entry**, and then select the desired VRF.
- Click **OK** to add the IPv4 Address Family.

4. [Optional] Add one or more neighbors. For more information, refer to "Adding a Neighbor" (Page 572).
5. [Optional] Add one or more redistributions. For more information, refer to "Adding a Redistribution" (Page 571).
6. Commit the changes.

### 12.11.10.3 Deleting an IPv4 Address Family

To delete an IPv4 address family, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then click **IPv4 VRF**.
2. Select the IPv4 address family to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.11.11 Managing Redistribution for IPv4 Address Families

Redistribution in general is the advertisement of routes by one protocol that have been learned via another dynamic routing protocol, a static route, or a directly connected router. It is deployed to promote interoperability between networks running different routing protocols. In the case of VRF, the OSPF dynamic routing protocol is supported.

For each VRF instance, one or more redistributions can be defined. A redistribution defines the source of the routing information, a metric and (optional) a pre-defined routing map.

The metric is used for route decision making within the Autonomous System (AS). Care must be taken to define a metric that is understood by the OSPF routing protocol.

### 12.11.11.1 Viewing a List of Redistributions

1. To view a list of redistributions defined for an IPv4 address family, navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
2. Select a VRF, and then select **Redistribute**. If redistributions have been configured, a list appears.

If no redistributions have been configured, add them as needed. For more information, refer to "Adding a Redistribution" (Page 571).

### 12.11.11.2 Adding a Redistribution

To add a redistribution for an IPv4 address family, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
2. Select a VRF, and then select **Redistribute**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Source	<b>Synopsis:</b> [ connected   ospf   static ] Protocol that is source of VRF information. Mandatory field.

5. Click **OK** to add the redistribution.
6. Configure the following parameter(s) as required:

Parameter	Description
Metric	<b>Synopsis:</b> An integer between 0 and 4294967295 The metric for redistributed routes.
Route Map	<b>Synopsis:</b> A string between 1 and 1024 characters long The route map name.

7. Commit the changes.

### 12.11.11.3 Deleting a Redistribution

To delete a redistribution defined for an IPv4 address family, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
2. Select a VRF, and then select **Redistribute**.
3. Select the redistribution to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.11.12 Managing Neighbors for IPv4 Address Families

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for VRF to operate.

**12.11.12.1 Viewing a List of Neighbors**

1. To view a list of neighbors configured for an IPv4 address family, navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
2. Select a VRF, and then select **Neighbor**. If neighbors have been configured, a list appears.

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 572).

**12.11.12.2 Adding a Neighbor**

To add a new neighbor to an IPv4 address family, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
2. Select a VRF, and then select **Neighbor**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long The BGP VRF neighbor IP address.

5. Click **OK** to add the address.
6. Configure the following parameter(s) as required:

Parameter	Description
Send Community	<b>Synopsis:</b> [ standard   extended   both   none ] <b>Default:</b> both Identifies the send Community. Default is both.
Neighbor Autonomous System ID	<b>Synopsis:</b> An integer between 1 and 4294967295 A BGP neighbor.
Maximum Hop Count	<b>Synopsis:</b> An integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
Maximum Prefix	<b>Synopsis:</b> An integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
Next Hop Calculation	Disables the next hop calculation for this neighbor.
Password	<b>Synopsis:</b> A string Password.

Parameter	Description
Source Address for Updates	<b>Synopsis:</b> A string between 7 and 15 characters long Source IP address of routing updates.
Disable Connected Verification	Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
Soft Reconfiguration	Per neighbor soft reconfiguration.
Weight	<b>Synopsis:</b> An integer The default weight for routes from this neighbor.
IN	<b>Synopsis:</b> A string between 1 and 1024 characters long Apply route map to incoming routes.
OUT	<b>Synopsis:</b> A string between 1 and 1024 characters long Apply route map to outbound routes.

7. Configure the prefix list distribution. For more information, refer to "Configuring the Distribution of Prefix Lists" (Page 573).
8. Commit the changes.

### 12.11.12.3 Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in an IPv4 address family, do the following:

1. Make sure the desired prefix list is configured for the BGP network. For more information, refer to "Adding a Prefix List" (Page 492).
2. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
3. Select a VRF, and then select **Neighbor**.
4. Select a neighbor, and then select **Distribute Prefix List**.
5. Select the check box under either **In** or **Out**, depending on the direction of the route (incoming or outbound).
6. Under **Prefix List**, select the desired prefix list.
7. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands" (Page 574).
8. Commit the changes.



#### 12.11.12.4 Tracking Commands

Network commands can be tracked using event trackers configured under **Layer 3 » Tracking**. For more information about event trackers, refer to "Managing Event Trackers" (Page 447).

A network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's RIP peers) when the tracked target is unavailable.

To track a command for an IPv4 address family, do the following:

1. Make sure a prefix list distribution path has been configured. For more information, refer to "Managing the Prefix List Distribution" (Page 477).
2. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
3. Select a VRF, and then select **Neighbor**.
4. Select a neighbor, and then select **Distribute Prefix List**.
5. Under **Track**, select the **Enabled** check box.
6. Configure the following parameter(s) as required:

Parameter	Description
Event	<b>Synopsis:</b> A string up to 64 characters long Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state.
Apply When	<b>Synopsis:</b> [ up   down ] <b>Default:</b> up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

7. Commit the changes.

#### 12.11.12.5 Deleting a Neighbor

To delete a VPNv4 neighbor, do the following:

1. Navigate to the **Address Family** tab under **Layer 3 » Routing » Dynamic Routing » BGP**, and then select **IPv4 VRF**.
2. Select a VRF, and then select **Neighbor**.
3. Select the neighbor to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.11.13 Managing Static VRF Routes

Routing information can be shared between routers using dynamic routing data or they can be manually configured. Static routes are explicit paths between routers that are manually configured. Static routes are commonly used for stable, often smaller networks whose configurations are not prone to change. They can be used to supplement dynamic routes.

### 12.11.13.1 Viewing a List of Static VRF Routes

1. To view a list of static IPv4 routes configured for a VRF instance, navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**. If neighbors have been configured, a list appears.

If no static routes have been configured, add routes as needed. For more information, refer to "Adding a Static VRF Route" (Page 575).

### 12.11.13.2 Adding a Static VRF Route

To add an IPv4 static route for a VRF instance, do the following:

1. Navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**.
3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	<b>Synopsis:</b> A string between 1 and 32 characters long The VRF name.

4. Click **OK** to add the route.
5. Configure the following parameter(s) as required:

Parameter	Description
Subnet (Network/Prefix)	<b>Synopsis:</b> A string between 9 and 18 characters long The subnet (network/mask) of the static route.

6. If the device has a Layer 3 switch installed, configure the following parameter(s) as required:

---

#### Note

Only TCP and UDP traffic flows will be accelerated by the IP/Layer 3 switch fabric. Non-IP packet types, such as ICMP and IGMP, will not be accelerated.

---

Parameter	Description
HW Accelerate	If the static unicast route can be hardware accelerated, this option will be available. For a static unicast route to be accelerated, the ingress and egress interfaces must be switched.

7. If necessary, configure a black hole connection for the static route. For more information, refer to "Configuring a Black Hole Connection for a Static VRF Route" (Page 576).
8. If necessary, add gateways for the static route. For more information, refer to "Adding a Gateway for a Static VRF Route" (Page 577).
9. If necessary, add interfaces for the static route. For more information, refer to "Adding a Gateway for a Static VRF Route" (Page 578).
10. Commit the changes.

### 12.11.13.3 Configuring a Black Hole Connection for a Static VRF Route

To configure a black hole connection for a static VRF route, do the following:

1. Navigate to the **VRF Static Route** tab under *Layer 3 » Routing » VRF » Static Routing*.
2. Select a VRF, and then select **IPv4 Route**.
3. Configure the following parameter(s) as required:

Parameter	Description
Distance	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1 The distance for this static route's blackhole. Default is 1.

4. Commit the change.

### 12.11.13.4 Deleting a Static VRF Route

To delete an IPv4 static route configured for a VRF instance, do the following:

1. Navigate to the **VRF Static Route** tab under *Layer 3 » Routing » VRF » Static Routing*.
2. Select a VRF, and then select **IPv4 Route**.
3. Select the route to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.11.14 Managing Gateways for Static VRF Routes

This section describes how to configure and manage gateways for static VRF routes.

### 12.11.14.1 Viewing a List of Gateways for Static VRF Routes

1. To view a list of gateway addresses assigned to an IPv4 static route, navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**.
3. Select a route, and then select **Via**. If gateway addresses have been configured, a list appears.

If no gateway addresses have been configured, add addresses as needed. For more information, refer to "Adding a Gateway for a Static VRF Route" (Page 577).

### 12.11.14.2 Adding a Gateway for a Static VRF Route

To add a gateway address for a static VRF route, do the following:

1. Navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**.
3. Select a route, and then select **Via**.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	<b>Synopsis:</b> A string between 7 and 15 characters long The gateway for the static route.

6. Click **OK** to add the gateway address.
7. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

8. Commit the changes.

**12.11.14.3 Deleting a Gateway for a Static VRF Route**

To delete a gateway address assigned to a static VRF route, do the following:

1. Navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**.
3. Select a route, and then select **Via**.
4. Select the gateway address to be deleted, and then click **Delete Entry**.
5. Commit the change.

**12.11.15 Managing Interfaces for Static VRF Routes**

This section describes how to manage interfaces used for static VRF routes.

**12.11.15.1 Viewing a List of Interfaces for Static VRF Routes**

1. To view a list of interfaces assigned to a static VRF route, navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**.
3. Select a route, and then select **Dev**. If interfaces have been configured, a list appears.

If no gateway addresses have been configured, add addresses as needed. For more information, refer to "Adding a Gateway for a Static VRF Route" (Page 578).

**12.11.15.2 Adding a Gateway for a Static VRF Route**

To add an interface for an static VRF route, do the following:

1. Navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
2. Select a VRF, and then select **IPv4 Route**.
3. Select a route, and then select **Dev**.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
Interface	<b>Synopsis:</b> A string The interface for the static route.

6. Click **OK** to add the interface.
7. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

- Commit the changes.

### 12.11.15.3 Deleting a Gateway for a Static VRF Route

To delete an interface assigned to a static VRF route, do the following:

- Navigate to the **VRF Static Route** tab under **Layer 3 » Routing » VRF » Static Routing**.
- Select a VRF, and then select **IPv4 Route**.
- Select a route, and then select **Dev**.
- Select the interface to be deleted, and then click **Delete Entry**.
- Commit the change.

### 12.11.16 Example: Configuring OSPF on a VRF-Lite Instance

This configuration example shows a Customer Edge device *R2* which is not VRF aware, establishing a neighbor relationship with Provider Edge device *R3*, which is VRF aware.

#### NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

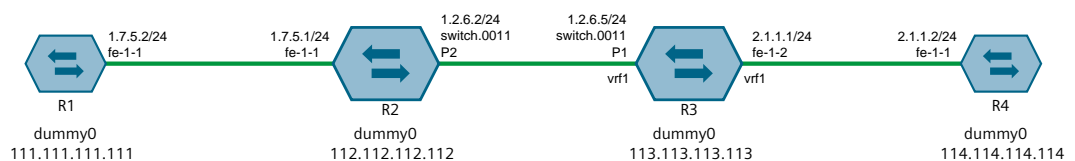


Figure 12.13 Topology – VRF-Lite Instance Configured with OSPF

#### Step 1: Configure OSPF on Router R2

In this scenario R2 is a RUGGEDCOM ROX II device acting as a non-VRF aware Customer Edge (CE) router.

- Enable OSPF. For more information, refer to "Configuring OSPF" (Page 523).

2. Set the router ID for OSPF to `112.112.112.112`. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).
3. Add area ID `0.0.0.0 0.0.0.0/0` for the dynamic OSPF route. For more information, refer to "Adding an Area" (Page 530).
4. Add interface `fe-1-1` for the OSPF network. For more information, refer to "Configuring a Routing Interface" (Page 539).
5. Set the default passive value of the interface to `false`. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).
6. Add interface `switch.0011`. For more information, refer to "Configuring a Routing Interface" (Page 539).
7. Assign IP address `1.2.6.2/24` to the `switch.0011` interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
8. Set the default passive value of the interface to `false`. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

## Step 2: Configure OSPF on Router R3

In this scenario R3 is a RUGGEDCOM ROX II device acting as a VRF aware Provider Edge (PE) router.

1. Enable OSPF. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).
2. Configure a VRF definition for `vrf1` with a route distinguisher of `10`. For more information, refer to "Adding a VRF Definition" (Page 562).
3. Define a route target for VRF1 of type **both** with the export community set to `100:1`. For more information, refer to "Adding a Route Target" (Page 563).
4. Set the router ID for OSPF to `113.113.113.113`. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).
5. Add area ID `0.0.0.0 0.0.0.0/0` for the dynamic OSPF route. For more information, refer to "Adding an Area" (Page 530).
6. Add interface `fe-1-2` for the OSPF network. For more information, refer to "Configuring a Routing Interface" (Page 539).
7. Set the default passive value of the interface to `false`. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).
8. Add interface `switch.0011`. For more information, refer to "Configuring a Routing Interface" (Page 539).
9. Assign IP address `1.2.6.5/24` to the `switch.0011` interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
10. Set the default passive value of the interface to `false`. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 564).

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

### Step 3: Verify the configuration

- Verify R2 and R3 have established an OSPF neighbor relationship.
  - For R2, navigate to **routing » status » ospf » neighbor**.

Values similar to the following are provided:

<b>ID</b>	113.113.113.113
<b>Address</b>	1.2.6.5
<b>Interface</b>	switch.0011:1.2.6.2
<b>Priority</b>	1
<b>State</b>	Full/Back
<b>Dead Time</b>	38.320s

- For R3, navigate to **routing » status » ospf » vrf1 » neighbor**.

Values similar to the following are provided:

Neighbor ID	112.112.112.112
Pri	1
State	Full/DR
Dead Time	36.247s
Address	1.2.6.2
Interface	switch.0011:1.2.6.5
RXmtL	0
RqstL	0
DBsmL	0

- VRF ping 1.7.5.1 from R3. If the configuration is successful R2 will respond. For more information, refer to "Pinging VRF Endpoints" (Page 41).
- Ping 2.1.1.1 from R2. If the configuration is successful R3 will respond.

### Final Configuration Example

#### R2 Configuration

```

routing ospf
  enabled
  router-id      112.112.112.112
  area 0.0.0.0 0.0.0.0/0
  !

interface fe-1-1
  no passive

interface switch.0011
  no passive
  
```

#### R3 Configuration

```

routing ospf
  enabled
  vrf vrf1
    enabled
  router-id      113.113.113.113
  area 0.0.0.0 0.0.0.0/0
  interface fe-1-2
    no passive
  interface switch.0011
    no passive
  
```



### 12.11.17 Example: Configuring BGP on a VRF-Lite Instance

This configuration example shows a Customer Edge device *R2* which is not VRF aware, establishing a neighbor relationship with Provider Edge device *R3*, which is VRF aware.

#### ⚠ NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

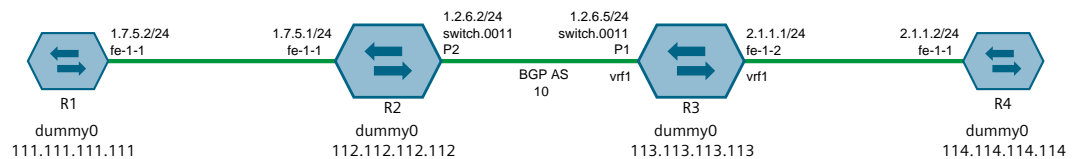


Figure 12.14 Topology – VRF-Lite Instance Configured with BGP

#### Step 1: Configure Router R2

In this scenario R2 is a RUGGEDCOM ROX II device acting as a non-VRF aware Customer Edge (CE) router.

1. Add VLAN 11. For more information, refer to "Adding a Static VLAN" (Page 321).
2. Assign PVID 11 to port P2. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276).
3. Assign IP address 1.2.6.2/24 to the switch.0011 interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
4. Assign IP address 112.112.112.112 to the *dummy0* interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
5. Enable BGP. For more information, refer to "Configuring BGP" (Page 484).
6. Assign Autonomous System ID (AS-ID) 10. For more information, refer to "Configuring BGP" (Page 484).
7. Add neighbor 1.2.6.5 and remote AS 10. For more information, refer to "Adding a Neighbor" (Page 497).
8. Define a redistribution metric for IPv4 family of type **connected**. For more information, refer to "Adding a Redistribution" (Page 571).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

#### Step 2: Configure Router R3

In this scenario R3 is a RUGGEDCOM ROX II device acting as a VRF aware Provider Edge (PE) router.

1. Assign IP address `113.113.113.113` to the `dummy0` interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
2. Configure a VRF definition for `VRF1` with a route distinguisher of `200:1`. For more information, refer to "Adding a VRF Definition" (Page 562).
3. Define a route target for `VRF1` of type **both** with the export community set to `100:1`. For more information, refer to "Adding a Route Target" (Page 563).
4. Make sure interfaces are configured with the IP addresses `1.2.6.5/24` and `2.1.1.1/24`.
5. Assign the interfaces in step 4 (Page 583) to forward traffic to `VRF1`. For more information, refer to "Configuring a VRF Interface" (Page 560).
6. Enable BGP. For more information, refer to "Configuring BGP" (Page 484).
7. Assign Autonomous System ID (AS-ID) `10`. For more information, refer to "Configuring BGP" (Page 484).
8. Add neighbor `1.2.6.2` and remote AS `10`. For more information, refer to "Adding a Neighbor" (Page 568).
9. Define a redistribution metric for IPv4 family of type **connected**. For more information, refer to "Adding a Redistribution" (Page 571).
10. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

### Step 3: Verify the configuration

1. Verify R2 and R3 have established an OSPF neighbor relationship.
  - For R2, navigate to **routing » status » bgp » neighbor**.

Values similar to the following are provided:

<b>ID</b>	1.2.6.5
<b>Version</b>	4
<b>Local AS</b>	10
<b>MSGRCVD</b>	6
<b>MSGSENT</b>	13
<b>Uptime</b>	00:04:25
<b>State</b>	Established
<b>Prefix Received</b>	1

- For R3, navigate to **ip » bgp » vrf1 » neighbors**.

Values similar to the following are provided:

<b>BGP Neighbor</b>	1.2.6.2
<b>Remote AS</b>	10
<b>Local AS</b>	10
<b>BGP Version</b>	4
<b>Remote Router ID</b>	192.168.1.112

<b>BGP State</b>	Established
<b>Up For</b>	00:24:44
<b>Last Read</b>	05:52:03
<b>Hold Time</b>	180
<b>Keepalive Interval</b>	60 seconds

2. VRF ping 1.7.5.1 from R3. If the configuration is successful R2 will respond. For more information, refer to "Pinging VRF Endpoints" (Page 41).
3. Ping 2.1.1.1 from R2. If the configuration is successful R3 will respond.

## Final Configuration R2

### Interface Configuration

```
# interface switch lm1 2 vlan pvid 11
#ip switch.0011 ipv4 address 1.2.6.2/24
#ip dummy0 ipv4 address 112.112.112.112/24
```

### BGP Configuration

```
routing bgp
enabled
as-id 10
neighbor 1.2.6.5
remote-as 10
!
redistribute connected
no metric
!
!
```

## Final Configuration R3

### Interface Configuration

```
#ip dummy0 ipv4 address 113.113.113.113/24
```

### VRF Definitions

```
global
vrf
  definition vrf1
  rd 200:1
  route-target both 100:1
```

### BGP Configuration

```
routing bgp
enabled
as-id 10
address-family ipv4
vrf vrf1
redistribute connected
neighbor 1.2.6.2
remote-as 10
```

### VRF Interface Configuration

```
ip switch.0011
 vrf-forwarding vrf1
 ipv4
  address 1.2.6.5/24
ip fe-1-2
 vrf-forwarding vrf1
 ipv4
  address 2.1.1.1/24
```

## 12.12 Managing Static Routing

Static routes can be manually added to the routing table when there are no notifications sent by other routers regarding network topology changes.

### 12.12.1 Viewing a List of Static Routes

To view a list of static routes configured on the device, navigate to **Layer 3 » Routing » Static Routing » {protocol}**, where {protocol} is either *IPv4* or *IPv6*. If routes have been configured, a list appears.

If no static routes have been configured, add routes as needed. For more information, refer to "Adding an IPv4 Static Route" (Page 585) or "Adding an IPv6 Static Route" (Page 586).

### 12.12.2 Adding an IPv4 Static Route

To add an IPv4 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv4**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

#### NOTICE

If the route is to be configured as a black hole route, make sure the subnet matches that of another static route. The black hole route will then act as a backup should the other static route go down.

Parameter	Description
Subnet (network/prefix)	<b>Synopsis:</b> A string between 9 and 18 characters long The subnet (network/mask) of the static route.

4. Click **OK** to add the route.
5. If the device has a Layer 3 switch installed, configure the following parameter(s) as required:

**Note**

Only TCP and UDP traffic flows will be accelerated by the IP/Layer 3 switch fabric. Non-IP packet types, such as ICMP and IGMP, will not be accelerated.

Parameter	Description
HW Accelerate	If the static unicast route can be hardware accelerated, this option will be available. For a static unicast route to be accelerated, the ingress and egress interfaces must be switched.

6. [Optional] Configure the route as a black hole route. For more information, refer to "Configuring a Black Hole Connection for an IPv4 Static Route" (Page 587).
7. [Optional] If the static route is not a black hole route, configure either the interface that connects to the next-hop router (if there is a direct connection) or the IP address (gateway) of the next-hop router. Only one can be configured per static route. For more information, refer to either "Adding a Gateway for an IPv4 Static Route" (Page 588) or "Adding an Interface for an IPv4 Static Route" (Page 590).
8. Commit the changes.

### 12.12.3 Adding an IPv6 Static Route

To add an IPv6 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv6**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Subnet (network/prefix)	<b>Synopsis:</b> A string between 4 and 43 characters long The subnet (network/mask) of the static route.

4. Click **OK** to add the route.
5. Configure the next hop IP address (gateway) or interface. Only one can be configured per static route. For more information, refer to "Configuring Gateways for IPv6 Static Routes" (Page 588) or "Configuring Interfaces for IPv6 Static Routes" (Page 589).
6. Commit the changes.

### 12.12.4 Deleting a Static Route

To delete a static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » {protocol}**, where {protocol} is either *IPv4* or *IPv6*.
2. Select the route to be deleted, and then click **Delete Entry**.
3. Commit the changes.

### 12.12.5 Configuring a Black Hole Connection for an IPv4 Static Route

When a black hole connection is configured for an IPv4 static route, the static route is considered a *black hole route*. Black hole routes cannot receive packets or send Internet Control Message Protocol (ICMP) messages back to the sender to confirm receipt. They are a void in which to silently discard packets when needed.


A typical scenario where a black hole route is needed is as follows:

- A continuous ping request is sent via a tunnel on the same static route, using the same session
- The session is held for a certain period of time (e.g. one minute) before it is closed
- If the ping request is reissued before the current session times out, a new session cannot be initiated and the static route is considered to be down

With a black hole route configured for the same subnet (network/mask), but with a higher administrative distance than the other static route, the device can redirect and discard the ping request without notifying the originator.

To configure a black hole connection for an IPV4 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv4**, and then select a subnet.
2. Select the check box under **Blackhole**.
3. Configure the following parameter(s) as required:

 <b>NOTICE</b>	
The administrative distance must be higher than the distance set for the other static route's gateway or interface. The route with the lower distance will be chosen first.	
Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1  The distance for this static route's blackhole. Default is 1.

4. Commit the changes.

## 12.12.6 Managing Gateways for Static Routes

If the device is not directly connected to the next-hop router, configure a static route to forward traffic to the next-hop router's IP address. This is referred to as a *gateway*. In the case of IPv6 static routes, only one gateway can be selected per route.

### 12.12.6.1 Configuring Gateways for IPv6 Static Routes

To configure a gateway address for an IPv6 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv6**, and then select a subnet.
2. Select the check box under **Via**.
3. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	<b>Synopsis:</b> A string between 6 and 40 characters long The gateway for the static route.
Gateway Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

4. Commit the changes.

### 12.12.6.2 Viewing a List of Gateways for IPv4 Static Routes

1. To view a list of gateway addresses assigned to an IPv4 static route, navigate to **Layer 3 » Routing » Static Routing » IPv4**.
2. Select a subnet, and then select **Via**. If gateway addresses have been configured, a list appears.

If no gateway addresses have been configured, add addresses as needed. For more information, refer to "Adding a Gateway for an IPv4 Static Route" (Page 588).

### 12.12.6.3 Adding a Gateway for an IPv4 Static Route

To add a gateway address for an IPv4 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv4**.
2. Select a subnet, and then select **Via**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	<b>Synopsis:</b> A string between 7 and 15 characters long The gateway for the static route.

- Click **OK** to add the gateway address.
- Configure the following parameter(s) as required:

Parameter	Description
Distance	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

- Commit the changes.

#### 12.12.6.4 Deleting a Gateway for an IPv4 Static Route

To delete a gateway for an IPv4 static route, do the following:

- Navigate to **Layer 3 » Routing » Static Routing » IPv4**.
- Select a subnet, and then select **Via**.
- Select the gateway address to be deleted, and then click **Delete Entry**.
- Commit the change.

### 12.12.7 Managing Interfaces for Static Routes

Static routes can be configured to forward packets to an exit interface. Assuming the device is directly connected to a neighboring router, the device will send Address Resolution Protocol (ARP) requests to determine the next hop IP address.

In the case of IPv6 static routes, only one interface can be selected per route.

#### 12.12.7.1 Configuring Interfaces for IPv6 Static Routes

To configure an interface for an IPv6 static route, do the following:

- Navigate to **Layer 3 » Routing » Static Routing » IPv6**, and then select a subnet.
- Select the check box under **Dev**.
- Configure the following parameter(s) as required:

Parameter	Description
Interface Name	<b>Synopsis:</b> A string The interface for the static route.



Parameter	Description
Interface Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

4. Commit the changes.

### 12.12.7.2 Viewing a List of Interfaces for IPv4 Static Routes

1. To view a list of interfaces assigned to an IPv4 static route, navigate to **Layer 3 » Routing » Static Routing » IPv4**.
2. Select a subnet, and then select **Dev**. If interfaces have been configured, a list appears.

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an Interface for an IPv4 Static Route" (Page 590).

### 12.12.7.3 Adding an Interface for an IPv4 Static Route

To add an interface for an IPv4 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv4**.
2. Select a subnet, and then select **Dev**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Interface	<b>Synopsis:</b> A string The interface for the static route.

5. Click **OK** to add the interface.
6. Configure the following parameter(s) as required:

Parameter	Description
Distance	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

7. Commit the changes.

### 12.12.7.4 Deleting an Interface for an IPv4 Static Route

To delete an interface for an IPv4 static route, do the following:

1. Navigate to **Layer 3 » Routing » Static Routing » IPv4**.

2. Select a subnet, and then select **Dev**.
3. Select the interface to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.13 Managing Static Multicast Routing

Static multicast routing allows network designers to control the flow of multicast traffic by manually adding static routes to the routing table.

### 12.13.1 Enabling/Disabling Static Multicast Routing

To enable or disable static multicast routing, do the following:

1. Navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enabled	Enables static multicast routing service

3. Commit the change.

### 12.13.2 Managing Static Multicast Groups

Define a static multicast group for each multicast route. Multiple routes can be configured, as long as the source and multicast IP addresses are unique to the route.

#### NOTICE

The source IP address for static routes is always a unicast address (e.g. 192.168.0.10), while the destination IP address is always a multicast address (e.g. 225.2.100.1).

#### 12.13.2.1 Viewing a List of Static Multicast Groups

To view a list of static multicast groups, navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**. If static multicast groups have been configured, a list appears under **Mcast Group**.

If no static multicast groups have been configured, add groups as needed. For more information about adding static multicast groups, refer to "Adding a Static Multicast Group" (Page 592).

### 12.13.2.2 Adding a Static Multicast Group

To add a static multicast group, do the following:

1. Navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**.
2. Under **Mcast Group**, click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string up to 32 characters long Describes the multicast group, spaces are not allowed.

4. Click **OK** to add the group.
5. Configure the following parameter(s) as required:

#### Note

Only TCP and UDP traffic flows will be accelerated by the IP/Layer 3 switch fabric. Non-IP packet types, such as ICMP and IGMP, will not be accelerated.

Parameter	Description
Source IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The expected source IP address of the multicast packet, in the format xxx.xxx.xxx.xxx. This address is uniquely paired with the multicast address. You cannot use this IP address to create another multicast routing entry with a different Multicast-IP address.
Multicast IP	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 7 and 39 characters long  The multicast IP address to be forwarded, in the format xxx.xxx.xxx.xxx  The address must be in the range of 224.0.0.0 to 239.255.255.255. This address is uniquely paired with the source IP address. You cannot use this IP address to create another multicast routing entry with a different Source-IP address.
In Interface	<b>Synopsis:</b> A string  The interface upon which the multicast packet arrives.
HW Accelerate	If the multicast route can be hardware accelerated, the option will be available. For a multicast route to be accelerated, the ingress and egress interfaces must be switched.

6. Configure out-interfaces. For more information, refer to "Adding an Out-Interface" (Page 593).
7. Commit the changes.

### 12.13.2.3 Deleting a Static Multicast Group

To delete a static multicast group, do the following:

1. Navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**.
2. Under **Mcast Group**, select the multicast group to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.13.3 Managing Out-Interfaces

An out-interface is the interface to which multicast packets are forwarded. Multiple out-interfaces can be defined for each static multicast group.

### 12.13.3.1 Viewing a List of Out-Interfaces

1. To view a list of out-interfaces, navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**.
2. Select a multicast group, and then select **Out Interface**. If out-interfaces have been configured, a list appears.

If no out-interfaces have been configured, add groups as needed. For more information about adding out-interfaces, refer to "Adding an Out-Interface" (Page 593).

### 12.13.3.2 Adding an Out-Interface

To add an out-interface, do the following:

1. Navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**.
2. Select a multicast group, and then select **Out Interface**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	<b>Synopsis:</b> A string

5. Click **OK**.
6. Commit the changes.

### 12.13.3.3 Deleting an Out-Interface

To delete an out-interface, do the following:

1. Navigate to the **Static** tab under **Layer 3 » Routing » Multicast Routing**.
2. Select a multicast group, and then select **Out Interface**.
3. Select the out-interface to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 12.14 Managing Dynamic Multicast Routing

This section describes concepts and configuration related to dynamic multicast routing using PIM-SM and PIM-SSM.

### 12.14.1 Understanding Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a collection of multicast routing protocols that provide one-to-many and many-to-many distribution of multicast packets over an IP network. PIM is protocol-independent in that it does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols. PIM can accommodate any unicast routing protocol in use on the network.

RUGGEDCOM ROX II supports two types of PIM: PIM - Sparse Mode (PIM-SM) and PIM - Source Specific Multicast (PIM-SSM).

#### 12.14.1.1 PIM-SM Concepts

Protocol Independent Multicast - Sparse Mode (PIM-SM) is a dynamic multicast routing protocol that can dynamically prune and maintain multicast routes. PIM relies on the router's unicast routing table for its capabilities and does not rely on any specific method for learning routes, therefore it is "Protocol Independent".

#### PIM-SM Terms

The following terms are used in PIM-SM:

- **Rendezvous Point**  
The rendezvous point (RP) is a destination in the network (one of the routers), where all multicast traffic is first registered. Whenever a PIM router receives a multicast stream, the source and the multicast address are registered with the rendezvous point.
- **Boot Strap Router**  
A PIM-SM boot strap router (BSR) is a router that announces the location of the rendezvous point to all other PIM routers on the network.

- **Designated Router**  
A designated router (DR) is a router directly attached to a multicast host or device.
- **Shared Tree**  
The shared tree, also known as the RP-Tree, is a traffic distribution tree which begins from the rendezvous point. The rendezvous point will forward the particular multicast group traffic through this tree whenever there are subscribers for a given multicast flow. Note that the shared tree is on a per-group basis. This means that the shared tree for one group could be different than the shared tree for another on the same network depending on the distribution of the multicast traffic subscribers.
- **Shortest Path Tree**  
The shortest path tree (SPT) is a traffic distribution tree which begins at the source of the multicast traffic or rather the router nearest to the source. The shortest path tree is activated whenever there is a shorter path between the source and the receiver. The shortest path tree can only be triggered by the rendezvous point or the router connected directly to the subscriber.
- **mroute**  
The routing paths between the producer IP host and the rendezvous point.
- **groute**  
The routing paths between the multicast traffic subscriber and the rendezvous point.

## PIM-SM Operation

When a PIM router receives a subscription from a host, e.g. Host A, for particular multicast traffic, the directly attached designated router (DR) sends an IGMP **Join** message for this multicast group towards the rendezvous point (RP). The message is sent hop-by-hop and thus any routers encountering the message would register the group and send the message onwards towards the RP. This would create the shared tree (RP-tree). The tree will not be complete, however, until any sources appear.

When a host or device sends multicast traffic destined to the multicast group subscribed by A, the directly attached designated router takes the traffic, encapsulates it with PIM Register headers and unicasts them to the RP. When the RP receives this traffic, it decapsulates the packets and sends the data towards the subscriber through the RP tree. The routers that receive these packets simply pass them on over the RP-Tree until it reaches the subscriber. Note that there may be other subscribers in the network and the path to those subscribers from the RP is also part of the RP Tree.

After the shared tree has been established, the traffic flows from the source to the RP to the receiver. There are two inefficiencies in this process. One, the traffic is encapsulated at the source and decapsulated at the RP, which may be a performance penalty for a high level of traffic. Two, the traffic may be taking a longer path than necessary to reach its receivers.

After the shared tree has been established, the RP may choose to send a **Join** message to the source declaring that it only wants traffic for a group (e.g. group

G) from the source (e.g. source S). The DR for the source then starts sending the traffic in multicast form (instead of unicast). Without encapsulation, there is little performance overhead other than what is normal for the traffic when routing in general. The RP will continue sending the traffic over the RP-tree after it receives it. This also means that the traffic may reach the RP-tree before it reaches the RP (in the case where the source branches off the RP-tree itself) which will also have the additional benefit of traffic flowing more efficiently towards receivers that are on the same side of the RP-tree as the source.

If the DR to the receiver decided that traffic coming from the RP-tree was using a sub-optimal path than if it was received from the source itself, it would issue a source-specific **Join** message towards the source. This would then make all intermediate routers register the Join message and then traffic would start flowing along that tree. This is the shortest path tree (SP-tree). At this point, the receiver would receive the traffic from both the RP-tree and the SP-tree. After the flow starts from the SP-tree, the DR will drop the packets from the RP-tree and send a prune message for that traffic towards the RP. This will stop the traffic from arriving from the RP. This scenario will most likely only occur when the traffic has to take a detour when arriving from the RP. Otherwise the RP-tree itself is used.

### **PIM-SM and VRRP Interoperability**

PIM-SM and VRRP operate independently. As such, Reverse Path Forwarding (RPF) checks will fail if the RP is behind a VRIP address.

#### **12.14.1.2 Internet Group Management Protocol**

Internet Group Management Protocol (IGMP) is the protocol used by hosts and routers to join and leave multicast groups. Routers will send IGMP queries at regular intervals querying whether there are any hosts interested in IP multicast traffic. Whenever an attached host is interested in receiving traffic for a certain group, it will send an IGMP report message expressing its interest. The router will then a) propagate this Join message to another router and b) send the relevant traffic to the segment to which the host is attached.

RUGGEDCOM ROX II supports both IGMPv2 and IGMPv3. IGMPv3 is backwards compatible with IGMPv2.

PIM-SM operates with IGMPv2. PIM-SSM operates with IGMPv3, which supports source-specific multicast capability.

#### **12.14.1.3 PIM-SSM**

Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) is derived from PIM-SM. Where PIM-SM accepts traffic from any multicast source on the network, the PIM-SSM protocol instead specifies the host(s) from which it will accept multicast traffic.

PIM-SSM operates with the IGMPv3 protocol. IGMPv3 supports source filtering, and is backwards-compatible with IGMPv2. For SSM to run with IGMPv3, SSM must be supported in the device, the host where the application is running, and the application itself. For more information about enabling IGMPv3 on the device, refer to "Enabling/Disabling a PIM-SM Interface" (Page 601).

In a network topology, only the last-hop device(s) must be PIM-SSM-compatible. Other devices in the network can be running PIM-SM.

A network configured to accept PIM-SM traffic can support PIM-SSM traffic at the same time. However, the full range of protocols required with PIM-SM (i.e. Rendezvous Point, Bootstrap Router, Designated Router, Shared Tree and Shortest Path Tree) are not required with PIM-SSM.

---

### Note

#### IGMPv3 and PIM-SSM

IGMP Join messages from Designated Routers can only be received by PIM-SSM if the **source-filter** for the DR is set to **include** mode.

---

## 12.14.2 Viewing the Status of PIM-SM

To view the status of PIM-SM, do the following:

1. Navigate to the **BSR** tab under **Layer 3 » Routing » Status » Multicast Routing » PIM-SM**. The address of the BSR is displayed.
2. Navigate to the **VInterface** tab under **Layer 3 » Routing » Status » Multicast Routing » PIM-SM**. The status of the configured devices is displayed.

---

### Note

A default rendezvous point with a local address of *169.254.0.1* always appears in the table. This internal rendezvous point is a placeholder to reserve the source-specific multicast address range.

Parameter	Description
Index	<b>Synopsis:</b> An integer Virtual interface index.
Local Address	<b>Synopsis:</b> A string between 1 and 16 characters long Local address.
Subnet	<b>Synopsis:</b> A string between 1 and 20 characters long Subnet.
Flags	<b>Synopsis:</b> A string between 1 and 128 characters long Flags indicates virtual interface information. <ul style="list-style-type: none"> <li>• <b>DISABLED:</b> The virtual interface is administratively disabled for PIM-SM.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>DOWN: This virtual interface is down.</li> <li>DR: Designated router.</li> <li>NO-NBR: No neighbor on this virtual interface.</li> <li>PIM: PIM neighbor.</li> <li>DVMRP: DVMRP neighbor.</li> </ul>
id	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>Neighbor address.</p>

3. Navigate to the **Mroute** tab under **Layer 3 » Routing » Status » Multicast Routing » PIM-SM**. The routing paths between the producer IP host and the rendezvous point are displayed.

Parameter	Description
Group	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>Multicast group address.</p>
Source	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>Source IP address.</p>
RP Address	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>RP (Rendezvous Point) address.</p>
Flags	<p><b>Synopsis:</b> A string between 1 and 128 characters long</p> <p>Flags.</p> <ul style="list-style-type: none"> <li>SPT: IIF (incoming interface) toward source.</li> <li>WC: (*,G) entry.</li> <li>RP: IIF (incoming interface) toward RP.</li> <li>CACHE: A mirror for the kernel cach.</li> <li>ASSERT: Upstream is not that of source.</li> <li>SG: (S,G) pure, not hanging off of (*,G).</li> <li>PMBR: (*,*,RP) entry (for interop).</li> </ul>

4. Navigate to the **Groute** tab under **Layer 3 » Routing » Status » Multicast Routing » PIM-SM**. The routing paths between the multicast traffic subscriber and the rendezvous point are displayed.

Parameter	Description
Group	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>Multicast group address.</p>
RP Address	<p><b>Synopsis:</b> A string between 1 and 16 characters long</p> <p>RP (Rendezvous Point) address.</p>

Parameter	Description
Flags	<p><b>Synopsis:</b> A string between 1 and 128 characters long</p> <p>Flags.</p> <ul style="list-style-type: none"> <li>• SPT: IIF (incoming interface) toward source.</li> <li>• WC: (*,G) entry.</li> <li>• RP: IIF (incoming interface) toward RP.</li> <li>• CACHE: A mirror for the kernel cach.</li> <li>• ASSERT: Upstream is not that of source.</li> <li>• SG: (S,G) pure, not hanging off of (*,G).</li> <li>• PMBR: (*,*,RP) entry (for interop).</li> </ul>

5. Navigate to the **RP** tab under **Layer 3 » Routing » Status » Multicast Routing » PIM-SM**. The RP server addresses are displayed.
6. Navigate to the **SSM Group** tab under **Layer 3 » Routing » Status » Multicast Routing » PIM-SM**. The multicast group addresses are displayed.

### 12.14.3 Viewing the Status of Dynamic Multicast Routing

To view the status of dynamic multicast routing, navigate to the **Multicast Routing** tab under **Layer 3 » Routing » Status**. If multicast routes have been configured, a list appears.

### 12.14.4 Configuring PIM-SM

PIM-SM can be used to establish and dynamically manage the Multicast Routing table.

To configure PIM-SM, do the following:

1. Make sure at least one non-passive interface with an IP address is available for PIM-SM. For more information, refer to "Managing PIM-SM Interfaces" (Page 601).
2. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Parameters**.
3. Configure the following parameters as required:

Parameter	Description
PIM-SM	Enable PIM-SM service.
Default Preference	<p><b>Synopsis:</b> An integer equal to or greater than 1</p> <p><b>Default:</b> 1024</p> <p>Default preference value. Preferences are used by assert elections to determine upstream routers.</p>

Parameter	Description
Default Metric	<p><b>Synopsis:</b> An integer equal to or greater than 1</p> <p><b>Default:</b> 1024</p> <p>Default metric value. Metric is the cost of sending data through interface.</p>
Broken Cisco Checksum	If your RP is a cisco and shows many PIM_REGISTER checksum errors from this router, setting this option will help.

4. If the device is to be a Rendezvous Point (RP) in a shared tree, set the device as an RP candidate. For more information, refer to "Setting the Device as an RP Candidate" (Page 600).
5. If the device is to be a Boot Strap Router (BSR), set the device as an BSR candidate. For more information, refer to "Setting the Device as an RP Candidate" (Page 600).
6. Define which multicast groups the device will handle. For more information, refer to "Adding a Multicast Group Prefix" (Page 604).
7. Commit the changes.

### 12.14.5 Setting the Device as a BSR Candidate

To set the device as a BSR candidate, do the following:

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Parameters**.
2. Under **BSR Candidate**, select the **Enabled** check box.
3. Configure the following parameters as required:

Parameter	Description
Local Address	<p><b>Synopsis:</b> A string between 7 and 15 characters long</p> <p>Local address to be used in the Cand-BSR messages. If not specified, the largest local IP address will be used (excluding passive interfaces).</p>
Priority	<p><b>Synopsis:</b> An integer between 1 and 255</p> <p>Bigger value means higher priority</p>

4. Commit the changes.

### 12.14.6 Setting the Device as an RP Candidate

To set the device as an RP candidate, do the following:

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Parameters**.

2. Under **RP Candidate**, select the **Enabled** check box.
3. Configure the following parameters as required:

Parameter	Description
Local Address	<b>Synopsis:</b> A string between 7 and 15 characters long  Local address to be used in the Cand-RP messages. If not specified, the largest local IP address will be used (excluding passive interfaces).
Timer	<b>Synopsis:</b> An integer between 10 and 65535 <b>Default:</b> 60  The number of seconds to wait between advertising Cand-RP message.
Priority	<b>Synopsis:</b> An integer between 1 and 255  Priority of this CRP, smaller value means higher priority.

4. Commit the changes.

## 12.14.7 Managing PIM-SM Interfaces

PIM-SM requires at least one interface on which to receive or transmit advertisements. The interface must be non-passive and be assigned an IP address.

### 12.14.7.1 Viewing a List of PIM-SM Interfaces

To view a list of PIM-SM interfaces, navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Interface**. If PIM-SM interfaces have been configured, a list appears.

If no PIM-SM interfaces have been configured, enable interfaces as needed. For more information about enabling PIM-SM interfaces, refer to "Enabling/Disabling a PIM-SM Interface" (Page 601).

### 12.14.7.2 Enabling/Disabling a PIM-SM Interface

To enable or disable a PIM-SM interface, do the following:

---

#### Note

Enabling IGMPv3 on an interface also enables PIM-SSM. IGMPv3 is backwards compatible with IGMPv2.

---

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Interface**.

**Note**

A maximum of 30 non-passive interfaces can be active for PIM-SM.

- For the desired interface, configure the following parameter(s) as required:

Parameter	Description
Passive	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Whether an interface is active or passive.</p>
IGMP Version	<p><b>Synopsis:</b> [ v2   v3 ]</p> <p><b>Default:</b> v2</p> <p>The version of IGMP. Options include:</p> <ul style="list-style-type: none"> <li>v2: IGMP version 2.</li> <li>v3: IGMP version 3. Backwards compatible with v2.</li> </ul>

**Note**

Clear the **Passive** check box to activate PIM-SM on the interface, or check the **Passive** check box to disable PIM-SM on the interface.

- Make sure the chosen interface is assigned an IP address. For more information, refer to "Managing IP Addresses for Routable Interfaces" (Page 223).
- For VLAN interfaces only, if IGMP snooping is enabled on the interface, make sure the IGMP query interval is set to 125 seconds. For more information, refer to "Configuring IGMP Snooping" (Page 306).  
The same is required for any Layer 2 switches on the network.
- Commit the changes.

## 12.14.8 Managing Static RP Addresses

A commonly used method for locating Rendezvous Points (RPs) is to target them directly by IP address, as opposed to locating them dynamically. Use static IP addresses when there are only a small number of RPs on the network and/or the RP assignment does not change often. It is important though that all static RP addresses be mirrored on all PIM-SM enabled devices in the multicast domain.

### 12.14.8.1 Viewing a List of Static RP Addresses

To view a list of static RP addresses, navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **RP Address**. If addresses have been configured, a list appears.

If no addresses have been configured, add addresses as needed. For more information, refer to "Adding a Static RP Address" (Page 603).

### 12.14.8.2 Adding a Static RP Address

To add a static RP address, do the following:

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **RP Address**.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Address	<b>Synopsis:</b> A string between 7 and 15 characters long Static RP (Rendezvous Point) address.
Group	<b>Synopsis:</b> A string between 9 and 18 characters long The multicast group the RP handles.

4. Click **OK** to add the static RP address.
5. Configure the following parameters as required:

#### Note

A higher value means a higher rendezvous point priority.

Parameter	Description
Priority	<b>Synopsis:</b> An integer between 1 and 255 Priority of the rendezvous point. A higher value means a higher priority.

6. Commit the changes.

### 12.14.8.3 Deleting a Static RP Address

To delete a static RP address, do the following:

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **RP Address**.
2. Select the RP address to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.14.9 Managing Multicast Group Prefixes

When nominated to a Rendezvous Point (RP), the device can serve up to 20 groups of multicast devices. The device is associated with a multicast group by defining the prefix for the group's multicast IP address (e.g. 225.1.2.0/24).

### 12.14.9.1 Viewing a List of Multicast Group Prefixes

To view a list of multicast group prefixes, navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Group Prefix**. If prefixes have been configured, a list appears.

If no prefixes have been configured, add prefixes as needed. For more information, refer to "Adding a Multicast Group Prefix" (Page 604).

### 12.14.9.2 Adding a Multicast Group Prefix

To add a multicast group prefix, do the following:

#### Note

A maximum of 20 group prefixes can be defined for PIM-SM.

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Group Prefix**.
2. Click **Add Entry**.
3. Configure the following parameters as required:

Parameter	Description
Multicast Group Prefix	<b>Synopsis:</b> A string between 9 and 18 characters long Multicast group prefix (for example, 225.1.2.0/24).

4. Click **OK**.
5. Commit the changes.

### 12.14.9.3 Deleting a Multicast Group Prefix

To delete a multicast group prefix, do the following:

1. Navigate to the **PIM-SM** tab under **Layer 3 » Routing » Multicast Routing**, and then select **Group Prefix**.
2. Select the prefix to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 12.14.10 Example: Configuring Protocol Independent Multicast

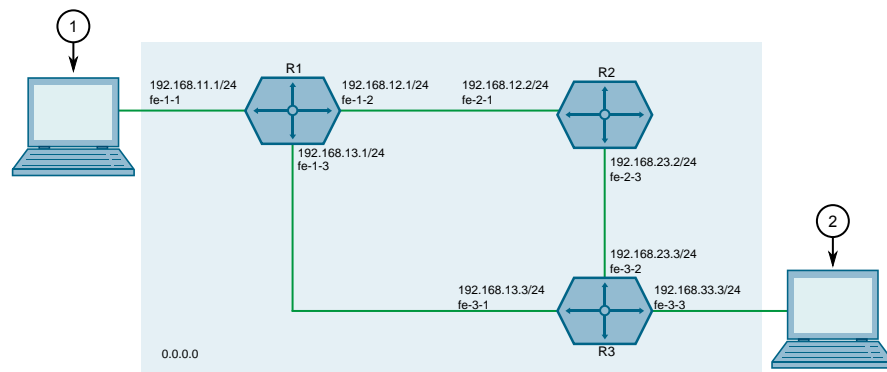
This section describes how to configure both PIM-SM and PIM-SSM using router ports in an OSPF network.

### Configuring PIM-SM

The following topology depicts a scenario where PIM-SM is being deployed in a simple OSPF network. Routers R1, R2 and R3 all reside in OSPF area 0.0.0.0.

#### NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① Producer
- ② Subscriber

Figure 12.15 PIM-SM Topology

To configure PIM-SM per the topology, do the following:

1. On R1, assign IP addresses to interfaces. For more information, refer to "Adding an IPv4 Address" (Page 225).

Interface	IP Address/Prefix
fe-1-1	192.168.11.1/24
fe-1-2	192.168.12.1/24
fe-1-3	192.168.13.1/24

2. On R2, assign IP addresses to interfaces. For more information, refer to "Adding an IPv4 Address" (Page 225).

Interface	IP Address/Prefix
fe-2-1	192.168.12.2/24
fe-2-3	192.168.23.2/24



3. On R3, assign IP addresses to interfaces. For more information, refer to "Adding an IPv4 Address" (Page 225).

Interface	IP Address/Prefix
fe-3-1	192.168.13.3/24
fe-3-2	192.168.23.3/24
fe-3-3	192.168.33.3/24

4. Configure OSPF. For more information, refer to "Configuring OSPF" (Page 523).
  - a. Enable OSPF on routers R1, R2 and R3.
  - b. Add the following areas:

Router	Area ID	IP Address/Prefix
R1	0.0.0.0	192.168.11.0/24
R1	0.0.0.0	192.168.12.0/24
R1	0.0.0.0	192.168.13.0/24
R2	0.0.0.0	192.168.12.0/24
R2	0.0.0.0	192.168.23.0/24
R3	0.0.0.0	192.168.13.0/24
R3	0.0.0.0	192.168.23.0/24
R3	0.0.0.0	192.168.33.0/24

- c. Make sure the default value for the interfaces is active (not passive):

Router	Interface	Passive Default Value
R1	fe-1-2	False
R1	fe-1-3	False
R2	fe-2-1	False
R2	fe-2-3	False
R3	fe-3-1	False
R3	fe-3-2	False

5. Enable PIM-SM on routers R1, R2 and R3. For more information, refer to "Configuring PIM-SM" (Page 599).
6. Enable PIM-SM on all multicast path interfaces. For more information, refer to "Enabling/Disabling a PIM-SM Interface" (Page 601).
7. Configure the Rendezvous Point (RP).
  - a. On R2, assign an IPv4 address to the desired interface to be used for the RP. For example, assign address is 2.2.2.2/32 to the dummy0 interface. For more information, refer to "Adding an IPv4 Address" (Page 225).
  - b. Configure router R2 as the rendezvous point (RP). For example, assign static address 2.2.2.2/32, and group address 234.1.6.1/24. For more information, refer to "Adding a Static RP Address" (Page 603).
  - c. On R1 and R3, add the RP address. For more information, refer to "Adding a Static RP Address" (Page 603).
8. Verify the configuration.

- a. Make sure routers R1, R2 and R3 can ping one another.
- b. Make sure the producer and subscriber can ping each other.

### Final PIM-SM Configuration Example

The following configuration reflects the topology:

- **R1**

```
R1# show running-config routing multicast dynamic pim-sm
routing multicast dynamic pim-sm
enabled
no broken-cisco-checksum
interface dummy0
!
interface fe-1-2
no passive
!
interface fe-1-3
no passive
!
interface fe-cm-1
!
interface gre-g1
no passive
!
interface switch.0001
no passive
!
rp-address 2.2.2.2 234.1.6.1/32
!
!
```

- **R2**

```
R2# show running-config routing multicast dynamic pim-sm
routing multicast dynamic pim-sm
enabled
no broken-cisco-checksum
interface dummy0
no passive
!
interface fe-2-1
no passive
!
interface fe-2-3
no passive
!
interface fe-cm-1
!
interface switch.0001
!
rp-address 2.2.2.2 234.1.6.1/32
!
group-prefix 234.1.6.1/24
!
!
```

- **R3**

```
R3# show running-config routing multicast dynamic pim-sm
routing multicast dynamic pim-sm
enabled
```

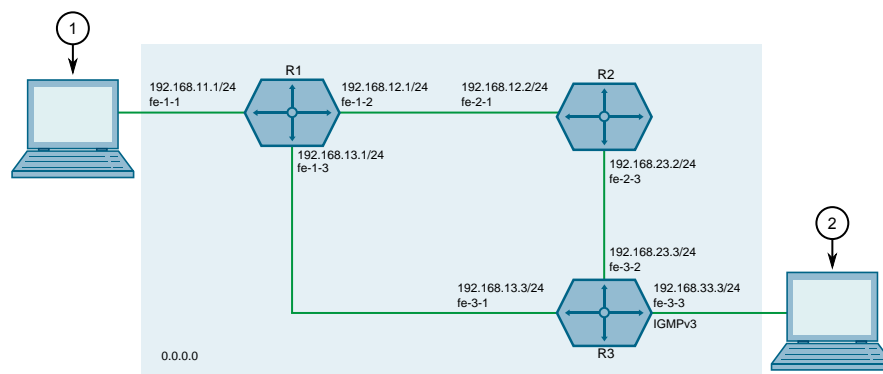
```

no broken-cisco-checksum
interface dummy0
  no passive
!
interface fe-3-1
  no passive
!
interface fe-3-2
  no passive
!
interface fe-3-5
!
interface fe-cm-1
!
interface gre-g1
  no passive
!
interface switch.0001
  no passive
!
rp-address 2.2.2.2 234.1.6.1/32
!
!
!

```

## Configuring PIM-SSM

PIM-SSM configuration is similar to PIM-SM configuration, however IGMPv3 must be enabled on the subscriber-facing interface.



- ① Producer
- ② Subscriber

Figure 12.16 PIM-SM Topology

To configure PIM-SSM per the topology, do the following:

1. Configure routers R1, R2 and R3 per subsection "Configuring PIM-SM" (Page 605).
2. On router R3, activate PIM-SSM by selecting IGMPv3 as the IGMP version on the port facing the subscriber. For more information, refer to "Enabling/Disabling a PIM-SM Interface" (Page 601).

3. Verify the configuration by making sure clients are properly registered on the subscriber (R3).
  - a. Configure R3 to send IGMPv3 reports to the desired multicast groups. For example:

Multicast Group	Source IP	Virtual Interface Index
232.1.2.9	192.168.11.4	4
232.1.2.8	192.168.11.4	4
232.1.2.7	192.168.11.4	4
232.1.2.6	192.168.11.4	4
232.1.2.5	192.168.11.4	4

For more information, refer to "Configuring IGMP Snooping" (Page 306).

- b. On R1 and R3, verify the groups listed in step 3a (Page 609) are registered as SSM groups. For more information, refer to "Viewing the Status of PIM-SM" (Page 597).
- c. Verify the requested UDP/TCP multicast traffic is being forwarded to R3 based on the source IP and the multicast group being requested.
- d. On R1, verify that only the traffic being forwarded to R3 through the best route (in this example the direct connection fe-1-3) is what is being requested and the non-requested traffic is not being forwarded.
- e. Verify that R3 is receiving multicast traffic from R1 through interface fe-3-1.

## Final PIM-SSM Configuration Example

The following configuration reflects the topology:

- **R1**

```
R1# show running-config routing multicast dynamic pim-sm
routing multicast dynamic pim-sm
  enabled
  no broken-cisco-checksum
  interface dummy0
  !
  interface fe-1-2
    no passive
  !
  interface fe-1-3
    no passive
  !
  interface fe-cm-1
  !
  interface gre-g1
    no passive
  !
  interface switch.0001
    no passive
  !
  !
```

- **R2**

```
R2# show running-config routing multicast dynamic pim
routing multicast dynamic pim-sm
```

```
enabled
no broken-cisco-checksum
interface dummy0
!
interface fe-2-1
no passive
!
interface fe-2-3
no passive
!
interface fe-cm-1
!
interface switch.0001
!
!
```

- **R3**

```
R3# show running-config routing multicast dynamic pim
routing multicast dynamic pim-sm
enabled
no broken-cisco-checksum
interface dummy0
!
interface fe-3-1
no passive
!
interface fe-3-2
no passive
!
interface fe-3-5
!
interface fe-cm-1
!
interface gre-g1
no passive
!
interface switch.0001
no passive
igmp-version v3
!
!
```

## Network Redundancy

This chapter describes protocols and features that allow RUGGEDCOM ROX II to operate with redundancy, protecting the network from crippling service disruptions from single points of failure.

### 13.1 Managing VRRP

The Virtual Router Redundancy Protocol (VRRP) is a gateway redundancy protocol. It provides a gateway failover mechanism invisible to hosts and other devices that send traffic through the gateway.

VRRP eliminates a single point of failure associated with statically routed networks by providing automatic failover using alternate routers. The RUGGEDCOM ROX II VRRP daemon (keepalived) is an [RFC 5798](http://tools.ietf.org/html/rfc5798) [http://tools.ietf.org/html/rfc5798] version 2 and version 3 compliant implementation of VRRP.

---

**Note**

RFC 5798 defines the standard for VRRP version 3 on IPv4 and IPv6. Only IPv4 is supported in this release of RUGGEDCOM ROX II.

---

#### 13.1.1 VRRP Concepts

This section describes some of the concepts important to the implementation of the Virtual Router Redundancy Protocol (VRRP) in RUGGEDCOM ROX II.

##### 13.1.1.1 Static Routing vs. VRRP

Many network designs employ a statically configured default gateway in the network hosts. A static default gateway is simple to configure, requires little if any overhead to run, and is supported by virtually every IP implementation. When the Dynamic Host Configuration Protocol (DHCP) is employed, hosts may accept a configuration for only a single default gateway.

Unfortunately, this approach creates a single point of failure. Loss of the router supplying the default gateway, or the router's WAN connection, results in isolating the hosts that rely upon the default gateway.

There are a number of ways to provide redundant connections for the hosts. Some hosts can configure alternate gateways while others are intelligent enough to participate in dynamic routing protocols such as the Routing Information Protocol

(RIP) or Open Shortest Path First (OSPF) routing protocol. Even when available, these approaches are not always practical due to administrative and operation overhead.

VRRP solves the problem by allowing the establishment of a *virtual router group*, composed of a number of routers that provide one gateway IP. VRRP uses an election protocol to dynamically assign responsibility for the gateway to one of the routers in the group. This router is called the Master.

If the Master (or, optionally, a condition) fails, the alternate (or backup) routers in the group elect a new Master. The new master owns the virtual IP address and issues a gratuitous ARP to inform the network of where the gateway can be reached.

Since the host's default route and MAC address does not change, packet loss at the hosts is limited to the amount of time required to elect a new router.

### 13.1.1.2 VRRP Terminology

Each physical router running VRRP is known as a VRRP Router. Two or more VRRP Routers can be configured to form a *Virtual Router*. Each VRRP Router may participate in one or more Virtual Routers.

Each Virtual Router has a user-configured Virtual Router Identifier (VRID) and a Virtual IP address or set of IP addresses on the shared LAN. Hosts on the shared LAN are configured to use these addresses as the default gateway.

Each router in the Virtual Router Group has a specific priority, which is a number between 1 and 255. The router with the highest priority (or highest number) is elected the Master, while all other routers are considered Backups.

On RUGGEDCOM RX5000/MX5000/MX5000RE devices with RUGGEDCOM ROX II v2.3 or higher installed, if the router with the highest priority is in a fault state, the backup VRRP Router can delay its transition to becoming the Master router. The length of the delay is user-defined.

VRRP can also monitor a specified interface and give up control of a gateway IP to another VRRP Router if that interface goes down.

### An Example of VRRP

In the following example, host 1 uses a gateway of 1.1.1.253 and host 2 uses a gateway of 1.1.1.252. The 1.1.1.253 gateway is provided by VRID 10. In normal practice, router 1 will provide this virtual IP since its priority for VRID 10 is higher than that of router 2. If router 1 becomes inoperative or if its w1ppp link fails, it will relinquish control of gateway IP 1.1.1.253 to router 2.

In a similar fashion host 2 can use the VRID 11 gateway address of 1.1.1.252, which will normally be supplied by router 2.

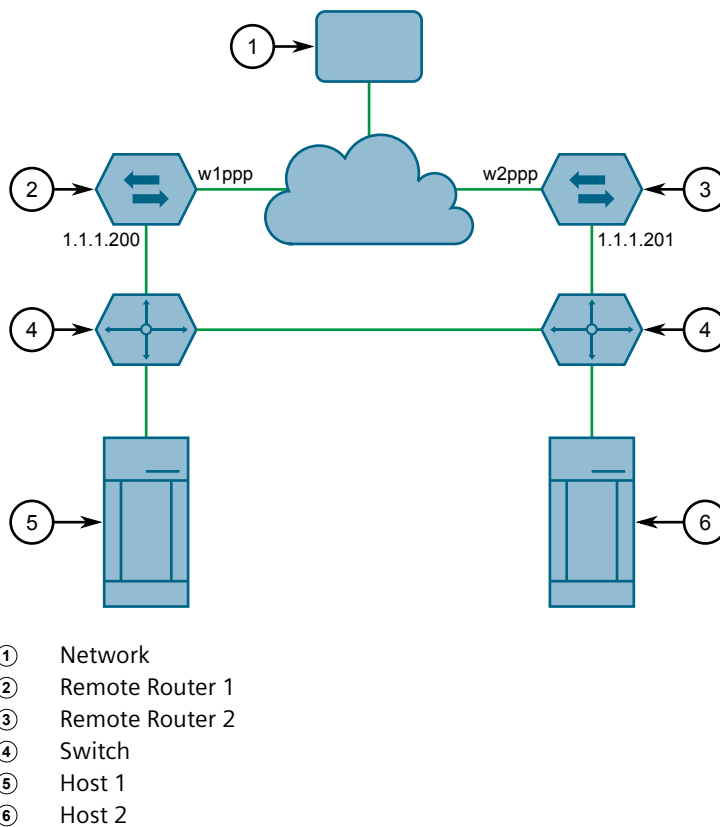


Figure 13.1 VRRP Example

In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
<ul style="list-style-type: none"> <li>VRID 10 Gateway IP: 1.1.1.253</li> <li>VRID 10 Priority: 100</li> <li>VRID 10 Monitor Interface: w1ppp</li> <li>VRID 11 Gateway IP: 1.1.1.252</li> <li>VRID 11 Priority: 50</li> </ul>	<ul style="list-style-type: none"> <li>VRID 10 Gateway IP: 1.1.1.253</li> <li>VRID 10 Priority: 50</li> <li>VRID 11 Gateway IP: 1.1.1.252</li> <li>VRID 11 Priority: 100</li> <li>VRID 11 Monitor Interface: w2ppp</li> </ul>

Traffic from host 1 is sent through router 1, and traffic from host 2 is sent through router 2. A failure of either router or their WAN link will be recovered by the other router.

Note that both routers can always be reached by the hosts at their *real* IP addresses.

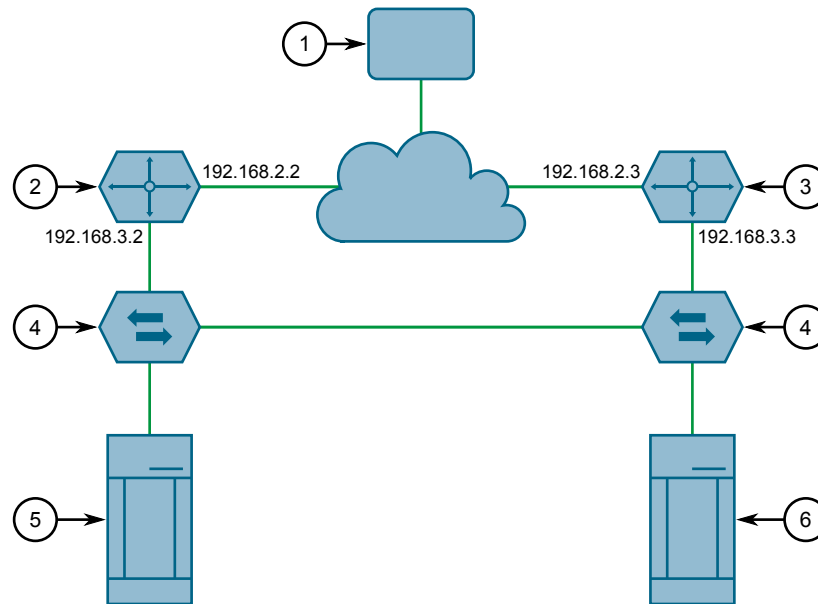
Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

### An Example of VRRP Groups

In the next example, both host 1 and host 2 use a gateway of 192.168.3.10. The external side can access the internal side by gateway 192.168.2.10. VRID\_20 and VRID\_21 are grouped together. Normally, router 1 will provide both an internal and external access gateway, as its priority is higher than those on Router 2. When either



the internal or external side of Router 1 becomes inoperative, Router 1 will remove give control of both 192.168.2.10 and 192.168.3.10 gateways to Router 2.



- ① Network
- ② Remote Router 1
- ③ Remote Router 2
- ④ Switch
- ⑤ Host 1
- ⑥ Host 2

Figure 13.2 VRRP Group Example

In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
<ul style="list-style-type: none"> <li>• VRID_20 Gateway IP: 192.168.2.10</li> <li>• VRID_20 Priority: 100</li> <li>• VRID_21 Gateway IP: 192.168.3.10</li> <li>• VRID_21 Priority: 100</li> </ul>	<ul style="list-style-type: none"> <li>• VRID_20 Gateway IP: 192.168.2.10</li> <li>• VRID_20 Priority: 50</li> <li>• VRID_21 Gateway IP: 192.168.3.10</li> <li>• VRID_21 Priority: 50</li> </ul>

Other VRRP parameters are the Advertisement Interval and Gratuitous ARP Delay. The advertisement interval is the time between which advertisements are sent. A backup router will assume the role of Master three advertisement intervals after the Master fails. If a monitored interface goes down, a Master router will immediately signal an election and allow a Backup router to assume the Master roles.

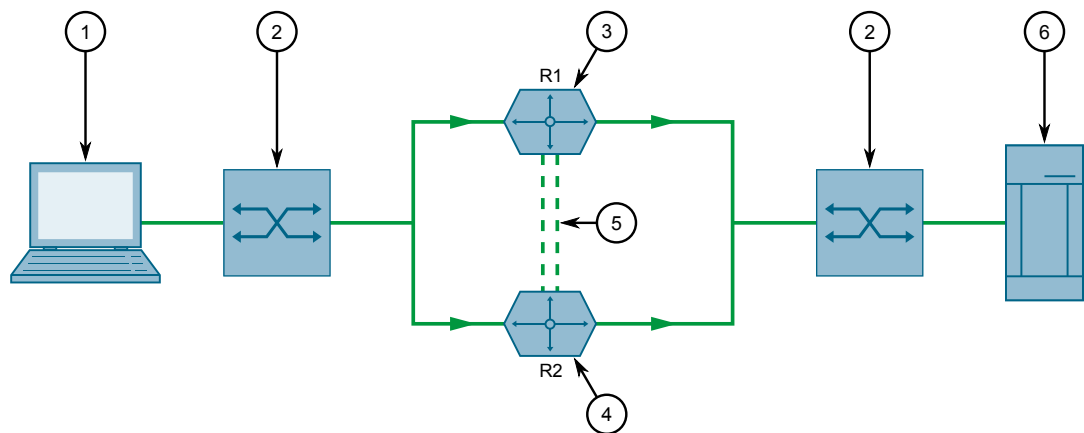
The router issues a set of gratuitous ARPs when moving between Master and Backup roles. These unsolicited ARPs teach the hosts and switches in the network of the current MAC address and port associated with the gateway. The router will issue a second set of ARPs after the time specified by the Gratuitous ARP delay.

### 13.1.1.3 Connection Synchronization

When failover occurs, hosts must typically either reconnect manually to the backup firewall, or wait for the connection to automatically reconnect. This can sometimes take several minutes.

When connection synchronization is enabled, stateful connections are maintained when a VRRP master router fails, resulting in a seamless failover to the VRRP backup router. This is done by synchronizing the firewall and NAT states between the master and backup routers.

In the following example, when the master router (R1) fails, the firewall connection and NAT states are initialized automatically for the backup router (R2). The backup router then becomes the new VRRP master.



- ① Host A
- ② Switch
- ③ Primary VRRP Firewall and Router (R1)
- ④ Backup VRRP Firewall and Router (R2)
- ⑤ Dedicated Links
- ⑥ Host B

Figure 13.3 Connection Synchronization Example

## 13.1.2 Viewing the Status of VRRP

To view the status of VRRP, navigate to the **Status** tab under **Layer 3 » VRRP**.

This following information is provided:

Parameter	Description
Instance Name	<b>Synopsis:</b> A string The VRRP instance name.
State	<b>Synopsis:</b> A string The VRRP instance state.

Parameter	Description
Priority	<b>Synopsis:</b> A string The VRRP instance priority.
Time of Change to Current State	<b>Synopsis:</b> A string The time of change to the current state.
Interface State	<b>Synopsis:</b> A string The VRRP interface state.
monitor-interface-state	<b>Synopsis:</b> A string Monitors the interface state.

### 13.1.3 Enabling/Disabling VRRP

To enable or disable VRRP, do the following:

1. Navigate to the **Configurations** tab under **Layer 3 » VRRP**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enabled VRRP Service	Enables or disables the VRRP service.
Router ID	<b>Synopsis:</b> A string The router ID for VRRP logs.

3. Commit the changes.

### 13.1.4 Managing VRRP Trackers

VRRP trackers monitor the state/condition of a route. When the route is unavailable, VRRP will lower its priority or transition it to a fault state.

---

#### Note

The decision to increase or decrease the priority of a route must be done in coordination with any backup VRRP Routers since the priority decides whether a router becomes a Master or a Backup. For example, if Router X's priority is 150 and Router Y's priority is 145, Router X's priority must be lowered by 6 to make it a Backup router.

---

### 13.1.4.1 Viewing a List of VRRP Trackers

To view a list of VRRP trackers, navigate to the **Trackers** tab under **Layer 3 » VRRP**. If trackers have been configured, a list appears.

If no VRRP trackers have been configured, add trackers as needed. For more information, refer to "Adding a VRRP Tracker" (Page 617).

### 13.1.4.2 Adding a VRRP Tracker

To add a VRRP tracker, do the following:

1. Navigate to the **Trackers** tab under **Layer 3 » VRRP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 64 characters long The name of the tracker.

4. Click **OK** to add the tracker.
5. Configure the following parameter(s) as required:

Parameter	Description
Track Type	<b>Synopsis:</b> [ route ] <b>Default:</b> route The type of condition for the tracker to check.
Network	<b>Synopsis:</b> A string between 9 and 18 characters long The network to track. The tracker checks for a route to this network in the routing table.
Interface	<b>Synopsis:</b> A string The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
Interval	<b>Synopsis:</b> An integer between 1 and 120 The number of seconds between tracker queries.
Weight	<b>Synopsis:</b> An integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the tracker falls. When positive, the priority increases by this amount when the tracker rises. When not set, the state changes to the fault state when the tracker falls.

Parameter	Description
Rise	<b>Synopsis:</b> An integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
Fall	<b>Synopsis:</b> An integer between 1 and 65535 The number of unsuccessful tracker queries before changing the router priority.

6. Commit the changes.

### 13.1.4.3 Deleting a VRRP Tracker

To delete a VRRP tracker, do the following:

1. Navigate to the **Trackers** tab under **Layer 3 » VRRP**.
2. Select the tracker to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.1.5 Managing VRRP Groups

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

### 13.1.5.1 Viewing a List of VRRP Groups

To view a list of VRRP groups, navigate to the **Group** tab under **Layer 3 » VRRP**. If groups have been configured, a list appears.

If no VRRP groups have been configured, add groups as needed. For more information, refer to "Adding a VRRP Group" (Page 618).

### 13.1.5.2 Adding a VRRP Group

To add a VRRP group, do the following:

1. Navigate to to the **Group** tab under **Layer 3 » VRRP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Group Name	<b>Synopsis:</b> A string between 1 and 64 characters long The VRRP group name.

4. Click **OK** to add the group.
5. Commit the change.

### 13.1.5.3 Deleting a VRRP Group

To delete a VRRP group, do the following:

1. Navigate to to the **Group** tab under **Layer 3 » VRRP**.
2. Select the group to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.1.6 Managing VRRP Instances

VRRP instances define the interfaces monitored by VRRP. Two or more instances can be added to the same VRRP group, which allows them to failover together.

### 13.1.6.1 Viewing a List of VRRP Instances

To view a list of VRRP instances, navigate to the **Instance** tab under **Layer 3 » VRRP**. If instances have been configured, a list appears.

If no VRRP instances have been configured, add instances as needed. For more information, refer to "Adding a VRRP Instance" (Page 619).


### 13.1.6.2 Adding a VRRP Instance

To add a VRRP instance, do the following:

1. Make sure a VRRP group has been configured. For more information, refer to "Adding a VRRP Group" (Page 618).
2. Navigate to the **Instance** tab under **Layer 3 » VRRP**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Instance Name	<p><b>Synopsis:</b> A string between 1 and 64 characters long</p> <p>The name of the VRRP instance - the name must not include spaces.</p>

5. Click **OK** to add the instance.
6. Configure the following parameter(s) as required:

<p> <b>NOTICE</b></p> <p>When <b>Use Virtual Mac</b> is enabled, an additional firewall interface <i>vrrp.{ VRID }</i> is required, where { VRID } is the name of the virtual router identifier. For more information about adding a firewall interface, refer to "Adding an Interface" (Page 205).</p>
--

**Note**

A preemption occurs when either:

- a backup VRRP router gains higher priority and transitions to the Master state
- VRRP is initiated and this router has higher priority than that of any VRRP router on the network

**Note**

The VRRP Instance Form displays some fields differently depending on whether version 2 or version 3 is chosen in the version field.

- Choosing VRRP version 2 displays the **Advertisement Interval** field.
- Choosing VRRP version 3 displays the **Advertisement Interval Millisecond** field.

Parameter	Description
VRRP Version	<p><b>Synopsis:</b> An integer between 2 and 3</p> <p><b>Default:</b> 2</p> <p>Configure VRRP version for this instance.</p>
Interface	<p><b>Synopsis:</b> A string</p> <p>The interface used by the VRRP service to communicate with other VRRP-enabled routers using the VRRP protocol. Additionally, this interface hosts the Virtual IP (VRIP) when the 'Use Virtual MAC' parameter is not enabled.</p>
Virtual Router ID	<p><b>Synopsis:</b> An integer between 1 and 255</p> <p>The Virtual Router ID. All routers supplying the same VRIP should have the same VRID.</p>

Parameter	Description
Priority	<b>Synopsis:</b> An integer between 0 and 255  The priority for the VRRP instance. When electing the master, the highest priority wins. The configurable range is 1 to 255. A value of zero (0) is invalid.
Advertisement Interval	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1  VRRP2 advertisement interval, in seconds.
Advertisement Interval (ms)	<b>Synopsis:</b> An integer between 20 and 3000 <b>Default:</b> 1000  VRRP3 advertisement interval in millisecond, must be multiple of 10.
Gratuitous ARP Delay	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 5  Gratuitous ARP delay, in seconds. Sets the delay after the router changes state state before a second set of gratuitous ARPs are sent.
No Preempt	When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
Preempt Delay	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0  The time, in seconds, after startup until preemption.
Fault to Master Delay	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0  The delay, in seconds, before a transition from the fault state to the master state occurs, thereby preempting the current master.
Use Virtual MAC	When enabled, the router uses a virtual MAC address for the Virtual IP (VRIP).
VRRP Group	<b>Synopsis:</b> A string between 1 and 64 characters long  Binds this VRRP instance to a VRRP group.

7. [Optional] Add one or more VRRP monitors. For more information, refer to "Adding a VRRP Monitor" (Page 622).
8. [Optional] Add one or more track scripts. For more information, refer to "Adding a Track Script" (Page 623).
9. Add one or more virtual IP addresses. For more information, refer to "Adding a Virtual IP Address" (Page 624).
10. Commit the changes.



### 13.1.6.3 Deleting a VRRP Instance

To delete a VRRP instance, do the following:

1. Navigate to the **Instance** tab under **Layer 3 » VRRP**.
2. Select the instance to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.1.7 Managing VRRP Monitors

A VRRP monitor selects an extra interface to monitor. If the interface becomes unavailable, the router will relinquish control of the gateway IP address to another VRRP Router.

### 13.1.7.1 Viewing a List of VRRP Monitors

To view a list of VRRP monitors, navigate to the **Monitor - { name }** tab under **Layer 3 » VRRP » Instance**, where { name } is the name of the VRRP instance. If monitors have been configured, a list appears.

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to "Adding a VRRP Monitor" (Page 622).

### 13.1.7.2 Adding a VRRP Monitor

To add a VRRP monitor, do the following:

1. Navigate to the **Monitor - { name }** tab under **Layer 3 » VRRP » Instance**, where { name } is the name of the VRRP instance.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Monitor Interface	<b>Synopsis:</b> A string between 1 and 15 characters long The name of the interface.

4. Click **OK** to add the monitor.
5. Configure the following parameter(s) as required:

Parameter	Description
Weight	<b>Synopsis:</b> An integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the interface fails. When positive, the priority increases by

Parameter	Description
	this amount when the interface is up. When not set, the state changes to the fault state when the interface fails.

6. Commit the change.

### 13.1.7.3 Deleting a VRRP Monitor

To delete a VRRP monitor, do the following:

1. Navigate to the **Monitor - { name }** tab under **Layer 3 » VRRP » Instance**, where { name } is the name of the VRRP instance.
2. Select the monitor to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.1.8 Managing Track Scripts

Track scripts are used to associate VRRP trackers with VRRP instances.

### 13.1.8.1 Viewing a List of Track Scripts

To view a list of track scripts, navigate to the **Instance** tab under **Layer 3 » VRRP**, and then click the **Track Script** tab for the desired instance. If track scripts have been configured, a list appears.

If no track scripts have been configured, add track scripts as needed. For more information, refer to "Adding a Track Script" (Page 623).

### 13.1.8.2 Adding a Track Script

To add a track script, do the following:

1. Navigate to the **Instance** tab under **Layer 3 » VRRP**, and then click the **Track Script** tab for the desired instance.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Tracker	<b>Synopsis:</b> A string between 1 and 64 characters long Select a tracker to monitor VRRP instance.

4. Click **OK** to add the track script. A dialog box appears.
5. Configure the following parameter(s) as required:

Parameter	Description
Weight	<p><b>Synopsis:</b> An integer between -254 and 254</p> <p>This setting overwrites the weight setting in the tracker. If negative, the priority decreases by this amount when the tracker falls. If positive, the priority increases by this amount when the tracker rises. If not set, the weight value in the tracker will be used.</p>

6. Commit the change.

### 13.1.8.3 Deleting a Track Script

To delete a track script, do the following:

1. Navigate to the **Instance** tab under **Layer 3 » VRRP**, and then click the **Track Script** tab for the desired instance.
2. Select the track script to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.1.9 Managing Virtual IP Addresses

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

### Note

A VRRP packet will be ignored if any virtual IP address listed in the packet is not defined on the device. A syslog message is added for every 20 ignored VRRP packets.

### 13.1.9.1 Viewing a List of Virtual IP Addresses

To view a list of virtual IP addresses, navigate to the **Instance** tab under **Layer 3 » VRRP**, and then click the **VRIP** tab for the desired VRRP instance. If addresses have been configured, a list appears.

If no virtual IP addresses have been configured, add addresses as needed. For more information, refer to "Adding a Virtual IP Address" (Page 624).

### 13.1.9.2 Adding a Virtual IP Address

To add a virtual IP address, do the following:

1. Navigate to the **Instance** tab under **Layer 3 » VRRP**, and then click the **VRIP** tab for the desired VRRP instance.

2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Virtual IP Address/Netmask	<b>Synopsis:</b> A string between 9 and 18 characters long The virtual IP address/netmask.

4. Click **OK** to add the virtual IP address.
5. Commit the change.

### 13.1.9.3 Deleting a Virtual IP Address

To delete a virtual IP address, do the following:

1. Navigate to the **Instance** tab under **Layer 3 » VRRP**, and then click the **VRIP** tab for the desired VRRP instance.
2. Select the address to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.1.10 Managing Connection Synchronization

This section describes how to configure connection synchronization between two VRRP-enabled routers.

### 13.1.10.1 Configuring Connection Synchronization

To configure connection synchronization, do the following for *each* VRRP-enabled device:

#### NOTICE

Well-formed stateful firewall rules are required. For more information, refer to "Stateless vs. Stateful Firewalls" (Page 195).

1. Configure a firewall with stateful firewall rules to control inbound and outbound traffic. For more information, refer to "Adding a Firewall" (Page 198).
2. Make sure the VRRP service is enabled. For more information, refer to "Enabling/Disabling VRRP" (Page 616).
3. Configure VRRP instances and groups. For more information, refer to "Adding a VRRP Instance" (Page 619) and "Adding a VRRP Group" (Page 618).
4. Define one or more dedicated links for each VRRP group. For more information, refer to "Adding a Dedicated Link" (Page 626).

5. Select a link to be the default dedicated link for any VRRP group not assigned a dedicated link. For more information, refer to "Selecting a Default Dedicated Link" (Page 627).
6. Enable the configuration synchronization service. For more information, refer to "Enabling/Disabling Connection Synchronization" (Page 626).

Once the configuration is complete, verify the status of the service on both devices. For more information, refer to "Viewing the Status of Each Dedicated Link" (Page 628).

### 13.1.10.2 Enabling/Disabling Connection Synchronization

To enable or disable connection synchronization, do the following:

1. Navigate to the **Conn Sync Parameters** tab under **Layer 3 » VRRP » Conn Sync**.
2. Click **Enabled** to enable connection synchronization, or clear **Enabled** to disable the service.
3. Commit the change.

### 13.1.10.3 Viewing a List of Dedicated Links

To view a list of dedicated links, navigate to the **Dedicated Link** tab under **Layer 3 » VRRP » Conn Sync**. If dedicated links have been configured, a list appears.

If no dedicated links have been configured, add dedicated links as needed. For more information, refer to "Adding a Dedicated Link" (Page 626).

### 13.1.10.4 Adding a Dedicated Link

To add a dedicated link, do the following:

1. Navigate to the **Dedicated Link** tab under **Layer 3 » VRRP » Conn Sync**.

---

**Note**

RUGGEDCOM ROX II supports up to four dedicated links.

---

2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 16 characters long Dedicated link name.

4. Click **OK** to add the dedicated link. A dialog box appears.

5. Configure the following parameter(s) as required:

Parameter	Description
Interface	<b>Synopsis:</b> A string between 1 and 15 characters long The interface name of the dedicated link.
IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long The IPv4 or IPv6 address of the dedicated link interface.
Multicast Address	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 7 and 39 characters long <b>Default:</b> 225.0.0.50 The destination IPv4 or IPv6 multicast address of the dedicated link.
Group ID	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 3780 The multicast group ID of the cluster.
Sending Buffer Size	<b>Synopsis:</b> An integer between 64 and 2560 <b>Default:</b> 1220 The sending socket buffer size in kB.
Receiving Buffer Size	<b>Synopsis:</b> An integer between 64 and 2560 <b>Default:</b> 1220 The receiving socket buffer size in kB.

6. Commit the change.

### 13.1.10.5 Deleting a Dedicated Link

To delete a dedicated link, do the following:

1. Navigate to the **Dedicated Link** tab under **Layer 3 » VRRP » Conn Sync**.
2. Select the dedicated link to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 13.1.10.6 Selecting a Default Dedicated Link

To select a default a dedicated link, do the following:

1. Navigate to the **Conn Sync Parameters** tab under **Layer 3 » VRRP » Conn Sync**.
2. Configure the following parameter(s) as required:

Parameter	Description
Default Dedicated Link	<b>Synopsis:</b> A string between 1 and 16 characters long The default dedicated link.

3. Commit the change.

### 13.1.10.7 Viewing the Status of Each Dedicated Link

To view the status of all dedicated links, do the following:

- Navigate to the **Conn Sync Status** tab under **Layer 3 » VRRP » Status**.

The following information is provided:

Parameter	Description
Name	<b>Synopsis:</b> A string The conn-sync dedicated link interface name.
State	<b>Synopsis:</b> A string The conn-sync dedicated link status.
Role	<b>Synopsis:</b> A string The conn-sync dedicated link role.
Byte Sent	<b>Synopsis:</b> An integer The number of bytes sent on conn-sync dedicated link.
Byte Received	<b>Synopsis:</b> An integer The number of bytes received on conn-sync dedicated link.
Packet Sent	<b>Synopsis:</b> An integer The number of packets sent on conn-sync dedicated link.
Packet Received	<b>Synopsis:</b> An integer The number of packets received on conn-sync dedicated link.
Error Sent	<b>Synopsis:</b> An integer The number of errors sent on conn-sync dedicated link.
Error Received	<b>Synopsis:</b> An integer The number of errors received on conn-sync dedicated link.

## 13.2 Managing VRRP within VRF

RUGGEDCOM ROX II supports VRRP configuration within VRF definitions, for IPv4 addresses. This allows gateway redundancy to be applied to individual VRF instances.

For more information about virtual routing and forwarding, refer to "VRF Concepts" (Page 558).

### 13.2.1 Configuring VRRP within VRF

To configure VRRP within a VRF, do the following:

1. Configure virtual routing and forwarding. For more information, refer to "Configuring VRF" (Page 559).
2. Enable the VRRP service for each VRF definition. For more information, refer to "Adding VRRP Service to a VRF" (Page 630).
3. [Optional] Add VRRP trackers as needed. For more information, refer to "Adding a VRRP Tracker for a VRF" (Page 631).
4. [Optional] Add VRRP groups as needed. For more information, refer to "Adding a VRRP Group for a VRF" (Page 633).
5. [Optional] Add VRRP monitors as needed. For more information, refer to "Adding a VRRP Monitor to a VRF" (Page 637).
6. [Optional] Add track scripts as needed. For more information, refer to "Adding a VRRP Track Script to a VRF" (Page 638).
7. Add a virtual IP address for the VRF. For more information, refer to "Adding a Virtual IP Address to a VRF" (Page 639).
8. Verify the network configuration.

### 13.2.2 Viewing the VRRP Status for a VRF

To view the VRRP status for a VRF, navigate to the **VRRP Status** tab under **Layer 3 » Routing » VRF » Status » VRRP-VRF**. If VRRP instances have been configured, a list appears.

This table provides the following information:

Parameter	Description
Instance Name	<b>Synopsis:</b> A string The VRRP instance name.
State	<b>Synopsis:</b> A string The VRRP instance state.
Priority	<b>Synopsis:</b> A string The VRRP instance priority.



## 13.2.3 Configuring VRRP Service for a VRF

Parameter	Description
Time of Change to Current State	<b>Synopsis:</b> A string The time of change to the current state.
Interface State	<b>Synopsis:</b> A string The VRRP interface state.
Monitored Interface State	<b>Synopsis:</b> A string Monitors the interface state.

## 13.2.3 Configuring VRRP Service for a VRF

This section describes how to view, add and delete VRRP for a VRF.

## 13.2.3.1 Viewing a List of VRFs Configured with VRRP Service

To view a list of VRFs configured with VRRP service, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » VRRP - VRF**. If a VRF has been configured with VRRP service, a list appears.

If no VRF has been configured with VRRP service, add as needed. For more information, refer to "Adding VRRP Service to a VRF" (Page 630).

## 13.2.3.2 Adding VRRP Service to a VRF

To add VRRP service to a VRF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » VRRP - VRF**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	<b>Synopsis:</b> A string between 1 and 32 characters long The VRF name.

4. Click **OK**. A dialog box appears.
5. Configure the following parameter(s) as required:

Parameter	Description
Enable VRRP Service for VRF	Enables or disables the VRRP service.

Parameter	Description
Route ID	<b>Synopsis:</b> A string The router ID for VRRP logs.

6. Commit the change.

### 13.2.3.3 Deleting VRRP Service from a VRF

To delete VRRP service from a VRF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » VRRP - VRF**.
2. Select the VRRP for VRF to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 13.2.4 Managing VRRP Trackers for a VRF

VRRP trackers monitor the state/condition of a route. When the route is unavailable, VRRP will lower its priority or transition it to a fault state.

### Note

The decision to increase or decrease the priority of a route must be done in coordination with any backup VRRP Routers since the priority decides whether a router becomes a Master or a Backup. For example, if Router X's priority is 150 and Router Y's priority is 145, Router X's priority must be lowered by 6 to make it a Backup router.

### 13.2.4.1 Viewing a List of VRRP Trackers for a VRF

1. To view a list of VRRP trackers for a VRF, navigate to the **VRF** tab under **Layer 3 » Routing » VRF » VRRP - VRF**.
2. Select a VRF and then click the **Trackers** tab. If trackers have been configured, a list appears.

If no VRRP trackers have been configured, add trackers as needed. For more information, refer to "Adding a VRRP Tracker for a VRF" (Page 631).

### 13.2.4.2 Adding a VRRP Tracker for a VRF

To add a VRRP tracker for a VRF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, and then select a VRF.
2. Select the **Trackers** tab.

3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Tracker Name	<b>Synopsis:</b> A string between 1 and 64 characters long The name of the tracker.

5. Click **OK** to add the tracker.
6. Configure the following parameter(s) as required:

Parameter	Description
Tracker Type	<b>Synopsis:</b> [ route ] <b>Default:</b> route The type of condition for the tracker to check.
Network	<b>Synopsis:</b> A string between 9 and 18 characters long The network to track. The tracker checks for a route to this network in the routing table.
Interface	<b>Synopsis:</b> A string The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
Interval	<b>Synopsis:</b> An integer between 1 and 120 The number of seconds between tracker queries.
Weight	<b>Synopsis:</b> An integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the tracker falls. When positive, the priority increases by this amount when the tracker rises. When not set, the state changes to the fault state when the tracker falls.
Rise	<b>Synopsis:</b> An integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
Fall	<b>Synopsis:</b> An integer between 1 and 65535 The number of unsuccessful tracker queries before changing the router priority.

7. Commit the changes.

### 13.2.4.3 Deleting a VRRP Tracker for a VRF

To delete a VRRP tracker for a VRF, do the following:

1. Navigate to the **VRF** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, and then select a VRF.
2. Select the **Trackers** tab.
3. Select the tracker to be deleted, and then click **Delete Entry**.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Commit the change.

## 13.2.5 Managing VRRP Groups for a VRF

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

### 13.2.5.1 Viewing a List of VRRP Groups for a VRF

1. To view a list of VRRP groups for a VRF, navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Select the **Groups** tab. If groups have been configured, a list appears.

If no VRRP groups have been configured, add groups as needed. For more information, refer to "Adding a VRRP Group" (Page 618).

### 13.2.5.2 Adding a VRRP Group for a VRF

To add a VRRP group for a VRF, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Select the **Groups** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Group Name	<b>Synopsis:</b> A string between 1 and 64 characters long The VRRP group name.

5. Click **OK** to add the group.
6. Commit the change.

### 13.2.5.3 Deleting a VRRP Group

To delete a VRRP group, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Select the **Groups** tab.
3. Select the group to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 13.2.6 Managing VRRP Instances for a VRF

VRRP instances can be configured for one or more VRF definitions. This is done by enabling VRRP for a VRF and then configuring the required VRRP parameters.

### 13.2.6.1 Viewing a List of VRRP Instances for a VRF

1. To view a list of VRRP instances defined for a VRF, navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Select the **Instance** tab. If instances have been configured, a list appears.

If no instances have been configured for a VRF, add instances as needed. For more information, refer to "Adding a VRRP Instance for a VRF" (Page 634).

### 13.2.6.2 Adding a VRRP Instance for a VRF

To add a VRRP instance for a VRF, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Select the **Instance** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Instance Name	<b>Synopsis:</b> A string between 1 and 64 characters long The name of the VRRP instance - the name must not include spaces.

5. Click **OK** to add the instance.
6. Configure the following parameters for the instance:

**⚠ NOTICE**

When **Use Virtual Mac** is enabled, an additional firewall interface `vrrp`. `{ VRID }` is required, where `{ VRID }` is the name of the virtual router identifier. For more information about adding a firewall interface, refer to "Adding an Interface" (Page 205).

Parameter	Description
VRRP Version	<b>Synopsis:</b> An integer between 2 and 3 <b>Default:</b> 2 Configure VRRP version for this instance.
Interface	<b>Synopsis:</b> A string The interface used by the VRRP service to communicate with other VRRP-enabled routers using the VRRP protocol. Additionally, this interface hosts the Virtual IP (VRIP) when the 'Use Virtual MAC' parameter is not enabled.
Virtual Router ID	<b>Synopsis:</b> An integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID.
Priority	<b>Synopsis:</b> An integer between 0 and 255 The priority for the VRRP instance. When electing the master, the highest priority wins. The configurable range is 1 to 255. A value of zero (0) is invalid.
Advertisement Interval	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1 VRRP2 advertisement interval, in seconds.
advert-interval-mil lisecond	<b>Synopsis:</b> An integer between 20 and 3000 <b>Default:</b> 1000 VRRP3 advertisement interval in millisecond, must be multiple of 10.
Gratuitous ARP Delay	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 5 Gratuitous ARP delay, in seconds. Sets the delay after the router changes state state before a second set of gratuitous ARPs are sent.
No Preempt	When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
Preempt Delay	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0 The time, in seconds, after startup until preemption.

Parameter	Description
Fault to Master Delay	<p><b>Synopsis:</b> An integer between 0 and 1000</p> <p><b>Default:</b> 0</p> <p>The delay, in seconds, before a transition from the fault state to the master state occurs, thereby preempting the current master.</p>
Use Virtual MAC	When enabled, the router uses a virtual MAC address for the Virtual IP (VRIP).
VRRP Group	<p><b>Synopsis:</b> A string between 1 and 64 characters long</p> <p>Binds this VRRP instance to a VRRP group.</p>

7. Commit the changes.

### 13.2.6.3 Deleting a VRRP Instance for a VRF

To delete a VRRP instance for a VRF, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Select the **Instance** tab.
3. Select the VRRP instance to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 13.2.7 Managing VRRP Monitors for a VRF

A VRRP monitor selects an extra interface to monitor. If the interface becomes unavailable, the router will relinquish control of the gateway IP address to another VRRP Router.

### 13.2.7.1 Viewing a List of VRRP Monitors for a VRF

1. To view a list of VRRP monitors for a VRF, navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
  2. Click the **Instance** tab, and then select an instance.
  3. Select the **Monitor** tab. If monitors have been configured, a list appears.
- If no monitors have been configured, add monitors as needed. For more information, refer to "Adding a VRRP Monitor to a VRF" (Page 637).

### 13.2.7.2 Adding a VRRP Monitor to a VRF

To add a VRRP monitor to a VRF, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **Monitor** tab.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
Extra Interface to Monitor	<b>Synopsis:</b> A string The name of the interface.

6. Click **OK** to add the monitor.
7. Configure the following parameter(s) as required:

Parameter	Description
Weight	<b>Synopsis:</b> An integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the interface fails. When positive, the priority increases by this amount when the interface is up. When not set, the state changes to the fault state when the interface fails.

8. Commit the changes.

### 13.2.7.3 Deleting a VRRP Monitor from a VRF

To delete a VRRP monitor, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **Monitor** tab.
4. Select the monitored interface to be deleted, and then click **Delete Entry**.
5. Commit the change.

## 13.2.8 Managing VRRP Track Scripts for a VRF

Track scripts are used to associate VRRP trackers with VRRP instances.



**13.2.8.1 Viewing a List of VRRP Track Scripts for a VRF**

1. To view a list of track scripts, navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **Track Script** tab. If track scripts have been configured, a list appears.

If no track scripts have been configured, add track scripts as needed. For more information, refer to "Adding a VRRP Track Script to a VRF" (Page 638).

**13.2.8.2 Adding a VRRP Track Script to a VRF**

To add a track script, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **Track Script** tab.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
Tracker	<b>Synopsis:</b> A string between 1 and 64 characters long Select a tracker to monitor VRRP instance.

6. Click **OK** to add the track script.
7. Configure the following parameter(s) as required:

Parameter	Description
weight	<b>Synopsis:</b> An integer between -254 and 254 This setting overwrites the weight setting in the tracker. If negative, the priority decreases by this amount when the tracker falls. If positive, the priority increases by this amount when the tracker rises. If not set, the weight value in the tracker will be used.

8. Commit the changes.

**13.2.8.3 Deleting a VRRP Track Script from a VRF**

To delete a track script, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.

3. Select the **Track Script** tab.
4. Select the tracker name to be deleted, and then click **Delete Entry**.
5. Commit the changes.

## 13.2.9 Managing Virtual IP Addresses for a VRF

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

### Note

A VRRP packet will be ignored if any virtual IP address listed in the packet is not defined on the device. A syslog message is added for every 20 ignored VRRP packets.

### 13.2.9.1 Viewing a List of Virtual IP Addresses

1. To view a list of virtual IP addresses, navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **VRIP** tab. If VRIPs have been configured, a list appears.

If no virtual IP addresses have been configured, add addresses as needed. For more information, refer to "Adding a Virtual IP Address to a VRF" (Page 639).

### 13.2.9.2 Adding a Virtual IP Address to a VRF

#### NOTICE

At least one virtual IP address is required for each configured VRF instance.

To add a virtual IP address to a VRF, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **VRIP** tab.
4. Click **Add Entry**.
5. Configure the following parameter(s) as required:

Parameter	Description
Virtual IP Address/Netmask	<b>Synopsis:</b> A string between 9 and 18 characters long The virtual IP address/netmask.

6. Click **OK** to add the virtual IP address.
7. Commit the change.

### 13.2.9.3 Deleting a Virtual IP Address from a VRF

To delete a virtual IP address from a VRF, do the following:

1. Navigate to the **VRF - { name }** tab under **Layer 3 » Routing » VRF » VRRP - VRF**, where { name } is the name of the VRF.
2. Click the **Instance** tab, and then select an instance.
3. Select the **VRIP** tab.
4. Select the address to be deleted, and then click **Delete Entry**.
5. Commit the change.

### 13.2.10 Example: Configuring VRRP within a VRF

This example demonstrates how to configure VRRP within a VRF instance.

The following topology depicts a scenario where a PC/host is attempting to send a packet to a destination via a default gateway (VRIP) owned by the VRRP routers. If the Master router (R1) fails, a backup router (R2) is elected Master and acts as the gateway. The previous Master then transitions to a fault state or becomes a backup.

#### NOTICE

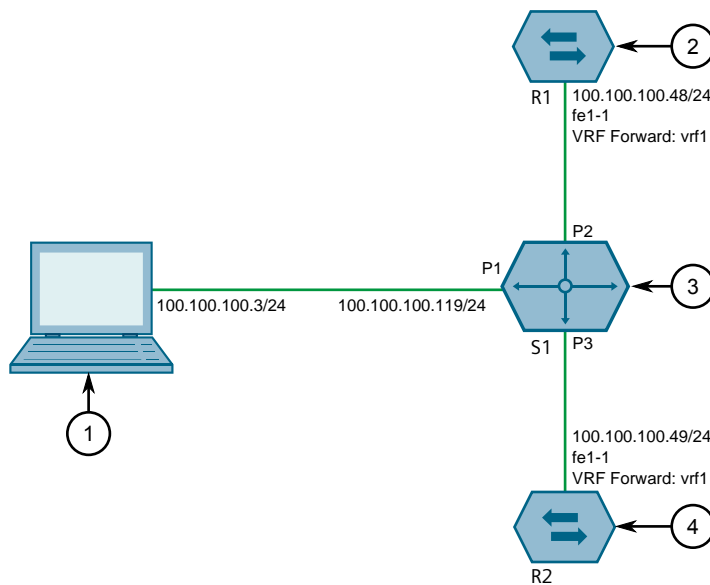
RUGGEDCOM ROX II supports VRRP within VRF for IPv4 addresses only.

#### NOTICE

Connection synchronization is not supported for VRRPs within a VRF. For more information about connection synchronization, refer to "Connection Synchronization" (Page 615).

#### NOTICE

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① PC
- ② Router R1
- ③ Layer 2 Switch S1
- ④ Router R2

Figure 13.4 Topology – VRRP within a VRF

To configure the devices per the topology, do the following:

1. Configure switch S1:

#### Note

The device may be a RUGGEDCOM ROX II device acting as Layer 2 switch, a RUGGEDCOM ROS device, or a third party Layer 2 device.

- a. Add VLAN 100. For more information, refer to "Adding a Static VLAN" (Page 321).
  - b. Assign IP address *100.100.100.119* to VLAN 100. For more information, refer to "Adding an IPv4 Address" (Page 225).
  - c. Assign VLAN 100 to ports 1, 2 and 3. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276).
2. Connect port 1 of switch S1 to a PC.
  3. Connect port 2 of switch S1 to router R1.
  4. Connect port 3 of switch S1 to router R2.
  5. Configure router R1:
    - a. Configure a VRF definition for *vrf1* with a route distinguisher of **100:1**. For more information, refer to "Adding a VRF Definition" (Page 562).
    - b. Define a route target for *vrf1* of type **both** with the export community set to **100:1**. For more information, refer to "Adding a Route Target" (Page 563).

- c. Make sure interface fe-1-1 is configured with the IP address 100.100.100.48/24.
- d. Assign the interfaces in step 5c (Page 642) to forward traffic to vrf1. For more information, refer to "Configuring a VRF Interface" (Page 560).
- e. Enable VRRP Service for VRF. For more information, refer to "Adding VRRP Service to a VRF" (Page 630).
- f. Configure a VRF instance with the following parameters:

Interface	Virtual Router ID	Priority
fe-1-1	101	150

For more information, refer to "Adding a VRRP Instance for a VRF" (Page 634).

- g. Add virtual IP address 100.100.100.101/24 to the VRF. For more information, refer to "Adding a Virtual IP Address to a VRF" (Page 639).
6. Configure router R2:
- a. Configure a VRF definition for vrf1 with a route distinguisher of **100:1**. For more information, refer to "Adding a VRF Definition" (Page 562).
  - b. Define a route target for vrf1 of type **both** with the export community set to **100:1**. For more information, refer to "Adding a Route Target" (Page 563).
  - c. Make sure interface fe-1-1 is configured with the IP address 100.100.100.49/24.
  - d. Assign the interfaces in step 6c (Page 642) to forward traffic to vrf1. For more information, refer to "Configuring a VRF Interface" (Page 560).
  - e. Enable VRRP Service for VRF. For more information, refer to "Adding VRRP Service to a VRF" (Page 630).
  - f. Configure a VRF instance with the following parameters:

Interface	VRID	Priority
fe-1-1	101	130

For more information, refer to "Adding a VRRP Instance for a VRF" (Page 634).

- g. Add virtual IP address 100.100.100.101/24 to the VRF. For more information, refer to "Adding a Virtual IP Address to a VRF" (Page 639).

### Verification

To verify the configuration, from the PC ping VRIP 100.100.100.101/24. If the configuration is successful the Master will respond.

### Final Configuration Example

The following configurations reflect the topology:

```

R1# show services vrrp vrf vrf1 status
-----
NAME          STATE    PRIORITY  TIME CHANGE          INTERFACE          MONITOR
              STATE    STATE     STATE                STATE              INTERFACE
              STATE    STATE     STATE                STATE              STATE
-----
vrf-ins1     master  150       Fri Jan 25 13:43:52 2019  fe-1-1 is Up
R2# show services vrrp vrf vrf1 status
-----
NAME          STATE    PRIORITY  TIME CHANGE          INTERFACE          MONITOR
              STATE    STATE     STATE                STATE              INTERFACE
              STATE    STATE     STATE                STATE              STATE
-----
vrf-ins1     backup  130       Fri Jan 25 13:43:52 2019  fe-1-1 is Up

```

## 13.3 Managing Link Failover Protection

Link failover provides an easily configurable means of raising a backup link upon the failure of a designated main link. The main and backup links can only be Ethernet.

Link failover can back up to multiple remote locations, managing multiple main-to-backup link relationships.

Link failover can also be used to migrate the default route from the main link to the backup link.

The time after a main link failure to backup link startup, and the time after a main link recovery to backup link stoppage, are configurable. The link failover function also provides failover status information and a test of the failover settings.

### 13.3.1 Viewing the Link Failover Log

To view the link failover log, do the following:

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Status** tab.
3. Under **View Logs**, click **Perform**.

### 13.3.2 Viewing the Link Failover Status

The Link Failover Status form displays the current link failover status. To view the link failover status, do the following:

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Status** tab.

This form provides the following information:

Parameter	Description
Main Link Status	<b>Synopsis:</b> A string The main link status.
Backup Link Status	<b>Synopsis:</b> A string The backup link status.
Main Ping Test	<b>Synopsis:</b> A string The results of pinging the target using the main interface.
Time of Last State Change	<b>Synopsis:</b> A string The time of the last state change.
Link Backup State	<b>Synopsis:</b> A string The backup link state.
Backup Interface In Use	<b>Synopsis:</b> A string The name of the backup interface that is being used.

### 13.3.3 Managing Link Failover Parameters

This section describes how to manage parameter settings for link failover.

#### 13.3.3.1 Viewing a List of Link Failover Parameters

To view a list of link failover parameters, navigate to the **Configurations** tab under **Layer 3 » Link Failover**. If parameters have been configured, a list appears.

If no parameters have been configured, add parameters as needed. For more information, refer to "Adding a Link Failover Parameter" (Page 644).

#### 13.3.3.2 Adding a Link Failover Parameter

To add a link failover parameter, do the following:

---

##### Note

The link failover feature can only be configured on a routable interface. For the link failover feature to be used on a switched port, another VLAN must be configured (for example, switch.0002) to logically differentiate the switched port from the default PVID VLAN 1 (switch.0001).

---

1. Navigate to the **Configurations** tab under **Layer 3 » Link Failover**.
2. Click **Add Entry**, and then select the main interface from the list.
3. Click **OK** to add the main interface.

4. Configure the following parameter(s) as required:

Parameter	Description
Enabled	Enables this link backup.
Ping Timeout	<b>Synopsis:</b> An integer between 1 and 65536 <b>Default:</b> 2 The time interval, in seconds, before immediately retrying a ping.
Ping Interval	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 60 The time interval, in seconds, between ping tests.
Ping Retry	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 3 The number of ping retries before constructing a path failure.
Start Delay	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 180 The delay time, in seconds, when first starting link failover.
Main Down Timeout	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 60 The delay time, in seconds, that the main trunk is down before starting the backup trunk.
Main Up Timeout	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 60 The delay time, in seconds, to confirm that the main trunk is up (returned to service) before stopping the backup trunk.

5. Commit the change.

### 13.3.3.3 Deleting a Link Failover Parameter

To delete a link failover parameter, do the following:

1. Navigate to the **Configurations** tab under **Layer 3 » Link Failover**.
2. Select the parameter to be deleted, and then click **Delete Entry**.
3. Commit the change.



### 13.3.4 Managing Link Failover Backup Interfaces

A backup interface is the interface to which link failover switches when the main interface is determined to be down. You can add up to three backup interfaces to each link failover configuration.

#### 13.3.4.1 Viewing a List of Link Failover Backup Interfaces

1. To view a list of link failover backup interfaces, navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Backup** tab. If backup interfaces have been configured, a list appears. If no backup interfaces have been configured, add backup interfaces as needed. For more information, refer to "Adding a Link Failover Backup Interface" (Page 646).

#### 13.3.4.2 Adding a Link Failover Backup Interface

To set a link failover backup interface, do the following:

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Backup** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Backup If	<b>Synopsis:</b> A string The interface used to back up the main interface.

5. Click **OK** to add the backup interface.
6. Configure the following parameter(s) as required:

#### Note

Do not configure the **Backup Gateway** parameter for Point to Point (P2P) links.

#### Note

The **On Demand** parameter is set at the interface itself.

Parameter	Description
Priority	<b>Synopsis:</b> [ third   second   first ] <b>Default:</b> first The priority which is applied to the backup interface when switching.

Parameter	Description
Transfer Default Route	The transfer default gateway on the switching main and backup interface. The default route on the device must have a <b>distance</b> greater than one.
Backup Gateway	<b>Synopsis:</b> A string up to 15 characters long The IP address of the backup gateway.
On Demand	<b>Synopsis:</b> [ true   false ] Displays the status of the interface's On-demand option. When enabled, link failover can set the interface to up or down as needed. The interface is down until needed by link failover. When disabled, link failover cannot set the interface to up or down. By default, the interface is always up.

7. Commit the changes.

### 13.3.4.3 Deleting a Link Failover Backup Interface

To delete a link failover backup interface, do the following:

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Backup** tab.
3. Select the backup interface to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 13.3.5 Managing Link Failover Ping Targets

A link failover ping target is an IP address that link failover pings to determine if the main link is down. The address can be a dedicated host or a dummy address on a router. Up to three link failover ping targets can be added to each link failover configuration.

### 13.3.5.1 Viewing a List of Link Failover Ping Targets

1. To view a list of link failover ping targets, navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Target** tab. If target host IPs have been configured, a list appears.

If no ping targets have been configured, add targets as needed. For more information, refer to "Adding a Link Failover Ping Target" (Page 648).

### 13.3.5.2 Adding a Link Failover Ping Target

To add a link failover ping target, do the following:

#### Note

Link failover pings each target separately. If all targets are down, the main link is considered to be down and it fails over to the backup interface. Backup links are used in the order of their Priority setting (first, second, and then third), always starting with the first priority interface. When a higher-priority interface becomes available again, the system reverts to the higher priority interface. For example, if the second priority interface is active, the system switches back to the first priority interface when the first priority interface becomes available again.

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Target** tab.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
Host IP	<b>Synopsis:</b> A string between 7 and 15 characters long The IP address of the target host to verify the main path.

5. Commit the change.

### 13.3.5.3 Deleting a Link Failover Ping target

To delete a link failover ping target, do the following:

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Target** tab.
3. Select the ping target to be deleted, and then click **Delete Entry**.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Commit the change.

## 13.3.6 Testing Link Failover

The link failover settings can be tested to confirm that each link failover configuration works properly. To launch the test, specify for how long the system should operate on the backup interface, and for how long the system should delay before starting the test. Canceling the test returns the interfaces to their pre-test condition.

While the test is running, monitor the status of the test to observe the main and backup link status, ping test results, state change, backup state, and backup interface information. As the test progresses, this information changes as link failover switches from the main interface to the backup interface. For more information on the **Link Fail Over Status** form, refer to "Viewing the Link Failover Status" (Page 643).

To launch a link failover test, do the following:

---

#### Note

The link failover test can be canceled at any time. For more information about canceling a link failover test, refer to "Canceling a Link Failover Test" (Page 649).

Canceling the test returns the interfaces to their pre-test condition.

---

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Status** tab.
3. Under **Start Link Failover Test**, click **Perform**.
4. Configure the following parameter(s) as required:

Parameter	Description
Test Duration	<p><b>Synopsis:</b> An integer between 1 and 65536</p> <p><b>Default:</b> 5</p> <p>The amount of time (in minutes) to run before restoring service to the main trunk.</p>
Start Test Delay	<p><b>Synopsis:</b> An integer between 1 and 65536</p> <p><b>Default:</b> 1</p> <p>The amount of waiting time (in minutes) before running the test.</p>

5. Click **OK** to begin the test.

### 13.3.7 Canceling a Link Failover Test

To cancel a link failover test, do the following:

1. Navigate to the **Configurations - { interface }** tab under **Layer 3 » Link Failover**, where { interface } is the name of the interface.
2. Select the **Status** tab.
3. Under **Cancel Link Failover Test**, click **Perform**.

## 13.4 Managing Spanning Tree Protocol

This section describes how to manage the Spanning Tree Protocol (STP).

## 13.4.1 RSTP Operation

The IEEE 802.1D Spanning Tree Protocol (STP) was developed to enable the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer halt after a link outage until all bridges in the network are guaranteed to be aware of the new topology. Using the values recommended by IEEE 802.1D, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (RSTP), first introduced by IEEE 802.1w and significantly improved in IEEE 802.1D-2004, was a further evolution of the IEEE 802.1D Spanning Tree Protocol. It replaced the settling period with an active handshake between bridges that guarantees the rapid propagation of topology information throughout the network.

### 13.4.1.1 RSTP States and Roles

RSTP bridges have roles to play, either root or designated. One bridge – the Root Bridge – is the logical center of the network. All other bridges in the network are Designated bridges. RSTP also assigns each port of the bridge a state and a role. The RSTP state describes what is happening at the port in relation to address learning and frame forwarding. The RSTP role basically describes whether the port is facing the center or the edges of the network and whether it can currently be used.

#### State

There are three RSTP states: Discarding, Learning and Forwarding.

The discarding state is entered when the port is first put into service. The port does not learn addresses in this state and does not participate in frame transfer. The port looks for RSTP traffic in order to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to learning.

The learning state is entered when the port is preparing to play an active part in the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP bridges, the time spent in this state is usually quite short. RSTP bridges operating in STP compatibility mode will spend six to 40 seconds in this state.

After *learning*, the bridge will place the port in the forwarding state. The port both learns addresses and participates in frame transfer while in this state.

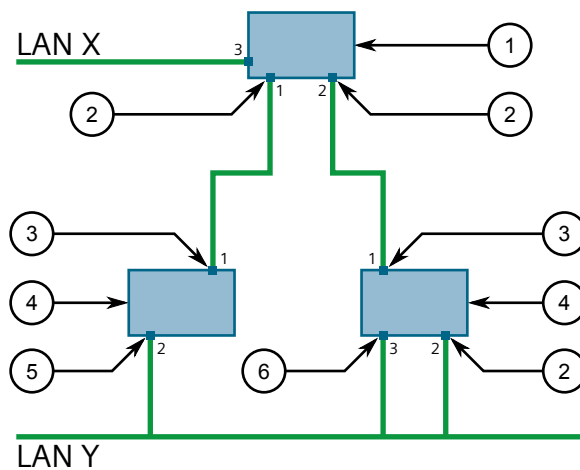
 <b>NOTICE</b>
---

Purely for purposes of management, RUGGEDCOM ROX II introduces two more states: <i>Disabled</i> and <i>Link Down</i> . The <i>Disabled</i> state refers to links for which RSTP has been disabled. The <i>Link Down</i> state refers to links for which RSTP is enabled but are currently down.
---

## Role

There are four RSTP port roles: Root, Designated, Alternate and Backup. If the bridge is not the root bridge, it must have a single Root Port. The Root Port is the “best” (i.e. quickest) way to send traffic to the root bridge.

A port is marked as Designated if it is the best port to serve the LAN segment it is connected to. All bridges on the same LAN segment listen to each other's messages and agree on which bridge is the Designated Bridge. The ports of other bridges on the segment must become either Root, Alternate or Backup ports.



- ① Root Bridge
- ② Designated Bridge
- ③ Designated Port
- ④ Root Port
- ⑤ Alternate Port
- ⑥ Backup Port

Figure 13.5 Bridge and Port Roles

A port is alternate when it receives a better message from another bridge on the LAN segment it is connected to. The message that an Alternate Port receives is better than the port itself would generate, but not good enough to convince it to become the Root Port. The port becomes the alternate to the current Root Port and will become the new Root Port should the current Root Port fail. The Alternate Port does not participate in the network.

A port is a Backup Port when it receives a better message from the LAN segment it is connected to, originating from another port on the same bridge. The port is a backup for another port on the bridge and will become active if that port fails. The Backup Port does not participate in the network.

### 13.4.1.2 Edge Ports

A port may be designated as an Edge Port if it is directly connected to an end station. As such, it cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages.

Edge ports that receive configuration messages immediately lose their Edge Port status and become normal spanning tree ports. A loop created on an improperly connected edge port is thus quickly repaired.

Because an Edge Port services only end stations, topology change messages are not generated when its link toggles.

### 13.4.1.3 Point-to-Point and Multipoint Links

RSTP uses a peer-peer protocol called Proposing-Agreeing to ensure transitioning in the event of a link failure. This protocol is point-to-point and breaks down in multipoint situations, i.e. when more than two bridges operate on a shared media link.

If RSTP detects this circumstance (based upon the port's half duplex state after link up) it will switch off Proposing-Agreeing. The port must transition through the learning and forwarding states, spending one forward delay in each state.

There are circumstances in which RSTP will make an incorrect decision about the point-to-point state of the link simply by examining the half-duplex status, namely:

- The port attaches only to a single partner, but through a half-duplex link.
- The port attaches to a shared media hub through a full-duplex link. The shared media link attaches to more than one RSTP enabled bridge.

In such cases, the user may configure the bridge to override the half-duplex determination mechanism and force the link to be treated in the proper fashion.

### 13.4.1.4 Path and Port Costs

The STP path cost is the main metric by which root and designated ports are chosen. The path cost for a designated bridge is the sum of the individual port costs of the links between the root bridge and that designated bridge. The port with the lowest path cost is the best route to the root bridge and is chosen as the root port.

---

#### Note

In actuality the primary determinant for root port selection is the root bridge ID. Bridge ID is important mainly at network startup when the bridge with the lowest ID is elected as the root bridge. After startup (when all bridges agree on the root bridge's ID) the path cost is used to select root ports. If the path costs of candidates for the root port are the same, the ID of the peer bridge is used to select the port. Finally, if candidate root ports have the same path cost and peer bridge ID, the port

ID of the peer bridge is used to select the root port. In all cases the lower ID, path cost or port ID is selected as the best.

---

### How Port Costs Are Generated

Port costs can be generated either as a result of link auto-negotiation or manual configuration. When the link auto-negotiation method is used, the port cost is derived from the speed of the link. This method is useful when a well-connected network has been established. It can be used when the designer is not too concerned with the resultant topology as long as connectivity is assured.

Manual configuration is useful when the exact topology of the network must be predictable under all circumstances. The path cost can be used to establish the topology of the network exactly as the designer intends.

### STP vs. RSTP Costs

The STP specification limits port costs to values of 1 to 65536. Designed at a time when 9600 bps links were state of the art, this method breaks down in modern use, as the method cannot represent a link speed higher than 10 Gbit/s.

To remedy this problem in future applications, the RSTP specification limits port costs to values of 1 to 20000000, and a link speed up to 10 Tbit/s can be represented with a value of 2.

#### 13.4.1.5 Bridge Diameter

The bridge diameter is the maximum number of bridges between any two possible points of attachment of end stations to the network.

The bridge diameter reflects the realization that topology information requires time to propagate hop by hop through a network. If configuration messages take too long to propagate end to end through the network, the result will be an unstable network.

There is a relationship between the bridge diameter and the maximum age parameter.

---

#### Note

The RSTP algorithm is as follows:

- STP configuration messages contain *age* information.
  - Messages transmitted by the root bridge have an age of 0. As each subsequent designated bridge transmits the configuration message it must increase the age by at least 1 second.
  - When the age exceeds the value of the maximum age parameter the next bridge to receive the message immediately discards it.
-



To achieve extended ring sizes, Siemens's eRSTP™ uses an age increment of  $\frac{1}{4}$  of a second. The value of the maximum bridge diameter is thus four times the configured maximum age parameter.

 **NOTICE**

Raise the value of the maximum age parameter if implementing very large bridged networks or rings.

#### 13.4.1.6 eRSTP

Siemens's enhanced Rapid Spanning Tree Protocol (eRSTP) improves the performance of RSTP in two ways:

- Improves the fault recovery time performance (< 5 ms per hop)
- Improves performance for large ring network topologies (up to 160 switches)

eRSTP is also compatible with standard RSTP for interoperability with commercial switches.

For example, in a network comprised of 15 RUGGEDCOM hardened Ethernet switches in a ring topology, the expected fault recovery time would be less than 75 ms (i.e. 5 ms x 15). However, with eRSTP, the worst case fault recovery time is less than 26 ms.

#### 13.4.1.7 Fast Root Failover

Siemens's *Fast Root Failover* feature is an enhancement to RSTP that may be enabled or disabled. Fast Root Failover improves upon RSTP's handling of root bridge failures in mesh-connected networks, resulting in slightly increased failover times for some non-root bridge scenarios.

 **NOTICE**

In networks mixing RUGGEDCOM and non-RUGGEDCOM switches, or in those mixing Fast Root Failover algorithms, RSTP Fast Root Failover will not function properly and root bridge failure will result in an unpredictable failover time. To avoid potential issues, note the following:

- When using the Robust algorithm, all switches must be RUGGEDCOM switches
- When using the Relaxed algorithm, all switches must be RUGGEDCOM switches, with the exception of the root switch
- All RUGGEDCOM switches in the network must use the same Fast Root Failover algorithm

Two Fast Root Failover algorithms are available:

- **Robust** – Guarantees a deterministic root failover time, but requires support from all switches in the network, including the root switch

- **Relaxed** – Ensures a deterministic root failover time in most network configurations, but allows the use of a standard bridge in the root role

---

**Note**

The minimum interval for root failures is one second. Multiple, near simultaneous root failures (within less than one second of each other) are not supported by Fast Root Failover.

---

### Fast Root Failover and RSTP Performance

- Running RSTP with Fast Root Failover disabled has no impact on RSTP performance.
- Fast Root Failover has no effect on RSTP performance in the case of failures that do not involve the root bridge or one of its links.
- The extra processing introduced by Fast Root Failover significantly decreases the worst-case failover time in mesh networks, with a modest increase in the best-case failover time. The effect on failover time in ring-connected networks, however, is only to increase it.

### Recommendations On the Use of Fast Root Failover

- It is not recommended to enable Fast Root Failover in single ring network topologies
- It is strongly recommended to always connect the root bridge to each of its neighbor bridges using more than one link

## 13.4.2 RSTP Applications

This section describes various applications of RSTP.

### 13.4.2.1 RSTP in Structured Wiring Configurations

RSTP may be used to construct structured wiring systems where connectivity is maintained in the event of link failures. For example, a single link failure of any link between A and N in figure 13.6, "Example - Structured Wiring Configuration" (Page 656) would leave all the ports of bridges 555 through 888 connected to the network.

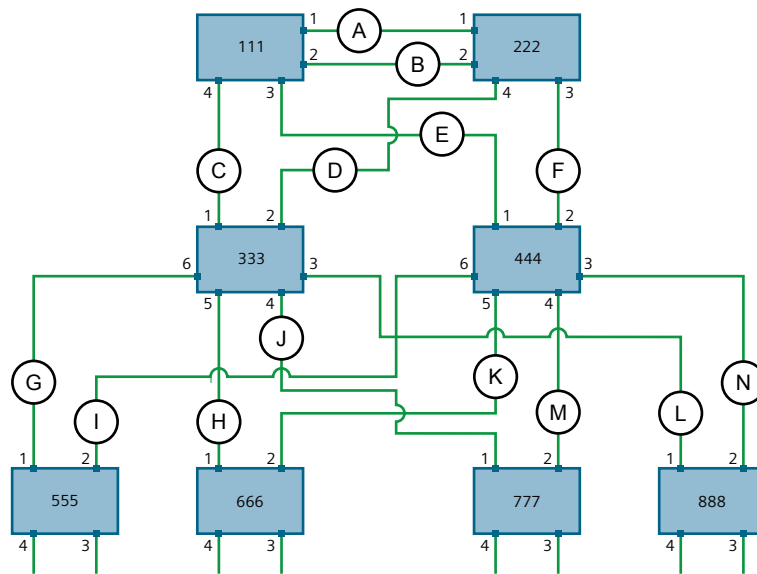


Figure 13.6 Example - Structured Wiring Configuration

To design a structured wiring configuration, do the following:

1. **Select the design parameters for the network.**

What are the requirements for robustness and network failover/recovery times? Are there any special requirements for diverse routing to a central host computer? Are there any special port redundancy requirements?

2. **Identify required legacy support.**

Are STP bridges used in the network? These bridges do not support rapid transitioning to forwarding. If these bridges are present, can they be re-deployed closer to the network edge?

3. **Identify edge ports and ports with half-duplex/shared media restrictions.**

Ports that connect to host computers, IEDs and controllers may be set to edge ports in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network. Ports with half-duplex/shared media restrictions require special attention in order to guarantee that they do not cause extended fail-over/recovery times.

4. **Choose the root bridge and backup root bridge carefully.**

The root bridge should be selected to be at the concentration point of network traffic. Locate the backup root bridge adjacent to the root bridge. One strategy that may be used is to tune the bridge priority to establish the root bridge and then tune each bridge's priority to correspond to its distance from the root bridge.

5. **Identify desired steady state topology.**

Identify the desired steady state topology taking into account link speeds, offered traffic and QOS. Examine the effects of breaking selected links, taking into account network loading and the quality of alternate links.

6. **Decide upon a port cost calculation strategy.**

Select whether fixed or auto-negotiated costs should be used? It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style. Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.

7. **Enable RSTP Fast Root Failover option.**

This is a proprietary feature of Siemens. In a mesh network with only RUGGEDCOM devices in the core of the network, it is recommended to enable the RSTP Fast Root Failover option to minimize the network downtime in the event of a Root bridge failure.

8. Calculate and configure priorities and costs.

9. Implement the network and test under load.

13.4.2.2 RSTP in Ring Backbone Configurations

RSTP may be used in ring backbone configurations where rapid recovery from link failure is required. In normal operation, RSTP will block traffic on one of the links. For an example, refer to link H in figure 13.7, "Example - Ring Backbone Configuration" (Page 657). In the event of a failure on link D, bridge 444 will unblock link H and bridge 333 will communicate with the network through link F.

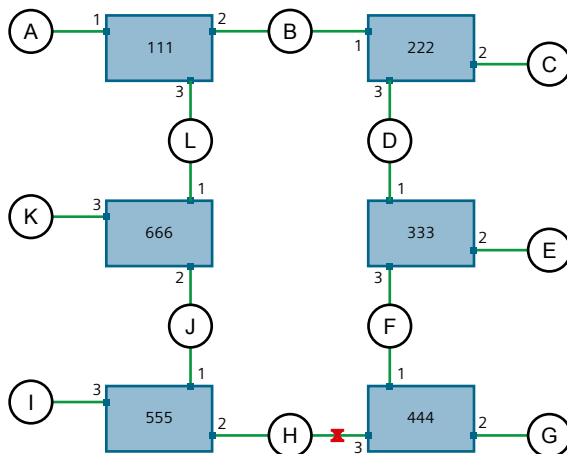


Figure 13.7 Example - Ring Backbone Configuration

To design a ring backbone configuration with RSTP, do the following:

1. **Select the design parameters for the network.**

What are the requirements for robustness and network fail-over/recovery times? Typically, ring backbones are chosen to provide cost effective but robust network designs.

2. **Identify required legacy support and ports with half-duplex/shared media restrictions.**

These bridges should not be used if network fail-over/recovery times are to be minimized.

3. **Identify edge ports.**

Ports that connect to host computers, IEDs and controllers may be set to edge ports in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network.

4. **Choose the root bridge.**

The root bridge can be selected to equalize either the number of bridges, number of stations or amount of traffic on either of its legs. It is important to realize that the ring will always be broken in one spot and that traffic always flows through the root.

5. **Assign bridge priorities to the ring.**

For more information, refer to the RUGGEDCOM White Paper "[Performance of the Rapid Spanning Tree Protocol in Ring Network Topology \[https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf\]](https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf)".

6. **Decide upon a port cost calculation strategy.**

It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style. Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.

7. **Disable RSTP Fast Root Failover option.**

This is a proprietary feature of Siemens. In RUGGEDCOM ROX II, the RSTP Fast Root Failover option is enabled by default. It is recommended to disable this feature when operating in a Ring network.

8. Implement the network and test under load.

### 13.4.2.3 RSTP Port Redundancy

In cases where port redundancy is essential, RSTP allows more than one bridge port to service a LAN. In the following example, if port 3 is designated to carry the network traffic of LAN A, port 4 will block traffic. Should an interface failure occur on port 3, port 4 will assume control of the LAN.

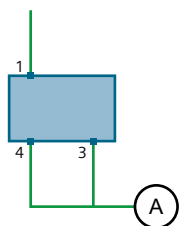


Figure 13.8 Example - Port Redundancy

### 13.4.3 MSTP Operation

The Multiple Spanning Tree (MST) algorithm and protocol provide greater control and flexibility than RSTP and legacy STP. MSTP (Multiple Spanning Tree Protocol) is an extension of RSTP, whereby multiple spanning trees may be maintained on the same bridged network. Data traffic is allocated to one or several spanning trees by mapping one or more VLANs to different Multiple Spanning Tree Instances (MSTIs).

The sophistication and utility of the MSTP implementation on a given bridged network is proportional to the amount of planning and design invested in configuring MSTP.

If MSTP is activated on some or all of the bridges in a network with no additional configuration, the result will be a fully and simply connected network. At best though, the result will be the same as a network using only RSTP. Taking full advantage of the features offered by MSTP requires a potentially large number of configuration variables to be derived from an analysis of data traffic on the bridged network, and from requirements for load sharing, redundancy, and path optimization. Once these parameters have all been derived, it is also critical they are consistently applied and managed across all bridges in an MST region.

By design, MSTP processing time is proportional to the number of active STP instances. This means MSTP will likely be significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

#### 13.4.3.1 MSTP Regions and Interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of inter-operating with bridges that support only RSTP or legacy STP, without requiring any special configuration.

An MST region may be defined as the set of interconnected bridges whose MST Region Identification is identical. The interface between MSTP bridges and non-MSTP bridges, or between MSTP bridges with different MST Region Identification information, becomes part of an MST Region boundary.

Bridges outside an MST region will see the entire region as though it were a single (R)STP bridge, with the internal detail of the MST region being hidden from the rest of the bridged network. In support of this, MSTP maintains separate *hop counters* for spanning tree information exchanged at the MST region boundary versus information propagated inside the region. For information received at the MST region boundary, the (R)STP Message Age is incremented only once. Inside the region, a separate Remaining Hop Count is maintained, one for each spanning tree instance. The external Message Age parameter is referred to the (R)STP Maximum Age Time, whereas the internal Remaining Hop Counts are compared to an MST region-wide Maximum Hops parameter.

**MSTI**

An MSTI (Multiple Spanning Tree Instance) is one of sixteen independent spanning tree instances that may be defined in an MST region (not including the IST). An MSTI is created by mapping a set of VLANs to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN-to-MSTI mappings must be identical for all bridges in an MST region.

RUGGEDCOM ROX II supports 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of others. Data traffic originating from the same source and bound to the same destination, but on different VLANs on different MSTIs, may therefore travel a different path across the network.

**IST**

An MST region always defines an IST (Internal Spanning Tree). The IST spans the entire MST region, and carries all data traffic that is not specifically allocated (by VLAN) to a specific MSTI. The IST is always computed and is defined to be MSTI zero.

The IST is also the extension inside the MST region of the CIST

**CST**

The CST (Common Spanning Tree) spans the entire bridged network, including MST regions and any connected STP or RSTP bridges. An MST region is seen by the CST as an individual bridge, with a single cost associated with its traversal.

**CIST**

The CIST (Common and Internal Spanning Tree) is the union of the CST and the ISTs in all MST regions. The CIST therefore spans the entire bridged network, reaching into each MST region via the latter's IST to reach every bridge on the network.

**13.4.3.2 MSTP Bridge and Port Roles**

MSTP supports the following bridge and port roles:

**Bridge Roles**

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.

Role	Description
MSTI Regional Root	The root bridge for an MSTI within an MSTP region. A root bridge is independently elected for each MSTI in an MSTP region.

## Port Roles

Each port on an MSTP bridge may have more than one CIST role depending on the number and topology of spanning tree instances defined on the port.

Role	Description
CIST Port Roles	<ul style="list-style-type: none"> <li>• The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region.</li> <li>• A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root.</li> <li>• Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.</li> </ul>
MSTI Port Roles	<p>For each MSTI on a bridge:</p> <ul style="list-style-type: none"> <li>• The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root.</li> <li>• A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root.</li> <li>• Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root.</li> </ul> <p>The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.</p>
Boundary Ports	<p>A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike.</p> <p>A Boundary Port may be:</p> <ul style="list-style-type: none"> <li>• The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port).</li> <li>• A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role.</li> </ul> <p>A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.</p>

### 13.4.3.3 Benefits of MSTP

MSTP is configured by default to arrive automatically at a spanning tree solution for each configured MSTI. However, advantages may be gained from influencing the



topology of MSTIs in an MST region by way of the Bridge Priority and the cost of each port.

#### Load Balancing

MSTP can be used to balance the data traffic load among sets of VLANs, enabling more complete utilization of a bridged network that has multiple redundant interconnections between bridges.

A bridged network controlled by a single spanning tree will block redundant links by design to avoid harmful loops. However, when using MSTP, any given link may have a different blocking state for MSTI, as maintained by MSTP. Any given link, therefore, might be in blocking state for some VLANs, and in forwarding state for other VLANs, depending on the mapping of VLANs to MSTIs.

It is possible to control the spanning tree solution for each MSTI, especially the set of active links for each tree, by manipulating per MSTI the bridge priority and the port costs of links in the network. If traffic is allocated judiciously to multiple VLANs, redundant interconnections in a bridged network, which would have gone unused when using a single spanning tree, can now be made to carry traffic.

#### Isolation of Spanning Tree Reconfiguration

A link failure in an MSTP region that does not affect the roles of Boundary ports will not cause the CST to be reconfigured, nor will the change affect other MSTP regions. This is due to the fact that MSTP information does not propagate past a region boundary.

#### MSTP versus PVST

An advantage of MSTP over the Cisco Systems Inc. proprietary Per-VLAN Spanning Tree (PVST) protocol is the ability to map multiple VLANs onto a single MSTI. Since each spanning tree requires processing and memory, the expense of keeping track of an increasing number of VLANs increases much more rapidly for PVST than for MSTP.

#### Compatibility with STP and RSTP

No special configuration is required for the bridges of an MST region to connect fully and simply to non-MST bridges on the same bridged network. Careful planning and configuration is, however, recommended to arrive at an optimal network design.

#### 13.4.3.4 Implementing MSTP on a Bridged Network

The following procedure is recommended for configuring MSTP on a network. Beginning with a set of MSTP-capable Ethernet bridges, do the following for each bridge on the network:

---

**Note**

Careful network analysis and planning should inform each step of creating an MSTP network.

---

**Note**

MSTP does not need to be enabled to map a VLAN to an MSTI. However, the mapping must be identical for each bridge that belongs to the MSTP region.

---

1. Disable STP. For more information, refer to "Configuring STP Globally" (Page 663).
2. Configure one or more Multiple Spanning Tree Instances (MSTI), each with a unique bridge priority. For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 670).
3. Create static VLANs and map them to the MSTIs. For more information, refer to "Adding a Static VLAN" (Page 321).
4. Configure individual MSTI for each switched Ethernet port and/or Ethernet trunk interface that will transmit/receive MST BPDU (Bridge Protocol Data Unit) traffic. For more information, refer to "Managing Multiple Spanning Tree Instances Per-Port" (Page 671).
5. Set the STP protocol version to MSTP, configure the MST region identifier and revision level, and then enable STP. For more information, refer to "Configuring STP Globally" (Page 663).

#### 13.4.4 Configuring STP Globally

To configure global settings for the Spanning Tree Protocol (STP), do the following:

---

**Note**

If necessary, Multiple Spanning Tree Instances (MSTI) can be added. For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 670).

---

#### Basic STP Settings

Configure the basic STP settings as follows:

1. Navigate to the **Spanning Tree Global** tab under **Layer 2 » Spanning Tree**.
2. Configure the following parameters as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables STP/RSTP/MSTP for the bridge globally. Note that STP/RSTP/MSTP is enabled on a port when it is enabled globally and along with enabling per port setting.</p>
STP Protocol Version	<p><b>Synopsis:</b> [ stp   rstp   mstp ]</p> <p><b>Default:</b> rstp</p> <p>The version (either only STP or Rapid STP or Multiple STP) of the Spanning Tree Protocol (STP) to support.</p>
Hello Time (s)	<p><b>Synopsis:</b> An integer between 1 and 10</p> <p><b>Default:</b> 2</p> <p>The time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic. (Relationship : <math>\text{maxAgeTime} \geq 2 * (\text{helloTime} + 1.0 \text{ seconds})</math>)</p>
Max Age (s)	<p><b>Synopsis:</b> An integer between 6 and 40</p> <p><b>Default:</b> 20</p> <p>The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network. (Relationship : <math>\text{maxAgeTime} \geq 2 * (\text{helloTime} + 1.0 \text{ seconds})</math>)</p>
Transmission Hold Count	<p><b>Synopsis:</b> An integer between 0 and 100</p> <p><b>Default:</b> 0</p> <p>The maximum number of configuration messages on each port that may be sent in a special event, such as recovering from a failure or bringing up a new link. After the maximum number of messages is reached, Rapid Spanning Tree Protocol (RSTP) will be limited to one message per second. Larger values allow the network to recover from failed links more quickly. If RSTP is being used in a ring architecture, the transmit count should be larger than the number of switches in the ring. If a number is not defined, the value is considered unlimited.</p>
Forwarding Delay(s)	<p><b>Synopsis:</b> An integer between 4 and 30</p> <p><b>Default:</b> 15</p> <p>The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.</p>
Maximum Hops	<p><b>Synopsis:</b> An integer between 6 and 40</p> <p><b>Default:</b> 20</p> <p>The maximum possible bridge diameter inside a Multiple Spanning Tree (MST) region. MST BPDUs propagating inside an MST region carry a time-to-live parameter decremented</p>

Parameter	Description
	by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, the BPDUs may be discarded due to their time-to-live information. This parameter is only applicable to Multiple Spanning Tree Protocol (MSTP) configurations.
MST Region Name	<b>Synopsis:</b> A string up to 32 characters long  The name of the MST region. All devices in the same MST region must have the same region name configured
MST Revision Level	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 0  The revision level for the MST configuration. Typically, all devices in the same MST region are configured with the same revision level. However, different revision levels can be used to create sub-regions under the same region name.

3. Commit the changes.

## eRSTP Settings

Configure the eRSTP settings as follows:

1. Navigate to the **eRSTP Parameters** tab under **Layer 2 » Spanning Tree**.
2. Configure the following parameters as required:

Parameter	Description
Max Network Diameter Multiplier	<b>Synopsis:</b> [ 1   4 ] <b>Default:</b> 4  The Max Network Diameter as a multiplier of the MaxAgeTime value.
BPDU Guard Mode	<b>Synopsis:</b> [ specify   noshutdown   untilreset ] <b>Default:</b> noshutdown  The Rapid Spanning Tree Protocol (RSTP) standard does not address network security. RSTP must process every received Bridge Protocol Data Unit (BPDU) and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. BPDU Guard is a feature that protects the network from BPDUs received by a port where RSTP-capable devices are not expected to be attached. If a BPDU is received by a port for which the 'Edge' parameter is set to 'TRUE' or RSTP is disabled, the port will be shut down for the time period specified by this parameter. <ul style="list-style-type: none"> <li>• NO SHUTDOWN: BPDU Guard is disabled.</li> <li>• UNTIL RESET: The port will remain shut down until the port reset command is issued by the user.</li> <li>• SPECIFY: A timeout period is specified for the port using the BPDU Timeout parameter.</li> </ul>

Parameter	Description
BPDU Timeout	<b>Synopsis:</b> An integer between 1 and 86400  The time for which a port is shutdown. Only applicable when BPDU Guard Mode is set to <b>specify</b> .
Fast Root Failover	<b>Synopsis:</b> [ on   off   on-with-standard-root ] <b>Default:</b> on  The Fast Root Failover algorithm. Options include: <ul style="list-style-type: none"> <li>• Off: The Fast Root Failover algorithm is disabled. As such, a root switch failure may result in excessive connectivity recovery time in a mesh network.</li> <li>• On: Fast Root Failover is enabled and the most robust algorithm is used, which restores network connectivity quickly in case of root bridge failure in a mesh network.</li> <li>• On with standard root: Fast Root Failover is enabled but a relaxed algorithm is used, allowing the use of a standard switch in the root role.</li> </ul>
IEEE802.1w Interoperability	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true  Enables/disables IEEE 802.1w Interoperability
Cost Style	<b>Synopsis:</b> [ stp   rstp ] <b>Default:</b> stp  The style of link costs to employ. STP uses 16-bit path costs based upon 1x10E9/link speed (4 for 1Gbps, 19 for 100 Mbps and 100 for 10 Mbps) whereas RSTP uses 32-bit costs based upon 2x10E13/link speed (20,000 for 1Gbps, 200,000 for 100 Mbps and 2,000,000 for 10 Mbps). Note that RSTP link costs are used only when the bridge version support is set to allow RSTP and the port does not migrate to the Spanning Tree Protocol (STP).

3. Commit the changes.

### RSTP Instance Settings

Configure the RSTP instance settings as follows:

1. Navigate to the **Bridge RSTP Parameters** tab under **Layer 2 » Spanning Tree » RSTP**.
2. Configure the following parameters as required:

Parameter	Description
Bridge Priority	<b>Synopsis:</b> [ 0   4096   8192   12288   16384   20480   24576   28672   32768   36864   40960   45056   49152   53248   57344   61440 ] <b>Default:</b> 32768  The priority assigned to the RSTP/Common Bridge Instance.

3. Commit the changes.

### 13.4.5 Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces

To configure the Spanning Tree Protocol (STP) for a switched Ethernet port, do the following:

1. Navigate to:
  - **For switched Ethernet ports:**  
the **Ports** tab under **Layer 2 » Spanning Tree » RSTP » Port/Trunk RSTP Parameters » { interface }**, where { interface } is the name given to the switched Ethernet port.
  - **For Ethernet trunk interfaces:**  
the **Trunks** tab under **Layer 2 » Spanning Tree » RSTP » Port/Trunk RSTP Parameters » { id }**, where { id } is the ID given to the interface.
2. Configure the following parameters as required:

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables/disables STP/RSTP on the interface.</p>
Admin Edge	<p><b>Synopsis:</b> [ forceTrue   forceFalse   auto ]</p> <p><b>Default:</b> auto</p> <p>Edge ports are ports that do not participate in the spanning tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP-disabled port, accidentally connecting an edge port to another port in the spanning tree will result in a detectable loop. The <b>Edgeness</b> of the port will be switched off and the standard RSTP rules will apply (until the next link outage).</p>
Admin Point to Point	<p><b>Synopsis:</b> [ forceTrue   forceFalse   auto ]</p> <p><b>Default:</b> auto</p> <p>RSTP uses a peer-to-peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating in full-duplex mode. The point-to-point parameter allows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges).</p>

Parameter	Description
Restricted Role	If enabled, causes the port not to be selected as the root port for the CIST or any MSTI, even though it has the best spanning tree priority vector. This parameter should be FALSE by default.
Restricted TCN	If TRUE, causes the port not to propagate received topology change notifications and topology changes to other ports. This parameter should be FALSE by default. If set, it can cause a temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent, incorrectly learned station location information.
RSTP Priority	<b>Synopsis:</b> [ 0   16   32   64   96   112   128   144   160   176   192   208   224   240 ] <b>Default:</b> 128  The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
STP Cost	<b>Synopsis:</b> [ auto-cost ] or An integer between 0 and 65535 <b>Default:</b> auto-cost  The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard STP port costs as negotiated (four for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
RSTP Cost	<b>Synopsis:</b> [ auto-cost ] or An integer between 0 and 2147483647 <b>Default:</b> auto-cost  The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.

3. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 670).
4. Commit the changes.

### 13.4.6 Managing Multiple Spanning Tree Instances Globally

MSTP (Multiple Spanning Tree Protocol), as defined by the IEEE 802.1 standard, maps multiple VLANs to a single Spanning Tree instance, otherwise referred to as a Multiple Spanning Tree Instance (MSTI).

Each MSTI is assigned an MST ID and a bridge priority:

- The MST ID is used to associate the MSTI with a VLAN.
- The bridge priority is used by all devices in the Spanning Tree topology to determine which device among them is elected the root device or backbone. An ideal root device is one that is central to the network and not connected to end devices.

For more information about MSTP, refer to "MSTP Operation" (Page 659).

### 13.4.6.1 Viewing Statistics for Multiple Spanning Tree Instances

To view statistics related to Multiple Spanning Tree Instances (MSTIs), navigate to the **Bridge MSTI Status** tab under **Layer 2 » Spanning Tree » MSTP**.

The table provides the following information:

Parameter	Description
MSTP Instance ID	<b>Synopsis:</b> An integer between 1 and 16 The bridge identifier of this bridge.
Status	<b>Synopsis:</b> [ none   designatedBridge   notDesignatedForAnyLAN   rootBridge ] The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports.
Root Priority	<b>Synopsis:</b> An integer The bridge identifier of the root bridge.
Root MAC	<b>Synopsis:</b> A string up to 17 characters long The bridge identifier of the root bridge.
Bridge Priority	<b>Synopsis:</b> An integer The bridge identifier of this bridge.
Bridge MAC	<b>Synopsis:</b> A string up to 17 characters long The bridge identifier of this bridge.
Root Port Slot	<b>Synopsis:</b> [ ---   sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   trnk ] If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network.
Root Port Port	<b>Synopsis:</b> An integer If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network.



**13.4.6.2 Viewing a List of Multiple Spanning Tree Instances**

To view a list of Multiple Spanning Tree Instances (MSTIs), navigate to the **Bridge MSTI Parameters** tab under **Layer 2 » Spanning Tree » MSTP**. If MSTIs have been configured, a list appears.

If no MSTIs have been configured, add instances as needed. For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 670).

**13.4.6.3 Adding a Multiple Spanning Tree Instance**

To add a Multiple Spanning Tree Instance (MSTI), do the following:

**Note**

RUGGEDCOM ROX II supports up to 16 MSTIs.

1. Navigate to the **Bridge MSTI Parameters** tab under **Layer 2 » Spanning Tree » MSTP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
MSTP Instance ID	<b>Synopsis:</b> An integer between 1 and 16 The Multiple Spanning Tree Protocol (MSTP) instance ID.

4. Click **OK** to create the instance.

 **NOTICE**

Since each MSTI acts as an independent RSTP instance, its configuration is similar to that of RSTP. However, until one or more VLANs are mapped to an MSTI, an MSTI is considered to be inactive.

5. Configure the following parameter(s) as required:

Parameter	Description
Bridge Priority	<b>Synopsis:</b> [ 0   4096   8192   12288   16384   20480   24576   28672   32768   36864   40960   45056   49152   53248   57344   61440 ] <b>Default:</b> 32768  Bridge priority provides a way to control the topology of the Spanning Tree Protocol (STP) connected network. The desired root and designated bridges can be configured for a particular topology. The bridge with the lowest priority will become the root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become the root. Designated bridges that (for redundancy purposes) service a common Local Area Network (LAN) also use priority to determine which bridge is active. In this way, careful selection of bridge priorities

Parameter	Description
	can establish the path of traffic flows in normal and abnormal conditions.

6. Map one or more static VLANs and map them to the MSTI. For more information, refer to "Adding a Static VLAN" (Page 321).
7. Commit the changes.

#### 13.4.6.4 Deleting a Multiple Spanning Tree Instance

To delete a Multiple Spanning Tree Instance (MSTI), do the following:

1. Navigate to the **Bridge MSTI Parameters** tab under **Layer 2 » Spanning Tree » MSTP**.
2. Select the instance to be deleted, and then click **Delete Entry**.
3. Commit the changes.

### 13.4.7 Managing Multiple Spanning Tree Instances Per-Port

This section describes how to configure and manage Multiple Spanning Tree Instances (MSTIs) for individual ports.

#### 13.4.7.1 Viewing Per-Port Multiple Spanning Tree Instance Statistics

To view Multiple Spanning Tree Instance (MSTI) statistics for individual switched Ethernet ports and/or Ethernet trunk interfaces, navigate to the **Port RSTP Statistics** tab under **Layer 2 » Spanning Tree » RSTP**:

This table provides the following information:

Parameter	Description
Slot	<p><b>Synopsis:</b> [ sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   trnk ]</p> <p>The slot of the module that contains this port.</p>
Port	<p><b>Synopsis:</b> An integer between 1 and 16</p> <p>The port number as seen on the front plate silkscreen of the module.</p>
STP State	<p><b>Synopsis:</b> [ disabled   blocking   listening   learning   forwarding   linkDown   discarding ]</p> <p>The status of this interface in the spanning tree:</p> <ul style="list-style-type: none"> <li>• Disabled: The Spanning Tree Protocol (STP) is disabled on this port.</li> <li>• Link Down: STP is enabled on this port but the link is down.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>Discarding: The link is not used in the STP topology but is standing by.</li> <li>Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic.</li> <li>Forwarding: The port is forwarding traffic.</li> </ul>
STP Role	<p><b>Synopsis:</b> [ ----   root   designated   alternate   backup   master ]</p> <p>The role of this port in the spanning tree:</p> <ul style="list-style-type: none"> <li>Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to.</li> <li>Root: The single port on the bridge, which provides connectivity towards the root bridge.</li> <li>Backup: The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by.</li> <li>Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by.</li> <li>Master: Only exists in Multiple Spanning Tree Protocol (MSTP). The port is a Multiple Spanning Tree (MST) region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree (CST) root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).</li> </ul>
STP Cost	<p><b>Synopsis:</b> An integer</p> <p>The total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured, 1 Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge.</p>
Desig Bridge Priority	<p><b>Synopsis:</b> An integer</p> <p>The bridge identifier of this bridge.</p>
Desig Bridge MAC	<p><b>Synopsis:</b> A string up to 17 characters long</p> <p>The bridge identifier of this bridge.</p>

### 13.4.7.2 Viewing a List of Per-Port Multiple Spanning Tree Instances

To view a list of the Multiple Spanning Tree Instances (MSTIs) for switched Ethernet ports or Ethernet trunk interfaces, navigate to:

- For switched Ethernet ports:  
the **MSTI Port** tab for the selected interface under **Layer 2 » Spanning Tree » MSTP » Port/Trunk MSTI Parameters**.

- **For Ethernet trunk interfaces:**  
the **Trunk Parameters** tab for the selected interface under **Layer 2 » Spanning Tree » MSTP » Port/Trunk MSTI Parameters**.

A list appears.

If no MSTIs have been configured, add them as needed. For more information, refer to "Adding a Port-Specific Multiple Spanning Tree Instance" (Page 673).

### 13.4.7.3 Adding a Port-Specific Multiple Spanning Tree Instance

To add a Multiple Spanning Tree Instance (MSTI) for a switched Ethernet port or an Ethernet trunk interface, do the following:

---

#### Note

RUGGEDCOM ROX II supports up to 16 MSTIs per port/interface.

---

1. Navigate to:
  - **For switched Ethernet ports:**  
the **MSTI Port** tab for the selected interface under **Layer 2 » Spanning Tree » MSTP » Port/Trunk MSTI Parameters**.
  - **For Ethernet trunk interfaces:**  
the **Trunk Parameters** tab for the selected interface under **Layer 2 » Spanning Tree » MSTP » Port/Trunk MSTI Parameters**.
2. Click **Add Entry**. A dialog box appears.
3. Configure the following parameter(s) as required:

Parameter	Description
MSTP ID	<b>Synopsis:</b> An integer between 1 and 16 MSTP Instance Identifier

4. Click **OK** to create the instance.

#### NOTICE

Since each MSTI acts as an independent RSTP instance, its configuration is similar to that of RSTP. However, until one or more VLANs are mapped to an MSTI, an MSTI is considered to be inactive.

5. Configure the following parameter(s) as required:

Parameter	Description
MSTP Priority	<p><b>Synopsis:</b> [ 0   16   32   64   96   112   128   144   160   176   192   208   224   240 ]</p> <p><b>Default:</b> 128</p> <p>The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.</p>
STP Cost	<p><b>Synopsis:</b> [ auto-cost ] or An integer between 0 and 65535</p> <p><b>Default:</b> auto-cost</p> <p>The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard STP port costs as negotiated (four for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.</p>
RSTP Cost	<p><b>Synopsis:</b> [ auto-cost ] or An integer between 0 and 2147483647</p> <p><b>Default:</b> auto-cost</p> <p>The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.</p>

6. Map one or more static VLANs and map them to the MSTI. For more information, refer to "Adding a Static VLAN" (Page 321).
7. Commit the changes.

#### 13.4.7.4 Deleting a Port-Specific Multiple Spanning Tree Instances

To delete a Multiple Spanning Tree Instance (MSTI) for a switched Ethernet port or an Ethernet trunk interface, do the following:

1. Navigate to:
  - **For switched Ethernet ports:**  
the **MSTI Port** tab for the selected interface under **Layer 2 » Spanning Tree » MSTP » Port/Trunk MSTI Parameters**.
  - **For Ethernet trunk interfaces:**  
the **Trunk Parameters** tab for the selected interface under **Layer 2 » Spanning Tree » MSTP » Port/Trunk MSTI Parameters**.
2. Select the interface to be deleted, and then click **Delete Entry**.

3. Commit the change.

## 13.4.8 Viewing the Status of RSTP

To view the status of the RSTP network, navigate to the **Bridge RSTP Status** tab under **Layer 2 » Spanning Tree » RSTP**. A table appears.

This following information is provided:

Parameter	Description
Status	<b>Synopsis:</b> [ none   designatedBridge   notDesignatedForAnyLAN   rootBridge ]  The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports.
Bridge Priority	<b>Synopsis:</b> An integer  The bridge identifier of this bridge.
Bridge MAC	<b>Synopsis:</b> A string up to 17 characters long  The bridge identifier of this bridge.
Root Priority	<b>Synopsis:</b> An integer  The priority value of the root bridge.
Root MAC	<b>Synopsis:</b> A string up to 17 characters long  The MAC address of the root bridge.
Regional Root Priority	<b>Synopsis:</b> An integer  The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to.
Regional Root MAC	<b>Synopsis:</b> A string up to 17 characters long  The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to.
Root Port Slot	<b>Synopsis:</b> [ ---   sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   trnk ]  If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network.
Root Port Port	<b>Synopsis:</b> An integer  If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network.
Root Path Cost	<b>Synopsis:</b> An integer  The total cost of the path to the root bridge, composed of the sum of the costs of each link in the path. If custom costs have not been

Parameter	Description
	configured. 1 Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge.
Regional Root Path Cost	<b>Synopsis:</b> An integer For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is the cost of the path to the Internal Spanning Tree (IST) root (i.e. regional root) bridge
Configured Hello time	<b>Synopsis:</b> An integer The configured hello time from the Bridge RSTP Parameters menu.
Learned Hello Time	<b>Synopsis:</b> An integer The actual hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Forward Delay	<b>Synopsis:</b> An integer The configured forward delay time from the Bridge RSTP Parameters menu.
Learned Forward Delay	<b>Synopsis:</b> An integer The actual forward delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Max Age	<b>Synopsis:</b> An integer The configured maximum age time from the Bridge RSTP Parameters menu.
Learned Max Age	<b>Synopsis:</b> An integer The actual maximum age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Total topology Changes	<b>Synopsis:</b> An integer A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems.

### 13.4.9 Viewing RSTP Per-Port Statistics

To view Rapid Spanning Tree Protocol (RSTP) statistics for each port, navigate to the **Port RSTP Statistics** tab under **Layer 2 » Spanning Tree » RSTP**. A table appears.

The following information is provided:

Parameter	Description
Slot	<p><b>Synopsis:</b> [ sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   trnk ]</p> <p>The slot of the module that contains this port.</p>
Port	<p><b>Synopsis:</b> An integer between 1 and 16</p> <p>The port number as seen on the front plate silkscreen of the module.</p>
STP State	<p><b>Synopsis:</b> [ disabled   blocking   listening   learning   forwarding   linkDown   discarding ]</p> <p>Describes the status of this interface in the spanning tree:</p> <ul style="list-style-type: none"> <li>• Disabled: Spanning Tree Protocol (STP) is disabled on this port.</li> <li>• Link Down: STP is enabled on this port but the link is down.</li> <li>• Discarding: The link is not used in the STP topology but is standing by.</li> <li>• Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic.</li> <li>• Forwarding : The port is forwarding traffic.</li> </ul>
Desig Bridge Priority	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p>Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.</p>
Desig Bridge MAC	<p><b>Synopsis:</b> A string up to 17 characters long</p> <p>Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.</p>
Oper Edge	<p><b>Synopsis:</b> [ true   false ]</p> <p>Whether or not the port is operating as an edge port.</p>

### 13.4.10 Clearing Spanning Tree Protocol Statistics

To clear all Spanning Tree Protocol statistics, do the following:

1. Navigate to the **Port RSTP Statistics** tab under **Layer 2 » Spanning Tree » RSTP**.
2. Under **Clear Spanning Tree Statistics**, click **Perform**.

## 13.5 Managing Redundant Network Access (RNA)

This section describes how to configure Redundant Network Access (RNA). RNA aides in the deployment of hitless network redundancy by duplicating all frames bound for the redundant network domain. It is designed for applications that require high availability.



**⚠ NOTICE**

RNA functions are only available for RUGGEDCOM MX5000 and MX5000RE devices equipped with a PRP module.

## 13.5.1 Understanding RNA

Layer 2 protocols – such as the Rapid Spanning Tree Protocol (RSTP), Resilient Ethernet Protocol (REP) and Media Redundancy Protocol (MRP) – help networks recover from failures by automatically changing the network configuration to allow the flow of traffic to resume, typically by opening a blocked port. However, this is a two-step process (fault detection followed by network reconfiguration) that can take a few milliseconds or a few seconds to complete, resulting in a noticeable network delay.

Redundant Network Access (RNA) provides instead *hitless* network recovery by deploying the Parallel Redundancy Protocol (PRP).

### 13.5.1.1 Parallel Redundancy Protocol (PRP)

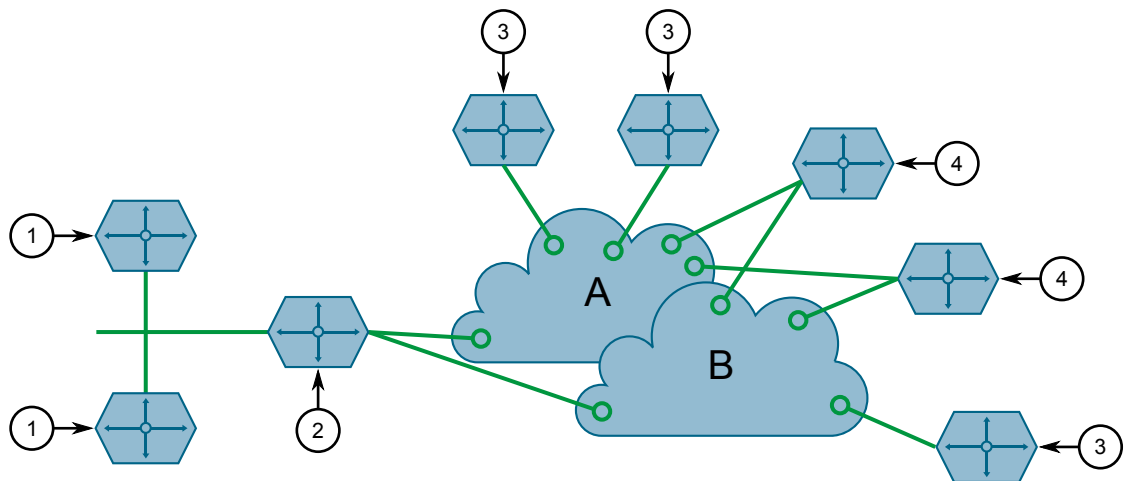
Defined by the IEC 62439-3 standard, the Parallel Redundancy Protocol (PRP) replicates each data packet over two physically independent Ethernet networks (LAN A and LAN B) to guarantee the delivery of at least one of the packets should one network fail.

In a PRP redundant network, there are *Double Attached Nodes (DANs)*, *Singly Attached Nodes (SANs)*, *Virtual DANs (VDANs)* and *RedBox* devices.

- **DANs**  
Double Attached Nodes (DANs) are PRP-aware devices that have a network port connected to LAN A and a network port connected to LAN B. DANs duplicate each received data packet and assign them both a Redundancy Check Trailer (RCT) before sending them simultaneously to their destination nodes. An RCT contains a sequence number that helps the destination node identify which packets are duplicates. Destination nodes remove the RCT from the first packet they receive and then consume them. If a second packet is received, the destination node knows to discard it.
- **SANs**  
Singly Attached Nodes (SANs) are PRP-unaware devices connected to either LAN A or LAN B.
- **RedBox**  
RedBox devices, or PRP Redundancy Boxes, function similarly to DANs, except they also act as proxies on behalf of other devices that are PRP-unaware and have only one network port.

- **VDANs**  
A Virtual DAN (VDAN) is any device that sits behind a RedBox. While these devices are unable to connect directly to the redundant network like other PRP-aware devices, they can function like a DAN through the RedBox.

In a PRP redundant network, RUGGEDCOM MX5000 and MX5000RE devices are configured as RedBox devices.



- ① VDAN
- ② RedBox (RUGGEDCOM MX5000 or MX5000RE)
- ③ SAN
- ④ DAN

Figure 13.9 Parallel Redundancy Protocol (PRP)

### 13.5.1.2 Supervision Frames

RedBoxes are required to send supervision frames on behalf of the VDANs they facilitate. For this, there is a separate *proxy nodes table* that lists the MAC address for each associated VDAN. Whenever the MAC address of a VDAN is learned, the RedBox adds it to the list and begins sending supervision frames to the redundancy network. The interval at which supervision frames are sent is user configurable.

Entries in both the node and proxy node tables will age out if a supervision or non-PRP frame is not received within 60 seconds of the last received frame.

### 13.5.1.3 PRP Requirements

Before deploying the device on a PRP-aware redundancy network, note the following requirements:

- Redundancy Check Trailer (RCT) sequence numbers expand each Ethernet frame by 6 octets. Make sure the redundancy network supports jumbo frames (more than 1522 bytes).

- In addition to expanded Ethernet frames, supervisory frames also consume bandwidth. Make sure to consider the overhead introduced by PRP when calculating network capacity requirements.

### 13.5.2 Configuring RNA

To configure RNA, do the following:

1. Navigate to the **Port Parameters** tab under **Layer 2 » Redundant Network Access**.
2. Configure the following parameter(s):

---

#### Note

Setting **Life Check Interval** to **0** will disable the generation of supervision frames.

---

Parameter	Description
Life Check Interval	<p><b>Synopsis:</b> An integer between 0 and 300</p> <p><b>Default:</b> 2</p> <p>Interval between PRP_Supervision frames sent in number of seconds.</p>

3. Commit the changes.

### 13.5.3 Viewing the Proxy Nodes Table

The proxy nodes table details information about each VDAN for which the device acts as a proxy to the redundancy network.

To view the proxy nodes table, navigate to the **Statistics** tab under **Layer 2 » Redundant Network Access**, and then select **Proxy Nodes Table**.

This table displays the following information about each node:

Parameter	Description
LRE Interface Stats Index	<p><b>Synopsis:</b> An integer</p> <p>A unique value for each LRE.</p>
LRE Proxy Node Index	<p><b>Synopsis:</b> An integer</p> <p>A unique value for each node in the LRE's proxy node table.</p>
LRE Proxy Node MAC Address	<p><b>Synopsis:</b> A string</p> <p>Each entry contains information about a particular node for which the LRE acts as a proxy for the PRP network.</p>

## 13.5.4 Viewing the Nodes Table

The nodes table is a list of all learned MAC addresses for DAN and SAN devices on the redundancy network.

To view the nodes table, do the following:

1. Navigate to the **Statistics** tab under **Layer 2 » Redundant Network Access**.
2. Select the **Nodes Table** tab.

This table displays the following information about each node:

Parameter	Description
LRE Interface Stats Index	<b>Synopsis:</b> An integer A unique value for each LRE.
LRE Nodes Index	<b>Synopsis:</b> An integer Unique value for each node in the LRE's node table.
LRE Nodes MAC Address	<b>Synopsis:</b> A string Each MAC address corresponds to a single Dual Attached Node
LRE Rem Node Type	<b>Synopsis:</b> [ danp   redboxp   vdanh   danh   redboxh   vdanh ] DAN type, as indicated in the received supervision frame.
LRE Time Last Seen A	<b>Synopsis:</b> An integer Time in TimeTicks (1/100s) since the last frame from this remote LRE was received over LAN A.
LRE Time Last Seen B	<b>Synopsis:</b> An integer Time in TimeTicks (1/100s) since the last frame from this remote LRE was received over LAN B.

## 13.5.5 Viewing Statistics Collected for RNA Ports

The device collects statistics on traffic traversing the RNA ports.

---

### Note

Statistics displayed are not updated automatically.

---

### Redundant Network Access Port Statistics

To view the collected statistics, navigate to the **Statistics** tab under **Layer 2 » Redundant Network Access**, select the **Ports** tab.

The number of nodes the RedBox is aware of on the redundancy and non-redundancy sides of the network is displayed. The MAC address being broadcast in supervision frames is also displayed.

Parameter	Description
Node Count	<b>Synopsis:</b> An integer Number of nodes currently discovered on the redundant side of the network.
Proxy Node Count	<b>Synopsis:</b> An integer Number of nodes currently discovered on the non-redundant side of the network.
Device Address	<b>Synopsis:</b> A string up to 17 characters long The MAC Address of this node used in supervision frames.

### Port A and Port B

To view the collected statistics, navigate to the **Statistics** tab under **Layer 2 » Redundant Network Access**, select the **Ports** tab, select an interface, and then select **Port A and B**. Activity on the redundancy network is displayed.

Parameter	Description
Received Packets Count	<b>Synopsis:</b> An integer The number of received packets.
Received Tagged Packets Count	<b>Synopsis:</b> An integer The number of received tagged packets.
Received Duplicated Packets Count	<b>Synopsis:</b> An integer The number of received duplicated packets.
Received Packets on Wrong LAN Count	<b>Synopsis:</b> An integer The number of received packets on the wrong RNA LAN port.
Received Packets with CRC Error Count	<b>Synopsis:</b> An integer The number of received bad packets (with any kind of error).

### 13.5.6 Clearing Statistics Collected for RNA Ports

Statistics collected for each RNA port can be cleared individually.

To clear the statistics for port A or B, do the following:

1. Navigate to the **Statistics** tab under **Layer 2 » Redundant Network Access**.
2. Select the **Ports** tab, and then select an interface.
3. Click **Perform** under either **Clear Port A Stats** or **Clear Port B Stats** to clear the statistics.

## 13.6 Managing the Media Redundancy Protocol (MRP)

RUGGEDCOM ROX II supports the Media Redundancy Protocol (MRP), a network redundancy protocol for mission-critical applications.

### 13.6.1 Understanding MRP

The Media Redundancy Protocol (MRP) is a networking protocol designed to implement redundancy and recovery in a ring topology of up to 50 devices. It allows rings of Ethernet switches to quickly overcome any single failure of an inter-switch link or switch in the MRP ring or interconnection topology.

MRP operates at the MAC layer of Ethernet switches and uses the functions of ISO/IEC/IEEE 8802-3 (IEEE 802.3) and IEEE 802.1Q, including the Filtering Database (FDB).

MRP is standardized by the International Electrotechnical Commission as IEC 62439-2.

#### 13.6.1.1 MRP Operation

An MRP ring consists of a single switch known as the Media Redundancy Manager (MRM). All other switches in the ring are Media Redundancy Clients (MRC).

Each MRM and MRC designates two ports to participate in the MRP ring.

In normal operation, an MRP ring operates in a **ring-closed** state. In this state, one of the ring ports on the MRM is blocked, while the other forwards traffic to the MRP ring. For MRCs, both ring ports are in the **forwarding** state.

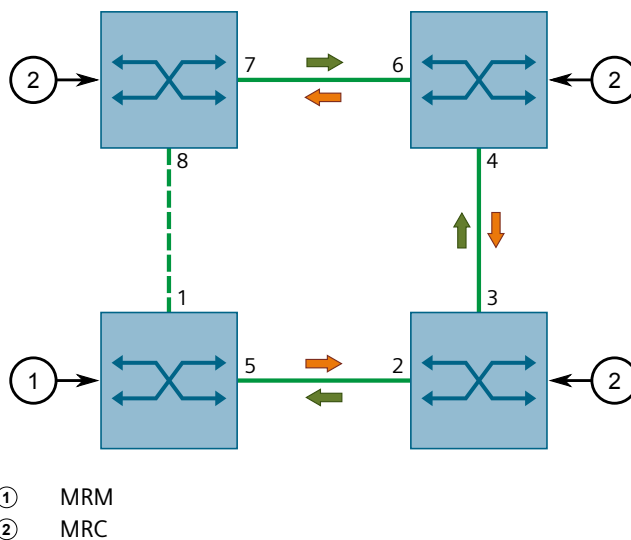
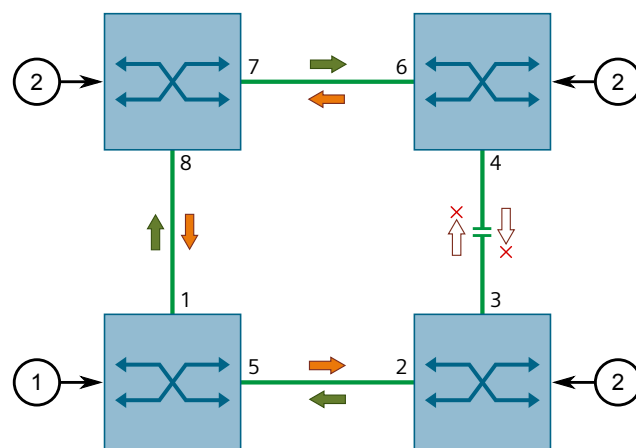


Figure 13.10 MRP Ring-Closed State

When a network failure (i.e. failed link between two switches) occurs, MRCs adjacent to the failure signal the fault to the MRM and the ring moves to a **ring-open** state. The following occurs in this state:

- For the MRM, the previously blocked ring port begins forwarding traffic along with the other ring port
- For MRCs adjacent to the network failure, the ring port connected to the broken link is disabled, while the other ring port continues to forward traffic
- Ring ports on all other MRCs continue to forward traffic



- ① MRM
- ② MRC

Figure 13.11 MRP Ring-Open State

**Note**

Frames will be lost when transitioning between ring states.

**13.6.1.2 MRA**

The MRM for an MRP ring can be chosen manually by setting the role for a switch to **manager**, or it can be decided automatically by one or more Media Redundancy Manager/Auto (MRA) switches.

An MRA decides or negotiates with other MRAs in the ring through an election process on which switch in the ring will be the MRM. Once an MRM is chosen, all MRAs in the ring automatically change to MRCs.

The MRM is chosen based on the priority defined for each switch.

**Note**

A switch cannot be an MRA if an MRM exists on the same MRP ring.

### 13.6.1.3 MRP Instances

An MRM can support up to four MRP rings, or instances. Each instance requires a unique domain ID and a dedicated pair of ring ports. The device must also be the MRM (or ring manager) in all instances.

MRCs belonging to an MRP instance must have the same domain ID as the MRM.

### 13.6.1.4 Requirements and Restrictions

Note the following requirements and restriction before deploying MRP:

- A switch acting as an MRM can support up to four MRP rings (or instances).
- Up to 50 MRCs are supported per MRP ring.
- MRP ring ports cannot be trunk or link aggregated ports.
- The same port cannot be used for more than one MRP ring.
- Only switchports can be chosen as ring ports in an MRP ring. Routable ports are not supported.
- RSTP must be disabled on any port used as an MRP ring port.

## 13.6.2 Configuring MRP Globally

To configure the Media Redundancy Protocol globally, do the following:

1. Navigate to the **MRP Global Parameters** tab under **Layer 2 » Media Redundancy**.
2. Configure the following parameter(s) as required:

Parameter	Description
Enable MRP	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables MRP globally.</p>
Auto Generate UUID	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables or disables the automatic generation of the MRP Universal Unique Identifier (UUID).</p>

3. Commit the changes.



### 13.6.3 Enabling/Disabling SNMP Traps for MRP

The following proprietary SNMP traps are available to indicate when MRP rings are open or closed:

- rcMrpManagerRingClosed
- rcMrpManagerRingOpen

For more information, refer to "Proprietary SNMP Traps" (Page 851).

These traps can be enabled or disabled as needed.

To enable/disable these SNMP traps, do the following:

1. Navigate to the **MRP Parameters** tab under **Layer 2 » Media Redundancy** and select the desired MRP instance.
2. Under **Ring SNMP Traps**, click **Enable** to enable SNMP traps, or clear the check box to disable the traps.
3. Commit the changes.

### 13.6.4 Viewing the List of MRP Instances

To view a list of configured MRP instances, navigate to the **MRP Parameters** tab under **Layer 2 » Media Redundancy**. If MRP instances have been configured, a list appears.

If no MRP instances have been configured, add them. For more information, refer to "Adding an MRP Instance" (Page 686).

### 13.6.5 Adding an MRP Instance

To configure an MRP instance, do the following:

 **NOTICE**

**Configuration hazard – risk of communication disruption**

RUGGEDCOM ROX II only allows multiple MRP instances if the device is the ring manager in each instance. A device can have up to four ring manager instances.

 **NOTICE**

**Configuration hazard – risk of communication disruption**

MRMs or MRAs acting as a ring manager must be either physically disconnected or have their primary ring port disabled (i.e. MRP ring open) before the MRM instance configuration can be changed.

For more information about configuring ports, refer to "Configuring a Switched Ethernet Port" (Page 276).

For more information about open and closed MRP rings, refer to "MRP Operation" (Page 683).

### Note

When using port security in an MRP ring, the MAC addresses of devices in the ring must be configured to allow communication between them. Also, the MRM's ring port must be configured in the **Static MAC Addresses** table for the ring to remain in a closed state.

For more information, refer to "Static MAC Address-Based Authentication in an MRP Ring" (Page 136).

1. Navigate to the **MRP Parameters** tab under **Layer 2 » Media Redundancy**.
2. Click **Add Entry**.
3. Configure the following parameters:

Parameter	Description
MRP Instance ID	<b>Synopsis:</b> An integer between 1 and 4 The MRP instance number.

4. Click **OK**.
5. Configure the following parameters:

Parameter	Description
Name	<b>Synopsis:</b> A string between 1 and 24 characters long <b>Default:</b> default-mrpdomain The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name.
Role	<b>Synopsis:</b> [ Disabled   Client   Manager   ManagerAuto ] <b>Default:</b> Client The role assigned to this MRP instance. <ul style="list-style-type: none"> <li>• Disabled – No role is assigned. The MRP instance is disabled.</li> <li>• Client – The device operates as a Media Redundancy Client (MRC).</li> <li>• Manager – The device operates as a Media Redundancy Manager (MRM).</li> <li>• ManagerAuto – The MRP instance automatically determines the role of the device.</li> </ul>
Priority	<b>Synopsis:</b> A string up to 4 characters long <b>Default:</b> 8000 The priority assigned to the MRP instance. This is used when negotiating with other MRP devices to determine which is the MRP Manager. <ul style="list-style-type: none"> <li>• 0000 - Highest priority (Manager)</li> </ul>

13.6.6 Deleting an MRP Instance

Parameter	Description
	<ul style="list-style-type: none"> <li>• 1000-7000 -High priority (Manager)</li> <li>• 8000 - Default priority (Manager)</li> <li>• 9000-E000 - Low priority (ManagerAuto)</li> <li>• F000 - Lowest priority (ManagerAuto)</li> </ul>
Domain ID	<p><b>Synopsis:</b> A string up to 32 characters long  <b>Default:</b> FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF</p> <p>A 128-bit domain UUID unique to a domain/ring. All MRP instances belonging to the same ring must have the same domain ID. If the Auto Generate UUID parameter is enabled, the system automatically generates the domain ID as an MD5 hash of the domain name. In this case, the domain ID cannot be modified.</p> <p>If the Auto Generate UUID parameter is disabled, the domain ID can be modified.</p>
Ring SNMP Traps	<p><b>Synopsis:</b> [ true   false ]  <b>Default:</b> true</p> <p>Enables/disables SNMP traps that indicate the status of the MRP ring. Only applies to the specific MRP instance and when the device is the Media Redundancy Manager (MRM). Traps will only be sent when enabled.</p>

Configure the following parameters to select the primary and secondary ring ports:

Parameter	Description
Primary Slot	MRP ring primary slot and port number.
Secondary Slot	MRP ring secondary slot and port number.

6. Commit the changes.

### 13.6.6 Deleting an MRP Instance

To delete an MRP instance, do the following:

1. If the device is an MRM or MRA acting as a ring manager, open the MRP ring before deleting the MRP instance.

This can be done by either disabling the primary and secondary ring ports via RUGGEDCOM ROX II, or physically disconnecting them.

For more information about disabling the ports, refer to "Configuring a Line Module" (Page 98).

2. Navigate to the **MRP Parameters** tab under **Layer 2 » Media Redundancy**.
3. Select the MRP instance to be deleted and then click **Delete Entry**.
4. Commit the change.

## 13.6.7 Viewing the Status of MRP Instances

To view the status of MRP instances, navigate to the **MRP Status** tab under **Layer 2 » Media Redundancy**. If MRP instances have been configured, a list appears.

The following information is provided per instance:

Parameter	Description
MRP Instance ID	<b>Synopsis:</b> An integer between 1 and 4 The Media Redundancy Protocol (MRP) instance
Name	<b>Synopsis:</b> A string The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name.
Role	<b>Synopsis:</b> [ disable   client   manager   managerAuto ] The role assigned to this MRP instance. <ul style="list-style-type: none"> <li>Disabled – No role is assigned. The MRP instance is disabled.</li> <li>Client – The device operates as a Media Redundancy Client (MRC).</li> <li>Manager – The device operates as a Media Redundancy Manager (MRM).</li> <li>ManagerAuto – The MRP instance automatically determines the role of the device.</li> </ul>
Ring Status	<b>Synopsis:</b> [ unknown   open   closed ] The status of the MRP ring. <ul style="list-style-type: none"> <li>Unknown - The status of the ring is unknown. This is displayed when the device is an MRC</li> <li>Open - The MRP ring is open. Both ring ports are forwarding packets.</li> <li>Closed - The MRP ring is closed. One ring port is forwarding packets, while the other is blocking packets.</li> </ul>
Primary Port	<b>Synopsis:</b> A string The MRP primary port of the MRP ring port.
Primary Port State	<b>Synopsis:</b> [ OFF   DOWN   BLOCKED   FORWARD   UNKNOWN ] The status of the primary ring port. Possible values include: <ul style="list-style-type: none"> <li>OFF - MRP is not running</li> <li>DOWN - The MRP ring port is down</li> <li>BLOCKED - The MRP ring port is blocking packets</li> <li>FORWARD - The MRP ring port is forwarding packets</li> <li>UNKNOWN - The MRP ring port is Unknown</li> </ul>
Secondary Port	<b>Synopsis:</b> A string The MRP secondary port of the MRP ring port.

13.6.8 Example: Configuring an MRP Ring

Parameter	Description
Secondary Port State	<p><b>Synopsis:</b> [ OFF   DOWN   BLOCKED   FORWARD   UNKNOWN ]</p> <p>The status of the secondary ring port. Possible values include:</p> <ul style="list-style-type: none"> <li>• OFF - MRP is not running</li> <li>• DOWN - The MRP ring port is down</li> <li>• BLOCKED - The MRP ring port is blocking packets</li> <li>• FORWARD - The MRP ring port is forwarding packets</li> <li>• UNKNOWN - The MRP ring port is Unknown</li> </ul>
Multi MRM Error	<p><b>Synopsis:</b> [ true   false ]</p> <p>Error indicated by an MRM when more than one MRM are active in the MRP ring.</p>
One Side RX Error	<p><b>Synopsis:</b> [ true   false ]</p> <p>Error indicated by an MRM when the test frames of an MRM has been seen, but only on one ring port.</p>

If no MRP instances have been configured, add them. For more information, refer to "Adding an MRP Instance" (Page 686).

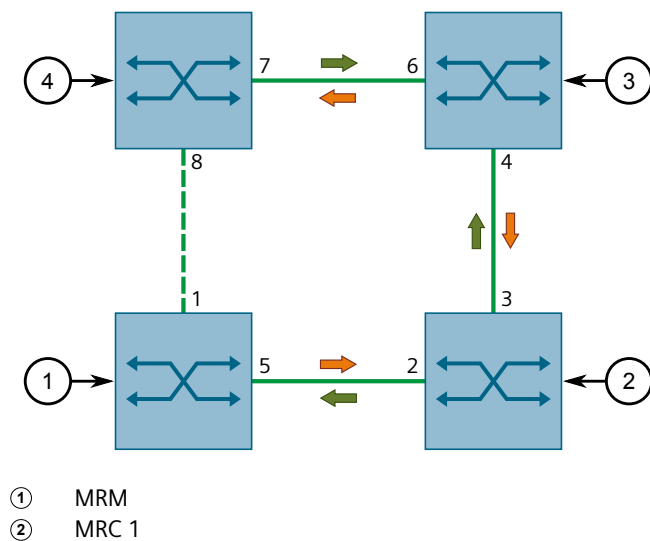
13.6.8 Example: Configuring an MRP Ring

This example demonstrates how to configure an MRP ring using four RUGGEDCOM ROX II devices.

In the following topology, the MRP ring is operating in the ring-closed state.

**⚠ NOTICE**

Values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ③ MRC 2
- ④ MRC 3

Figure 13.12 Topology – MRP Ring

To configure an MRP ring per the topology, do the following:

1. Make sure RSTP is disabled either globally or for each port participating in the MRP ring.

For more information about disabling RSTP globally, refer to "Configuring STP Globally" (Page 663).

For more information about disabling RSTP per port, refer to "Configuring a Switched Ethernet Port" (Page 276).

2. Enable MRP on the MRM and all MRCs.

For more information, refer to "Configuring MRP Globally" (Page 685).

3. Configure an MRP instance for the MRM as follows:

Parameter	Value
Name	{ name }
Role	Manager
PRM Port	5
SEC Port	1
Priority	1000

For more information about configuring MRP instances, refer to "Adding an MRP Instance" (Page 686).

4. Configure an MRP instance for each MRC as follows:

Parameter	Value		
	MRC 1	MRC 2	MRC 3
Name	MRC1	MRC2	MRC3
Role	Client	Client	Client
PRM Port	2	4	7
SEC Port	3	6	8
Priority	A000	A000	A000

For more information about configuring MRP instances, refer to "Adding an MRP Instance" (Page 686).

5. To verify the configuration, make sure the MRP Instance ID is generated automatically on the MRM and each MRC.

For more information about the MRP Instance ID, refer to "Adding an MRP Instance" (Page 686).



## Network Discovery and Management

RUGGEDCOM ROX II supports the following protocols for automatic network discovery, monitoring and device management:

- **Link Layer Device Protocol (LLDP)**  
Use LLDP to broadcast the device's network capabilities and configuration to other devices on the network, as well as receive broadcasts from other devices.
- **Simple Network Management Protocol (SNMP)**  
Use SNMP to notify select users or groups of certain events that happen during the operation of the device, such as changes to network topology, link state, spanning tree root, etc.
- **Network Configuration Protocol (NETCONF)**  
Use NETCONF to remotely download, upload, change, and delete configuration data on the device.

### 14.1 Managing LLDP


RUGGEDCOM ROX II supports the Link Layer Discovery Protocol (LLDP), a Layer 2 protocol for automated network discovery.

LLDP is an IEEE standard protocol (IEEE 802.11AB) that allows a networked device to advertise its own basic networking capabilities and configuration. It can simplify the troubleshooting of complex networks and can be used by Network Management Systems (NMS) to obtain and monitor detailed information about a network's topology. LLDP data are made available via SNMP (through support of LLDP-MIB).

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device's information at regular intervals, in 802.11AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) TLV containing 0 in the information field. This enables remote devices to remove the information associated with the local device in their databases. The LLDP receive module, when enabled, receives information about remote devices and updates its LLDP database of remote systems. When new or updated information is received, the receive module initiates a timer for the valid duration indicated by the TTL TLV in the received LLDPDU. A remote system's information is removed from the database when an LLDPDU is received from it with TTL TLV containing 0 in its information field.



<p> <b>NOTICE</b></p> <p><b>Security hazard – risk of unauthorized access and/or exploitation</b></p> <p>LLDP is not secure by definition. Avoid enabling LLDP on devices connected to external networks. Siemens recommends using LLDP only in secure environments operating within a security perimeter.</p>
---

**Note**

LLDP is implemented to keep a record of only one device per Ethernet port. Therefore, if there are multiple devices sending LLDP information to a switch port on which LLDP is enabled, information about the neighbor on that port will change constantly.

**14.1.1 Configuring LLDP**

To configure the Link Layer Discovery Protocol (LLDP), do the following:

1. Navigate to the **LLDP Global Parameters** tab under **Layer 2 » Net Discovery**.
2. Configure the following parameter(s) as required:

Parameter	Description
State	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables LLDP, making the device an LLDP agent.</p>
Transmission Interval (s)	<p><b>Synopsis:</b> An integer between 5 and 32768</p> <p><b>Default:</b> 30</p> <p>The time in seconds (s) between each subsequent transmission of an LLDP frame.</p>
Transmission Hold	<p><b>Synopsis:</b> An integer between 2 and 10</p> <p><b>Default:</b> 4</p> <p>The multiplier used to determine the time-to-live (TTL) value in an LLDP frame. The TTL value indicates the time in seconds (s) for which the information in an LLDP frame will be considered valid.</p> <p>The TTL value is equal to the value of the <b>Transmission Hold (tx-hold)</b> parameter multiplied by the value of the <b>Transmission Interval (tx-interval)</b> parameter.</p>
Reinitialization Delay (s)	<p><b>Synopsis:</b> An integer between 1 and 10</p> <p><b>Default:</b> 2</p> <p>The time in seconds (s) the LLDP agent will wait before attempting to re-enable LLDP on a port where it has been previously disabled.</p>

Parameter	Description
Transmission Delay (s)	<p><b>Synopsis:</b> An integer between 1 and 8192</p> <p><b>Default:</b> 2</p> <p>The time in seconds (s) the LLDP agent will wait before transmitting a new LLDP frame after the configuration of the device is changed.</p> <p>The value of the <b>Transmission Delay (tx-parameter)</b> should be no more than one quarter of the value of the <b>Transmission Interval (tx-interval)</b> parameter.</p>
Notification Interval (s)	<p><b>Synopsis:</b> An integer between 5 and 3600</p> <p><b>Default:</b> 5</p> <p>The time in seconds (s) between each subsequent transmission of an SNMP trap for LLDP. SNMP traps provide the network manager with updates about LLDP functions.</p>

3. Commit the change.

## 14.1.2 Viewing Global Statistics

To view global statistics for LLDP, navigate to the **LLDP Global Statistics** tab under **Layer 2 » Net Discovery**.

The following information is displayed:

Parameter	Description
Inserts	<p><b>Synopsis:</b> An integer between 0 and 4294967295</p> <p>The total number of new hosts added to the LLDP Neighbor Information Table.</p>
Deletes	<p><b>Synopsis:</b> An integer between 0 and 4294967295</p> <p>The total number of hosts deleted from the LLDP Neighbor Information Table.</p>
Drops	<p><b>Synopsis:</b> An integer between 0 and 4294967295</p> <p>The total number of hosts detected that could not be added to the LLDP Neighbor Information Table.</p>
Ageouts	<p><b>Synopsis:</b> An integer between 0 and 4294967295</p> <p>The number of times that an LLDP neighbor has been dropped because its time-to-live (TTL) value was exhausted. TTL values are specified in the LLDP frames sent from the neighbor to the device.</p>
Timestamp of Last Change	<p><b>Synopsis:</b> A string</p> <p>The timestamp at which the LLDP Global Statistics were last updated. Timestamps represent the amount of time elapsed since the device was powered on. Values are expressed in durations of years, months, weeks, days, hours, minutes, and/or seconds in ISO</p>

Parameter	Description
	8601 format (e.g. P1Y1M2W3DT2H3M30S represents 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30 seconds).

### 14.1.3 Viewing Global Statistics and Advertised System Information

To view system information that is advertised to neighbors, navigate to the **LLDP Local System** tab under **Layer 2 » Net Discovery**.

The following information is displayed:

Parameter	Description
Local Chassis Subtype	<p><b>Synopsis:</b> [ chassisComponent   interfaceAlias   portComponent   macAddress   networkAddress   interfaceName   local ]</p> <p>The source of the <b>Local Chassis ID (local-chassis-id)</b> parameter. Options include:</p> <ul style="list-style-type: none"> <li>chassisComponent - The <b>Local Chassis ID (local-chassis-id)</b> corresponds with the alias for a chassis component (entPhysicalAlias) in the ENTITY-MIB file</li> <li>interfaceAlias - The <b>Local Chassis ID (local-chassis-id)</b> corresponds with the alias for an interface (ifAlias) in the IF-MIB file</li> <li>portComponent - The <b>Local Chassis ID (local-chassis-id)</b> corresponds with the alias for a port or backplane component (entPhysicalAlias) in the ENTITY-MIB file</li> <li>macAddress - The <b>Local Chassis ID (local-chassis-id)</b> is a MAC address associated with the device</li> <li>networkAddress - The <b>Local Chassis ID (local-chassis-id)</b> is an IP address associated with the device</li> <li>interfaceName - The <b>Local Chassis ID (local-chassis-id)</b> corresponds with the default name for an interface (ifName) in the IF-MIB file</li> <li>local - The <b>Local Chassis ID (local-chassis-id)</b> is a locally defined value</li> </ul>
Local Chassis ID	<p><b>Synopsis:</b> A string up to 17 characters long</p> <p>The type-length-value (TLV) used to identify the device to LLDP neighbors.</p> <p>The value of the <b>Local Chassis ID (local-chassis-id)</b> parameter is categorized by the <b>Local Chassis Subtype (local-chassis-subtype)</b> parameter.</p>
Local System Name	<p><b>Synopsis:</b> A string up to 255 characters long</p> <p>An administratively assigned name, often the fully qualified domain name (FQDN), for the device.</p> <p>The <b>Local System Name (local-system-name)</b> parameter corresponds with the sysName object in the SNMPv2-MIB.</p>

## 14.1.3 Viewing Global Statistics and Advertised System Information

Parameter	Description
Local System Description	<p><b>Synopsis:</b> A string up to 255 characters long</p> <p>The default system description of the device, which includes the full name and version ID of its hardware, operating system, and networking software.</p> <p>The <b>Local System Description (local-system-desc)</b> parameter corresponds with the sysDescr object in the SNMPv2-MIB.</p>
System Capabilities	<p><b>Synopsis:</b> [ other   repeater   bridge   wlanAccessPoint   router   telephone   docsisCableDevice   stationOnly ]</p> <p>The network functions the device can serve. Options include:</p> <ul style="list-style-type: none"> <li>• other - The device can serve other, unspecified functions</li> <li>• repeater - The device can receive and regenerate IP packets within a single network</li> <li>• bridge - The device can join two or more networks into a single network</li> <li>• wlanAccessPoint - The device can forward network traffic to/from a WLAN</li> <li>• router - The device can forward IP packets from one wired network to another</li> <li>• telephone - The device can forward IP packets to/from a telephone network</li> <li>• docsisCableDevice - The device can forward IP packets to a Cable TV system</li> <li>• stationOnly - The device can only receive network traffic</li> </ul>
System Capabilities Enabled	<p><b>Synopsis:</b> [ other   repeater   bridge   wlanAccessPoint   router   telephone   docsisCableDevice   stationOnly ]</p> <p>The network functions the device currently serves. Options include:</p> <ul style="list-style-type: none"> <li>• other - The device serves other, unspecified functions</li> <li>• repeater - The device receives and regenerates IP packets within a single network</li> <li>• bridge - The device joins two or more networks into a single network</li> <li>• wlanAccessPoint - The device forwards network traffic to/from a WLAN</li> <li>• router - The device forwards IP packets from one wired network to another</li> <li>• telephone - The device forwards IP packets to/from a telephone network</li> <li>• docsisCableDevice - The device forwards IP packets to a Cable TV system</li> <li>• stationOnly - The device only receives network traffic</li> </ul>

### 14.1.4 Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, navigate to the **Port LLDP Neighbors** tab under **Layer 2 » Net Discovery**.

The table displays the following information:

Parameter	Description
Chassis ID	<p><b>Synopsis:</b> A string up to 17 characters long</p> <p>The type-length-value (TLV) used to identify the LLDP neighbor.</p> <p>The value of the <b>Chassis ID (chassis-id)</b> parameter is categorized by the <b>Chassis Subtype (chassis-subtype)</b> parameter.</p>
Port ID	<p><b>Synopsis:</b> A string up to 17 characters long</p> <p>The remote port from which the LLDP neighbor sends LLDP frames to the device.</p> <p>The value of the <b>Port ID (port-id)</b> parameter is categorized by the <b>Port Subtype (port-subtype)</b> parameter.</p>
System Name	<p><b>Synopsis:</b> A string up to 255 characters long</p> <p>An administratively assigned name, often the fully qualified domain name (FQDN), for the LLDP neighbor.</p> <p>The <b>System Name (system-name)</b> parameter corresponds with the sysName object in the SNMPv2-MIB associated with the LLDP neighbor.</p>
System Description	<p><b>Synopsis:</b> A string up to 255 characters long</p> <p>The default system description of the LLDP neighbor, which includes the full name and version ID of its hardware, operating system, and networking software.</p> <p>The <b>System Description (system-desc)</b> parameter corresponds with the sysDescr object in the SNMPv2-MIB associated with the LLDP neighbor.</p>
Port Description	<p><b>Synopsis:</b> A string up to 255 characters long</p> <p>The default description of the port from which the LLDP neighbor sends LLDP frames to the device. The port description includes the manufacturer, the product name, and the version of the port.</p> <p>The <b>Port Description (port-desc)</b> parameter corresponds with the ifDescr object in the IF-MIB associated with the LLDP neighbor.</p>
Management Address	<p><b>Synopsis:</b> A string up to 31 characters long</p> <p>An address associated with the LLDP neighbor that can be used to access information about the neighbor host.</p> <p>The value of the <b>Management Address (man-address)</b> parameter is categorized by the <b>Management Address Subtype (man-address-subtype)</b> parameter.</p>
Management Address Interface ID	<p><b>Synopsis:</b> An integer</p> <p>The interface with which the <b>Management Address (man-address)</b> of the LLDP neighbor is associated.</p>

Parameter	Description
	The value of the <b>Management Address Interface ID (man-address-if-id)</b> parameter is categorized by the <b>Management Address Interface Subtype (man-address-if-subtype)</b> parameter.
System Capabilities	<p><b>Synopsis:</b> [ other   repeater   bridge   wlanAccessPoint   router   telephone   docsisCableDevice   stationOnly ]</p> <p>The network functions the LLDP neighbor can serve. Possible values include:</p> <ul style="list-style-type: none"> <li>• other - The neighbor host can serve other, unspecified functions</li> <li>• repeater - The neighbor host can receive and regenerate IP packets within a single network</li> <li>• bridge - The neighbor host can join two or more networks into a single network</li> <li>• wlanAccessPoint - The neighbor host can forward network traffic to/from a WLAN</li> <li>• router - The neighbor host can forward IP packets from one wired network to another</li> <li>• telephone - The neighbor host can forward IP packets to/from a telephone network</li> <li>• docsisCableDevice - The neighbor host can forward IP packets to a Cable TV system</li> <li>• stationOnly - The neighbor host can only receive network traffic</li> </ul> <p>The network functions that the LLDP neighbor currently serves are specified by the <b>System Capabilities Enabled (system-caps-enabled)</b> parameter.</p>
System Capabilities Enabled	<p><b>Synopsis:</b> [ other   repeater   bridge   wlanAccessPoint   router   telephone   docsisCableDevice   stationOnly ]</p> <p>The network functions that the LLDP neighbor currently serves. Possible values include:</p> <ul style="list-style-type: none"> <li>• other - The neighbor host serves other, unspecified functions</li> <li>• repeater - The neighbor host receives and regenerates IP packets within a single network</li> <li>• bridge - The neighbor host joins two or more networks into a single network</li> <li>• wlanAccessPoint - The neighbor host forwards network traffic to/from a WLAN</li> <li>• router - The neighbor host forwards IP packets from one wired network to another</li> <li>• telephone - The neighbor host forwards IP packets to/from a telephone network</li> <li>• docsisCableDevice - The neighbor host forwards IP packets to a Cable TV system</li> <li>• stationOnly - The neighbor host only receives network traffic</li> </ul> <p>In addition to the network functions that the LLDP neighbor currently serves, the network functions that the LLDP neighbor can serve are specified by the <b>System Capabilities (system-caps)</b> parameter.</p>

Parameter	Description
Chassis Subtype	<p><b>Synopsis:</b> [ chassisComponent   interfaceAlias   portComponent   macAddress   networkAddress   interfaceName   local ]</p> <p>The source of the <b>Chassis ID (chassis-id)</b> parameter as advertised by LLDP neighbor. Possible values include:</p> <ul style="list-style-type: none"> <li>chassisComponent - The <b>Chassis ID (chassis-id)</b> corresponds with the alias for a chassis component (entPhysicalAlias) in the ENTITY-MIB file</li> <li>interfaceAlias - The <b>Chassis ID (chassis-id)</b> corresponds with the alias for an interface (ifAlias) in the IF-MIB file</li> <li>portComponent - The <b>Chassis ID (chassis-id)</b> corresponds with the alias for a port or backplane component (entPhysicalAlias) in the ENTITY-MIB file</li> <li>macAddress - The <b>Chassis ID (chassis-id)</b> is a MAC address as associated with the LLDP neighbor</li> <li>networkAddress - The <b>Chassis ID (chassis-id)</b> is an IP address associated with the LLDP neighbor</li> <li>interfaceName - The <b>Chassis ID (chassis-id)</b> corresponds with the default name for an interface (ifName) in the IF-MIB file</li> <li>local - The <b>Chassis ID (chassis-id)</b> is a value defined locally by the LLDP neighbor</li> </ul>
Port Subtype	<p><b>Synopsis:</b> [ interfaceAlias   portComponent   macAddress   networkAddress   interfaceName   agentCircuitId   local ]</p> <p>The source of the <b>Port ID (port-id)</b> parameter as advertised by LLDP neighbor. Possible values include:</p> <ul style="list-style-type: none"> <li>interfaceAlias - The <b>Port ID (port-id)</b> corresponds with the alias for an interface (ifAlias) in the IF-MIB file</li> <li>portComponent - The <b>Port ID (port-id)</b> corresponds with the alias for a port component (entPhysicalAlias) in the ENTITY-MIB file</li> <li>macAddress - The <b>Port ID (port-id)</b> is a MAC address associated with a remote port</li> <li>networkAddress - The <b>Port ID (port-id)</b> is an IP address associated with a remote port</li> <li>interfaceName - The <b>Port ID (port-id)</b> corresponds with the default name for a port (ifName) in the IF-MIB file</li> <li>agentCircuitId - The <b>Port ID (port-id)</b> corresponds with the Circuit ID for a port as defined by the DHCP agent</li> <li>local - The <b>Port ID (port-id)</b> is a value defined locally by the LLDP neighbor</li> </ul>
Management Address Subtype	<p><b>Synopsis:</b> [ other   ipv4   ipv6   nsap   hdhc   bbn1822   all802   e163   e164   f69   x121   ipx   appleTalk   decnetIV   banyanVines   e164withNsap   dns   distinguishedName   asNumber   xtpOverIpv4   xtpOverIpv6   xtpNativeModeXTP   fibreChannelWWPN   fibreChannelWWNN   gwid   afi   reserved ]</p> <p>The source of the <b>Management Address (man-address)</b> parameter as advertised by LLDP neighbor. Possible values include:</p> <ul style="list-style-type: none"> <li>other - The <b>Management Address (man-address)</b> is another, unspecified type of address</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• ipv4 - The <b>Management Address (man-address)</b> is an IPv4 address</li> <li>• ipv6 - The <b>Management Address (man-address)</b> is an IPv6 address</li> <li>• nsap - The <b>Management Address (man-address)</b> is an Network Service Access Point (NSAP) address</li> <li>• hdlc - The <b>Management Address (man-address)</b> is a High-level Link Control (HDLC) address</li> <li>• bbn1822 - The <b>Management Address (man-address)</b> is a numeric host address to be used in IMP-host exchanges</li> <li>• all802 - The <b>Management Address (man-address)</b> is an IEEE 802 address</li> <li>• e163 - The <b>Management Address (man-address)</b> is an E.163 telephone number</li> <li>• e164 - The <b>Management Address (man-address)</b> is an E.164 telephone number</li> <li>• f69 - The <b>Management Address (man-address)</b> is an F.69 telex number</li> <li>• x121 - The <b>Management Address (man-address)</b> is an X.121 address</li> <li>• ipx - The <b>Management Address (man-address)</b> is an IPX address</li> <li>• appleTalk - The <b>Management Address (man-address)</b> is an AppleTalk address</li> <li>• decnetIV - The <b>Management Address (man-address)</b> is a DECnet Phase IV address</li> <li>• banyanVines - The <b>Management Address (man-address)</b> is a VINES network address</li> <li>• e164withNsap - The <b>Management Address (man-address)</b> is a Network Service Access Point (NSAP)-encoded E.164 telephone number</li> <li>• dns - The <b>Management Address (man-address)</b> is a Domain Name Server (DNS) server</li> <li>• distinguishedName - The <b>Management Address (man-address)</b> is a Distinguished Name (DN) address</li> <li>• asNumber - The <b>Management Address (man-address)</b> is an Autonomous System Number (ASN)</li> <li>• xtpOverIpv4 - The <b>Management Address (man-address)</b> is an IPv4 address that uses Xpress Transport Protocol (XTP) instead of TCP</li> <li>• xtpOverIpv6 - The <b>Management Address (man-address)</b> is an IPv6 address that uses Xpress Transport Protocol (XTP) instead of TCP</li> <li>• xtpNativeModeXTP - The <b>Management Address (man-address)</b> is an Xpress Transport Protocol (XTP) address segment</li> <li>• fibreChannelWWPN - The <b>Management Address (man-address)</b> is an World Wide Port Name (WWPN)</li> <li>• fibreChannelWWNN - The <b>Management Address (man-address)</b> is an World Wide Node Name (WWNN)</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>gwid - The <b>Management Address (man-address)</b> is a Gateway Identifier (GWID)</li> <li>afi - The <b>Management Address (man-address)</b> is an Authority and Format Identifier (AFI)</li> <li>reserved - The <b>Management Address (man-address)</b> is a reserved IPv4 or IPv6 address</li> </ul>
Management Address Interface Subtype	<p><b>Synopsis:</b> [ unknown   ifIndex   systemPortNumber ]</p> <p>The source of the <b>Management Address Interface ID (man-address-if-id)</b> parameter as advertised by the LLDP neighbor. Possible values include:</p> <ul style="list-style-type: none"> <li>unknown - The <b>Management Address Interface ID (man-address-if-id)</b> is not known</li> <li>ifIndex - The <b>Management Address Interface ID (man-address-if-id)</b> corresponds with the indexed name for an interface (ifIndex) in the IF-MIB file</li> <li>systemPortNumber - The <b>Management Address Interface ID (man-address-if-id)</b> corresponds with a locally defined port number</li> </ul>
Timestamp of Last Change	<p><b>Synopsis:</b> A string</p> <p>The time at which the statistics for LLDP neighbors were last updated. Timestamps represent the amount of time elapsed since the device was powered on. Values are expressed in durations of years, months, weeks, days, hours, minutes, and/or seconds in ISO 8601 format (e.g. P1Y1M2W3DT2H3M30S represents 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30 seconds).</p>

### 14.1.5 Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, navigate to the **Port LLDP Stats** tab under **Layer 2 » Net Discovery**.

The table displays the following information:

Parameter	Description
Slot	<p><b>Synopsis:</b> [ ---   pm1   pm2   main   sm   lm1   lm2   lm3   lm4   lm5   lm6   swport   eth   serport   celport   wlanport   cm   em   trnk ]</p> <p>The slot number of the module that contains the port specified by the <b>Port (port)</b> parameter.</p>
Port	<p><b>Synopsis:</b> An integer between 1 and 16</p> <p>The port number as indicated on the front plate silkscreen of the module.</p> <p>The port is contained in the slot module specified by the <b>Slot (slot)</b> parameter.</p>
Frames Dropped	<p><b>Synopsis:</b> An integer between 0 and 4294967295</p> <p>The total number of incoming LLDP frames dropped by the port.</p>

Parameter	Description
Error Frames	<b>Synopsis:</b> An integer between 0 and 4294967295 The total number of incoming LLDP frames received on the port with detectable errors.
Frames In	<b>Synopsis:</b> An integer between 0 and 4294967295 The total number of incoming LLDP frames received on the port.
Frames Out	<b>Synopsis:</b> An integer between 0 and 4294967295 The total number of outgoing LLDP frames broadcast on the port.
Ageouts	<b>Synopsis:</b> An integer between 0 and 4294967295 The number of times that an LLDP neighbor has been dropped on the port because its time-to-live (TTL) value had been exhausted. TTL values are specified in the LLDP frames sent from the neighbor to the port.
TLVS Drops	<b>Synopsis:</b> An integer between 0 and 4294967295 The total number of TLVs discarded from LLDP frames received on the port.
TLVS Unknown	<b>Synopsis:</b> An integer between 0 and 4294967295 The total number of unrecognized TLVs in LLDP frames received on the port.

## 14.2 Managing SNMP

The Simple Network Management Protocol (SNMP) is used by network management systems and the devices they manage. It is used to report alarm conditions and other events that occur on the devices it manages.

In addition to SNMPv1 and SNMPv2, RUGGEDCOM ROX II also supports SNMPv3, which offers the following features:

- Provides the ability to send a notification of an event via *traps*. Traps are unacknowledged UDP messages and may be lost in transit.
- Provides the ability to notify via *informs*. Informs simply add acknowledgement to the trap process, resending the trap if it is not acknowledged in a timely fashion.
- Encrypts all data transmitted by scrambling the contents of each packet to prevent it from being seen by an unauthorized source. The AES CFB 128 and DES3 encryption protocols are supported.
- Authenticates all messages to verify they are from a valid source.
- Verifies the integrity of each message by making sure each packet has not been tampered with in-transit.

SNMPv3 also provides security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user

resides. A security level is a permitted level of security within a security model. A combination of a security model and security level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMP, note the following:

- each user belongs to a group
- a group defines the access policy for a set of users
- an access policy defines what SNMP objects can be accessed for: reading, writing and creating notifications
- a group determines the list of notifications its users can receive
- a group also defines the security model and security level for its users


For a list of supported SNMP MIBs, refer to "Supported MIBs" (Page 787).


For a list of supported SNMP traps, refer to "Standard SNMP Traps" (Page 849) and "Proprietary SNMP Traps" (Page 851).

### 14.2.1 Enabling and Configuring SNMP Sessions

To enable and configure SNMP sessions, do the following:

1. Navigate to the **Sessions** tab under **Administration » SNMP**.
2. Configure the following parameter(s):

 <b>NOTICE</b>
To generate all SNMP traffic for a specific interface, make sure the IP address for the desired interface is set for both the <b>Listen IP</b> and <b>Source IP for Traps</b> parameters.

 <b>NOTICE</b>
The <b>Authentication Failure Notification</b> parameter is used to notify users of generic authentication failures when the <b>Authentication Traps</b> parameter is enabled. For more information about SNMP notifications, refer to "Standard SNMP Traps" (Page 849) and "Proprietary SNMP Traps" (Page 851).

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables SNMP, making the device an SNMP agent.</p>
Listen IP	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> 0.0.0.0</p> <p>The IPv4 or IPv6 address to which SNMP requests are sent. The default value (i.e. 0.0.0.0) enables the device to receive SNMP requests via any IP address associated with the device.</p>

Parameter	Description
Listen Port	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p><b>Default:</b> 161</p> <p>The default port on which the SNMP agent will listen for SNMP requests. The port corresponds with the IP address specified by the <b>Listen IP (listen-ip)</b> parameter.</p>
Extra IP Ports	<p><b>Synopsis:</b> A string</p> <p>Additional IPv4 or IPv6 addresses and their associated ports on which the SNMP agent will listen for SNMP requests. IPv4 addresses and port numbers must be separated by a colon (e.g. 192.168.0.2:1). IPv6 addresses and port numbers must be separated by square brackets and a colon (e.g. [2001:db8:2728::2200]:1).</p> <p>If the <b>Listen IP (listen-ip)</b> parameter is set to a value other than 0.0.0.0, the port specified by the <b>Listen Port (port)</b> parameter must not be associated with any additional addresses.</p>
Maximum Number of SNMP Sessions	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 30</p> <p>The maximum number of concurrent SNMP sessions.</p>
SNMP Local Engine ID	<p><b>Synopsis:</b> A string</p> <p>The unique SNMP engine ID assigned to the SNMP agent. Options include either a blank value or an Engine ID consisting of 5 to 32 colon-separated octets (e.g. nn:nn:nn:nn:nn). Each octet is a 2-digit hexadecimal number. The default ID is the enterprise number of the device followed by its MAC address.</p> <p>The value of <b>Local SNMP Engine ID (snmp-engine-id)</b> must correspond with the value of <b>User SNMP Engine ID (id)</b>.</p>
Source IP for Traps	<p><b>Synopsis:</b> A string</p> <p>The source IP address for all notifications sent from the SNMP agent. The address may or may not belong to the device.</p>
Authentication Failure Notify Name	<p><b>Synopsis:</b> [ none   snmpv1_trap   snmpv2_trap   snmpv2_inform   snmpv3_trap   snmpv3_inform ]</p> <p><b>Default:</b> none</p> <p>The security model and notification type of the authenticationFailure notification, which the agent sends out when authentication fails. Options include:</p> <ul style="list-style-type: none"> <li>• none - The authenticationFailure notification is delivered to all management targets</li> <li>• snmpv1_trap - The authenticationFailure notification is delivered to management targets configured to receive SNMPv1 trap notifications</li> <li>• snmpv2_trap - The authenticationFailure notification is delivered to management targets configured to receive SNMPv2 trap notifications</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>snmpv2_inform - The authenticationFailure notification is delivered to management targets configured to receive SNMPv2 <b>inform</b> notifications</li> <li>snmpv3_trap - The authenticationFailure notification is delivered to management targets configured to receive SNMPv3 <b>trap</b> notifications</li> <li>snmpv3_inform - The authenticationFailure notification is delivered to management targets configured to receive SNMPv3 <b>inform</b> notifications</li> </ul>
Enabled Authentication Traps	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables the SNMP to send generic authentication traps.</p>
ROX Authentication Traps	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables/disables the SNMP to send detailed traps related to user authentication and password management.</p>
DSCP Value for SNMP Traffic	<p><b>Synopsis:</b> An integer between 0 and 63</p> <p><b>Default:</b> 0</p> <p>The priority level for traffic sent by the SNMP agent. Values must correspond with Differentiated Services Code Points (DSCPs), as described in RFC 2475.</p>

3. Commit the changes.

## 14.2.2 Viewing Statistics for SNMP

To view the statistics collected for SNMP, navigate to the **SNMP Statistics** tab under **Administration » SNMP**.

The table provides the following information:

Parameter	Description
Unsupported Security Levels	<p><b>Synopsis:</b> An integer</p> <p>The total number of incoming SNMP packets dropped because they requested an unknown or unavailable security level.</p>
Not In Time Windows	<p><b>Synopsis:</b> An integer</p> <p>The total number of incoming SNMP packets dropped because they were received after the authoritative SNMP engine's time out period expired.</p>
Unknown User Names	<p><b>Synopsis:</b> An integer</p> <p>The total number of incoming SNMP packets dropped because they referenced an unknown user.</p>

Parameter	Description
Unknown Engine IDs	<b>Synopsis:</b> An integer The total number of incoming SNMP packets dropped because they referenced an unknown SNMP Engine ID.
Wrong Digests	<b>Synopsis:</b> An integer The total number of incoming SNMP packets dropped because they contained an unexpected digest value (i.e. authentication key).
Decryption Errors	<b>Synopsis:</b> An integer The total number of incoming SNMP packets dropped because they could not be decrypted.

### 14.2.3 Discovering SNMP Engine IDs

To discover an ID of a remote SNMP protocol engine, do the following:

1. Navigate to the **SNMP Discover** tab under **Administration » SNMP**.
2. Under **Discover SNMP Engine ID**, click **Perform**.
3. Configure the following parameter(s) as required:

Parameter	Description
Address	<b>Synopsis:</b> A string between 7 and 15 characters long
SNMP Data Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 161 The SNMP data port the device listens on (if any).
SNMP Trap Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 162 The SNMP trap port the device listens on (if any).

4. Click **OK**.

Once discovered, the ID is displayed.

### 14.2.4 Managing SNMP Communities

This section describes how to manage SNMP communities.

#### 14.2.4.1 Viewing a List of SNMP Communities

To view a list of SNMP communities configured on the device, navigate to the **SNMP Community** tab under **Administration » SNMP**. A list appears.

By default, private and public communities are pre-configured. If additional communities are required, add them as needed. For more information, refer to "Adding an SNMP Community" (Page 708).

#### 14.2.4.2 Adding an SNMP Community

To add an SNMP community, do the following:

1. Navigate to the **SNMP Community** tab under **Administration » SNMP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Community Name	<b>Synopsis:</b> A string between 1 and 32 characters long The unique name for the SNMP community.

4. Click **OK** to create the community.
5. Configure the following parameter(s) as required:

Parameter	Description
Username	<b>Synopsis:</b> A string between 1 and 128 characters long The user name associated with the community string.

6. Commit the changes.

#### 14.2.4.3 Deleting an SNMP Community

To delete an SNMP community, do the following:

1. Navigate to the **SNMP Community** tab under **Administration » SNMP**.
2. Select the community to be deleted, and then click **Delete Entry**.
3. Commit the changes.

### 14.2.5 Managing SNMP Target Addresses

This section describes how to manage SNMP target addresses.

#### 14.2.5.1 Viewing a List of SNMP Target Addresses

To view a list of SNMP target addresses configured on the device, navigate to the **SNMP Target Address** tab under **Administration » SNMP**. If target addresses have been configured, a list appears.

If no SNMP target addresses have been configured, add target addresses as needed. For more information, refer to "Adding an SNMP Target Address" (Page 709).

### 14.2.5.2 Adding an SNMP Target Address

To add an SNMP target address, do the following:

1. Navigate to the **SNMP Community** tab under **Administration » SNMP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Target Name	<b>Synopsis:</b> A string between 1 and 32 characters long  The unique name for the SNMP target.

4. Click **OK** to create the protocol.
5. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> [ true   false ] <b>Default:</b> true  Enables/disables the SNMP agent to send traps to the SNMP target.
Target Address	<b>Synopsis:</b> A string  The IPv4 or IPv6 address for the SNMP target.
Trap Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 162  The UDP port on which the target will receive notifications. The trap port corresponds with the IP address specified by <b>Target Address (target-address)</b> .
Security Model	<b>Synopsis:</b> [ v1   v2c   v3 ] <b>Default:</b> v2c  The recognized security model of SNMP packets sent from the target. Options include: <ul style="list-style-type: none"> <li>• snmpv1 - Packets sent from the target use the SNMPv1 community-based security model.</li> <li>• snmpv2c - Packets sent from the target use the SNMPv2c community-based security model</li> <li>• snmpv3 - Packets sent from the target use the SNMPv3 user-based security model</li> </ul>



Parameter	Description
Username	<p><b>Synopsis:</b> A string between 1 and 128 characters long</p> <p>The recognized user name. Only this user name is permitted to exchange SNMP packets with the target.</p>
Security Level	<p><b>Synopsis:</b> [ noAuthNoPriv   authNoPriv   authPriv ]</p> <p><b>Default:</b> noAuthNoPriv</p> <p>The security level of SNMPv3 packets sent to or from the target. Options include:</p> <ul style="list-style-type: none"> <li>• authPriv - Users must be authenticated with a password in order to receive SNMPv3 packets sent from the target</li> <li>• authNoPriv - Users must be authenticated in order to receive SNMPv3 packets sent from the target. No password is required.</li> <li>• noAuthnoPriv - Users do not need to be authenticated to receive SNMPv3 packets sent from the target. No password is required.</li> </ul> <p><b>Security Model (security-model) must be set to snmpv3.</b></p>
Control Community	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p>Incoming SNMP requests from the specified community will be blocked. Values must correspond with preconfigured SNMPv1/v2c community names.</p>
Trap Type List	<p><b>Synopsis:</b> [ snmpv1_trap   snmpv2_trap   snmpv2_inform   snmpv3_trap   snmpv3_inform ]</p> <p><b>Default:</b> snmpv2_trap</p> <p>The types of notifications the target may receive. Options include:</p> <ul style="list-style-type: none"> <li>• snmpv1_trap - The target will receive <b>trap</b> notifications from SNMPv1 agents</li> <li>• snmpv2_trap - The target will receive <b>trap</b> notifications from SNMPv2c agents</li> <li>• snmpv2_inform - The target will receive and acknowledge <b>inform</b> notifications from SNMPv2c agents</li> <li>• snmpv3_trap - The target will receive <b>trap</b> notifications from SNMPv3 agents</li> <li>• snmpv3_inform - The target will receive and acknowledge <b>inform</b> notifications from SNMPv3 agents</li> </ul> <hr/> <p><b>Note</b></p> <p>Multiple options can be selected.</p>
Inform Timeout	<p><b>Synopsis:</b> An integer between 0 and 2147483647</p> <p><b>Default:</b> 6000</p> <p>The time in hectoseconds (hs or 100 s) the SNMP agent will wait for the target to acknowledge an inform notification. When this time expires, the SNMP agent will resend the notification until it is acknowledged.</p>

Parameter	Description
	The maximum number of attempts is defined by <b>Maximum Retries (inform-retries)</b> .
Inform Retries	<p><b>Synopsis:</b> An integer between 0 and 255</p> <p><b>Default:</b> 3</p> <p>The maximum number of times the agent will resend an unacknowledged inform notification. After this value is exceeded the SNMP session fails.</p>
Target Engine ID	<p><b>Synopsis:</b> A string</p> <p>The SNMP engine ID of the SNMP target. Options include either a blank value or an Engine ID consisting of 5 to 32 colon-separated octets (e.g. nn:nn:nn:nn:nn). Each octet is a 2-digit hexadecimal number.</p>

6. Commit the changes.

### 14.2.5.3 Deleting an SNMP Target Address

To delete an SNMP target address, do the following:

1. Navigate to the **SNMP Community** tab under **Administration » SNMP**.
2. Select the target address to be deleted, and then click **Delete Entry**.
3. Commit the changes.

## 14.2.6 Managing SNMP Users

This section describes how to manage SNMP users.

### 14.2.6.1 Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, navigate to the **SNMP User** tab under **Administration » SNMP**. If SNMP users have been configured, a list appears.

If no SNMP users have been configured, add users as needed. For more information, refer to "Adding an SNMP User" (Page 711).

### 14.2.6.2 Adding an SNMP User


To add an SNMP user, do the following:

1. Navigate to the **SNMP User** tab under **Administration » SNMP**.
2. Click **Add Entry**.

3. Configure the following parameter(s) as required:

Parameter	Description
User SNMP Engine ID	<p><b>Synopsis:</b> A string</p> <p>The unique SNMP engine ID assigned to the user. Engine IDs consist of 5 to 32 colon-separated octets (e.g. nn:nn:nn:nn:nn). Each octet is a 2-digit hexadecimal number. The default ID is the enterprise number of the device followed by its MAC address.</p> <p>The value of <b>Local SNMP Engine ID (snmp-engine-id)</b> must correspond with the value of <b>User SNMP Engine ID (id)</b>.</p>
Username	<p><b>Synopsis:</b> A string between 1 and 128 characters long</p> <p>The user name assigned to the user. The user can only communicate with SNMP targets that recognize their assigned user name.</p>

4. Click **OK** to create the protocol.

<p> <b>NOTICE</b></p> <p><b>Security hazard – risk of unauthorized access and/or exploitation</b></p> <p>Use only strong passwords when configuring SNMP users that consist of at least:</p> <ul style="list-style-type: none"> <li>• One lower case character</li> <li>• One upper case character</li> <li>• One number</li> <li>• One special character (i.e. !@#\$%^&amp;*()_+={}[];:’,&lt;.&gt;/? `~)</li> </ul> <p>Avoid weak passwords (e.g. <i>password1</i>, <i>123456789</i>, <i>abcdefgh</i>) or repeated characters (e.g. <i>abcabc</i>).</p>
---

5. Configure the following parameter(s) as required:

Parameter	Description
Authentication Protocol	<p><b>Synopsis:</b> [ none   md5   sha1 ]</p> <p><b>Default:</b> none</p> <p>The authentication method used for exchanges between the user and the SNMP engine. Options include:</p> <ul style="list-style-type: none"> <li>• none - Exchanges are not authenticated</li> <li>• md5 - The server uses the MD5 algorithm to authenticate exchanges</li> <li>• sha1 - The server uses the SHA-1 hash function to authenticate exchanges</li> </ul> <p>When md5 or sha1 is selected, <b>Authentication Key (auth-key)</b> must be defined.</p>

Parameter	Description
Authentication Key	<p><b>Synopsis:</b> A string at least 8 characters long</p> <p>The passphrase required to authenticate messages from the SNMP engine. The passphrase must be at least 8 characters long.</p> <p><b>Authentication Protocol (auth-protocol)</b> must be set to either md5 or sha1.</p>
Privacy Protocol	<p><b>Synopsis:</b> [ none   des3cbc   aescfb128 ]</p> <p><b>Default:</b> none</p> <p>The data encryption and decryption method for exchanges between the user and the SNMP engine. Options include:</p> <ul style="list-style-type: none"> <li>• none - Exchanges are not encrypted and decrypted</li> <li>• des3cbc - The server uses the 3DES-CBC algorithm to encrypt and decrypt exchanges</li> <li>• aescfb128 - The server uses the AES-CFB algorithm to encrypt and decrypt exchanges</li> </ul> <p>When des3cbc or aescfb128 is selected, <b>Privacy Key (privacy-key)</b> must be defined.</p>
Privacy Key	<p><b>Synopsis:</b> A string</p> <p>The privacy passphrase required to encrypt message to and decrypt messages from the SNMP engine. The passphrase must be at least 8 characters long.</p> <p><b>Privacy Protocol (privacy-protocol)</b> must be set to either des3cbc or aescfb128.</p>

6. Commit the changes.

### 14.2.6.3 Deleting an SNMP User

To delete an SNMP user, do the following:

1. Navigate to the **SNMP User** tab under **Administration » SNMP**.
2. Select the user to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 14.2.7 Managing SNMP Security Model Mapping

This section describes how to manage the mapping of SNMP security models.

### 14.2.7.1 Viewing a List of SNMP Security Models

To view a list of SNMP security models configured on the device, navigate to the **SNMP Security to Group** tab under **Administration » SNMP**. If security models have been configured, a list appears.

If no SNMP security models have been configured, add security models as needed. For more information, refer to "Adding an SNMP Security Model" (Page 714).

### 14.2.7.2 Adding an SNMP Security Model

To add an SNMP security model, do the following:

1. Navigate to the **SNMP Security to Group** tab under **Administration » SNMP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Security Model	<p><b>Synopsis:</b> [ v1   v2c   v3 ]</p> <p>The security model used by the SNMP group. Options include:</p> <ul style="list-style-type: none"> <li>• v1 - SNMPv1 users with the specified user name are mapped to the group</li> <li>• v2c - SNMPv2c users with the specified user name are mapped to the group</li> <li>• v3 - SNMPv3 users with the specified user name are mapped to the group</li> </ul>
Username	<p><b>Synopsis:</b> A string between 1 and 128 characters long</p> <p>The user name of the users to be mapped to the specified <b>Group (group)</b>.</p>

4. Click **OK** to create the protocol.
5. Configure the following parameter(s) as required:

Parameter	Description
Group	<p><b>Synopsis:</b> A string between 1 and 32 characters long</p> <p><b>Default:</b> all-rights</p> <p>The name of the group to which users with the specified <b>User Name (name)</b> that belong to the specified <b>Security Model (model)</b> will be mapped.</p>

6. Commit the changes.

### 14.2.7.3 Deleting an SNMP Security Model

To delete an SNMP security model, do the following:

1. Navigate to the **SNMP Security to Group** tab under **Administration » SNMP**.
2. Select the security model to be deleted then click **Delete Entry**.
3. Commit the changes.

## 14.2.8 Managing SNMP Group Access

This section describes how to manage access for SNMP groups.

### 14.2.8.1 Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, navigate to the **SNMP Access** tab under **Administration » SNMP**. If groups have been configured, a list appears.

If no SNMP groups have been configured, add groups as needed. For more information, refer to "Adding an SNMP Group" (Page 715).

### 14.2.8.2 Adding an SNMP Group

To add an SNMP group, do the following:

1. Navigate to the **SNMP Access** tab under **Administration » SNMP**.
2. Click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Group	<b>Synopsis:</b> A string between 1 and 32 characters long The unique name for the SNMP group.
Security Model	<b>Synopsis:</b> [ any   v1   v2c   v3 ] The SNMP security model to be used by group members. Options include: <ul style="list-style-type: none"> <li>• any - Members may belong to any SNMP security model</li> <li>• v1 - Members must be SNMPv1 users</li> <li>• v2c - Members must be SNMPv2c users</li> <li>• v3 - Members must be SNMPv3 users</li> </ul>
Security Level	<b>Synopsis:</b> [ noAuthNoPriv   authNoPriv   authPriv ] The SNMP security level for the group. Options include: <ul style="list-style-type: none"> <li>• authPriv: Members must be authenticated and encrypted to access the SNMP view(s) associated with the group</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>authNoPriv: Members must be authenticated to access the SNMP view(s) associated with the group. Encryption is not required.</li> <li>noAuthnoPriv: Members need neither be authenticated nor encrypted to access the SNMP view(s) associated with the group</li> </ul> <p>If the group includes SMPv1 or SMPv2c users, the <b>Security Level (level)</b> parameter must be set to noAuthnoPriv.</p>

- Click **OK** to create the protocol.
- Configure the following parameter(s) as required:

Parameter	Description
Read View Name	<p><b>Synopsis:</b> [ no-view   v1-mib   restricted   all-of-mib ]</p> <p><b>Default:</b> all-of-mib</p> <p>The read view to which members of the SNMP group have access. Options include:</p> <ul style="list-style-type: none"> <li>all-of-mib - Group members can view all objects in the MIB</li> <li>restricted - Group members can view only the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtrees in the MIB</li> <li>v1-mib - Group members can view only SNMPv1 objects in the MIB</li> <li>no-view - Group members cannot view any object in the MIB</li> </ul>
Write View Name	<p><b>Synopsis:</b> [ no-view   v1-mib   restricted   all-of-mib ]</p> <p><b>Default:</b> all-of-mib</p> <p>The write view to which members of the SNMP group have access. Options include:</p> <ul style="list-style-type: none"> <li>all-of-mib - Group members can make changes to all objects in the MIB</li> <li>restricted - Group members can make changes to only the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtrees in the MIB</li> <li>v1-mib - Group members can make changes to only SNMPv1 objects in the MIB</li> <li>no-view - Group members cannot make changes to any object in the MIB</li> </ul>
Notify View Name	<p><b>Synopsis:</b> [ no-view   v1-mib   restricted   all-of-mib ]</p> <p><b>Default:</b> all-of-mib</p> <p>The notify view to which members of the SNMP group have access. Options include:</p> <ul style="list-style-type: none"> <li>all-of-mib - Group members receive notifications from all objects in the MIB</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>restricted - Group members receive notifications from only the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtrees in the MIB</li> <li>v1-mib - Group members receive notifications from only SNMPv1 objects in the MIB</li> <li>no-view - Group members do not receive any notifications from the MIB</li> </ul>

6. Commit the changes.

### 14.2.8.3 Deleting an SNMP Group

To delete an SNMP group, do the following:

1. Navigate to the **SNMP Access** tab under **Administration » SNMP**.
2. Select the group to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 14.3 Managing NETCONF

The Network Configuration Protocol (NETCONF) is a network configuration protocol developed by the Internet Engineering Task Force (IETF). NETCONF provides functions to download, upload, change, and delete the configuration data on network devices. RUGGEDCOM ROX II devices also support the ability to collect data and perform direct actions on the device, such as rebooting the device, clearing statistics, and restarting services.

### Note

For more information about NETCONF and its use, refer to the "NETCONF Reference Guide for RUGGEDCOM ROX II v2.16".

### 14.3.1 Enabling and Configuring NETCONF Sessions

To enable and configure NETCONF sessions, do the following:

1. Navigate to the **NETCONF Sessions** tab under **Administration » Session Config**, and then select **NETCONF**.

#### NOTICE

#### Security hazard – risk of unauthorized access/exploitation

Configure an idle timeout period for NETCONF to prevent unauthorized access (e.g. a user leaves their station unprotected) or denial of access (e.g. a guest



user blocks an admin user by opening the maximum number of NETCONF sessions).

**Note**

Before configuring an idle timeout on a device managed by RUGGEDCOM NMS, make sure NMS is configured to support a timeout period for NETCONF sessions.

2. Configure the following parameter(s):

Parameter	Description
Enabled	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> true</p> <p>Enables NETCONF on the device, allowing it to receive and respond to NETCONF requests.</p>
Listen IP	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> 0.0.0.0</p> <p>The IPv4 or IPv6 address on which the device will listen for NETCONF requests. The default value (i.e. 0.0.0.0) enables the device to receive NETCONF requests via any IP address associated with the device.</p>
Listen Port	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p><b>Default:</b> 830</p> <p>The default port on which the device will listen for NETCONF requests. The port corresponds with the IP address specified by the <b>Listen IP (listen-ip)</b> parameter.</p>
Extra IP Ports	<p><b>Synopsis:</b> A string</p> <p>Additional IPv4 or IPv6 addresses and their associated ports on which the device will listen for NETCONF requests. IPv4 addresses and port numbers must be separated by a colon (e.g. 192.168.0.2:19343). IPv6 addresses and port numbers must be separated by square brackets and a colon (e.g. [2001:db8:2728::2200]:[19343]).</p> <p>If the <b>Listen IP (listen-ip)</b> parameter is set to a value other than "0.0.0.0," the port specified by the <b>Listen Port (port)</b> parameter must not be associated with any additional addresses.</p>
Maximum Number of NETCONF Sessions	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 10</p> <p>The maximum number of concurrent NETCONF sessions.</p>
Idle Timeout	<p><b>Synopsis:</b> A string</p> <p><b>Default:</b> PT0S</p> <p>The maximum period of time a NETCONF session will remain idle before being terminated. Values are expressed in durations of years, months, weeks, days, hours, minutes, and/or seconds in ISO 8601 format (e.g. P1Y1M2W3DT2H3M30S represents 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30</p>

Parameter	Description
	seconds). If the value is set to 0, a NETCONF session will never time out.  A session is not considered idle if the NETCONF server is waiting for notifications or if commits are pending. If the value of this parameter is changed during a session, the change will not take effect until the next session

3. Commit the changes.
4. [Optional] Enable the NETCONF summary log (saved under `/var/log/netconf.log`) to record all NETCONF protocol transactions. For more information, refer to "Enabling/Disabling the NETCONF Summary Log" (Page 70).
5. [Optional] Enable the NETCONF trace log (saved under `/var/log/netconf-trace.log`) to record the text of each NETCONF XML message received by and sent by the device. For more information, refer to "Enabling/Disabling the NETCONF Trace Log" (Page 70).

## 14.3.2 Viewing NETCONF Statistics

To view NETCONF related statistics, navigate to the **NETCONF Sessions** tab under **Administration » Session Config**, and then select **NETCONF State/Statistics**.

The following information is provided:

Parameter	Description
In Bad Hellos	<b>Synopsis:</b> An integer  The total number of NETCONF sessions dropped because the device received an invalid hello message. Errors in nested elements and/or attributes can invalidate a hello message.
In Sessions	<b>Synopsis:</b> An integer  The total number of NETCONF sessions initiated on the device.
Dropped Sessions	<b>Synopsis:</b> An integer  The total number of NETCONF sessions dropped on the device.
In RPCs	<b>Synopsis:</b> An integer  The total number of NETCONF requests (i.e. rpc messages) received.
In Bad RPCs	<b>Synopsis:</b> An integer  The total number of NETCONF requests (i.e. rpc messages) dropped because they contained non-conformant XML.
Out RPC Errors	<b>Synopsis:</b> An integer  The total number of NETCONF replies (i.e. rpc-reply messages) sent with a nested rpc-error element. The rpc-error element indicates to

Parameter	Description
	a client that one or more errors occurred in processing its NETCONF request (i.e. rpc message).
Out Notifications	<b>Synopsis:</b> An integer  The total number of notification messages sent.

## 14.4 Managing IPv4 Neighbors

RUGGEDCOM ROX II supports Address Resolution Protocol (ARP) tables for individual Layer 3 interfaces.

### 14.4.1 IPv4 Neighbor Concepts

An IPv4 neighbor is any host on the same local area network connected to the device via Ethernet cables or network switches. For the device to forward traffic to an IPv4 neighbor, it must know the host's IP address and physical address, or Media Access Control (MAC) address.

This information is collected separately for each Layer 3 interface in a dedicated ARP table (or cache) for quick IP address resolution.

Hosts communicate their IP and MAC addresses through ARP request and ARP response messages. When an interface has traffic to forward and the destination cannot be found in the ARP table, the device broadcasts an ARP request message to hosts on its local network. The host that matches the request responds with an ARP response message, which includes its MAC address and IP address. This information is then added to the interface's ARP table for future reference.

Host information is retained for each Layer 3 interface, unless explicitly cleared. Users have the option to clear select entries per interface.

### 14.4.2 Viewing IPv4 Neighbors

An ARP table (or cache) of IPv4 neighbor information is available for a Layer 3 interface if IPv4 neighbors are discovered.

To view the state of IPv4 neighbors for a Layer 3 interface, do the following:

1. Navigate to the **Interface** tab under **Interface » IP Interfaces**, and then select **Interface**.
2. Select an interface, and then select the **IPv4 Neighbors** tab.

### IPv4 Neighbor Information

The ARP table details the following for each entry:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string The IP address of the neighbor.
Neighbor MAC Address	<b>Synopsis:</b> A string The MAC address of the neighbor.
Neighbor State	<b>Synopsis:</b> A string The state of the neighbor. Possible values include: <ul style="list-style-type: none"> <li>• <b>permanent</b> – The entry is valid and permanent. Entries in this state must be cleared by a user.</li> <li>• <b>noarp</b> – The entry is valid, but no attempt to validate the entry will be made. It can be removed when its lifetime has expired.</li> <li>• <b>reachable</b> – The entry is valid until the reachability timeout expires.</li> <li>• <b>stale</b> – The entry is valid, but suspicious.</li> <li>• <b>incomplete</b> – The entry is not yet validated/resolved.</li> <li>• <b>delay</b> – Validation of the entry is delayed.</li> <li>• <b>probe</b> – The neighbor is being probed.</li> <li>• <b>failed</b> – The maximum number of probes has been exceeded and neighbor verification has failed.</li> </ul>

### 14.4.3 Clearing IPv4 Neighbors

Select IPv4 neighbors can be cleared from the ARP tables.

To clear an entry from the cache for a Layer 3 interface, do the following:

1. Navigate to the **Interface** tab under **Interface » IP Interfaces**, and then select **Interface**.
2. Select an interface, and then select the **IPv4 Neighbors** tab.
3. Select the IPv4 neighbor to be cleared, and then click **Clear**.



## Traffic Control and Classification

Use the traffic control and classification subsystems to control the flow of data packets to connected network interfaces. RUGGEDCOM ROX II also features tools for traffic analysis and characterization.

### 15.1 Managing Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to another mirror port. If a protocol analyzer were attached to the target port, the traffic stream of valid frames on any source port is made available for analysis.

Select a target port that has a higher speed than the source port. Mirroring a 100 Mbps port onto a 10 Mbps port may result in an improperly mirrored stream.

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port's transmission rate. This problem reaches its extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.

Invalid frames received on the source port will not be mirrored. These include CRC errors, oversized and undersized packets, fragments, jabbers, collisions, late collisions and dropped events).

---

#### Note

Port mirroring has the following limitations:

- The target port may sometimes incorrectly show the VLAN tagged/untagged format of the mirrored frames.
  - Network management frames (such as RSTP, GVRP, etc. ) may not be mirrored.
  - Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) may not be mirrored.
- 

#### 15.1.1 Configuring Port Mirroring

To configure port mirroring, do the following:

1. Navigate to **Layer 2 » Port Mirroring**.

**Note**

Mirror ports allow bidirectional traffic (i.e. the device will not block incoming traffic to the mirror port or ports). This can lead to traffic being forwarded to unintended ports. For increased security, configure ingress filtering to control traffic flow when port mirroring is enabled.

For information about configuring the device to control traffic flow when port mirroring is enabled, refer to the FAQ "How to Control Bidirectional Traffic when Using Port Mirroring" (<https://support.industry.siemens.com/cs/ww/en/view/109759351>).

For more information about enabling ingress filtering, refer to "Enabling/Disabling Ingress Filtering" (Page 319).

2. Configure the following parameter(s) as required:

Parameter	Description
Target Port	The interface where a monitoring device should be connected.
Admin State	Enabling port mirroring causes all frames received and/or transmitted by the source port to be transmitted out of the target port.

3. Add egress and ingress source ports. For more information, refer to "Adding an Egress Source Port" (Page 725) and "Adding an Ingress Source Port" (Page 725).
4. Commit the changes.

## 15.1.2 Managing Egress Source Ports

This section describes how to configure and manage egress source ports for port mirroring.

### 15.1.2.1 Viewing a List of Egress Source Ports

To view a list of egress source ports for port mirroring, navigate to **Layer 2 » Port Mirroring**. If source ports have been configured, a list appears under **Egress Source Ports**.

If no egress source ports have been configured, add egress source ports as needed. For more information, refer to "Adding an Egress Source Port" (Page 725).

### 15.1.2.2 Adding an Egress Source Port

To add an egress source port for port mirroring, do the following:

1. Navigate to **Layer 2 » Port Mirroring**.
2. Under **Egress Source Ports**, select the port(s) to be added from the multiple-selection list box.
3. Commit the changes.

### 15.1.2.3 Deleting an Egress Source Port

To delete an egress source port for port mirroring, do the following:

1. Navigate to **Layer 2 » Port Mirroring**.
2. Under **Egress Source Ports**, click the X beside the source port to be deleted.
3. Commit the change.

## 15.1.3 Managing Ingress Source Ports

This section describes how to configure and manage ingress source ports for port mirroring.

### 15.1.3.1 Viewing a List of Ingress Source Ports

To view a list of ingress source ports for port mirroring, navigate to **Layer 2 » Port Mirroring**. If source ports have been configured, a list appears under **Ingress Source Ports**.

If no ingress source ports have been configured, add ingress source ports as needed. For more information, refer to "Adding an Ingress Source Port" (Page 725).

### 15.1.3.2 Adding an Ingress Source Port

To add an ingress source port for port mirroring, do the following:

1. Navigate to **Layer 2 » Port Mirroring**.
2. Under **Ingress Source Ports**, select the port(s) to be added from the multiple-selection list box.
3. Commit the changes.



### 15.1.3.3 Deleting an Ingress Source Port

To delete an ingress source port for port mirroring, do the following:

1. Navigate to **Layer 2 » Port Mirroring**.
2. Under **Ingress Source Ports**, click the X beside the source port to be deleted.
3. Commit the change.

## 15.2 Managing Traffic Control

Traffic control is a firewall subsystem that manages the amount of bandwidth for each network interface that different types of traffic are permitted to use. For a traffic control configuration to work, a firewall must be configured.

---

### Note

For more information about firewalls, refer to "Managing Firewalls" (Page 195).

---

RUGGEDCOM ROX II allows up to four different firewall configurations, enabling users to quickly change between configurations. Users can quickly assess different configurations without needing to save and reload any part of the configuration. In contrast, there is only one traffic control configuration.

When enabled, a traffic control configuration is used with the current firewall configuration. A current firewall configuration is defined as one that is specified in either work-config and/or active-config. It does not have to be enabled to be validated.

---

### Note

Traffic control is not available for Ethernet traffic on any line module when Layer 3 hardware acceleration is enabled. It is intended to be used only on WAN interfaces.

---

### 15.2.1 Enabling and Configuring Traffic Control

Traffic control functions are divided into two modes:

- **Basic Mode**  
Basic mode offers a limited set of options and parameters. Use this mode to set the outgoing bandwidth for an interface, the interface priority (high, medium or low), and some simple traffic control characteristics. Basic traffic shaping affects traffic identified by protocol, port number, address and interface. Note that some of these options are mutually exclusive. Refer to the information given for each option.

In basic mode, a packet is categorized based on the contents of its Type of Service (ToS) field if it does not match any of the defined classes.

- **Advanced Mode**

In advanced mode, each interface to be managed is assigned a total bandwidth for incoming and outgoing traffic. Classes are then defined for each interface, each with its own minimum assured bandwidth and a maximum permitted bandwidth. The combined minimum of the classes on an interface must be no more than the total outbound bandwidth specified for the interface. Each class is also assigned a priority, and any bandwidth left over after each class has received its minimum allocation (if needed) will be allocated to the lowest priority class up until it reaches its maximum bandwidth, after which the next priority is allocated more bandwidth. When the specified total bandwidth for the interface is reached, no further packets are sent, and any further packets may be dropped if the interface queues are full.

Packets are assigned to classes on the outbound interface based on either a mark assigned to the packet, or the Type of Service (ToS) field in the IP header. If the ToS field matches a defined class, the packet is allocated to that class. Otherwise, it is allocated to any class that matches the mark assigned to the packet. If no class matches the mark, the packet is assigned to the default class.

Marks are assigned to packets by traffic control rules that are based on a number of parameters, such as IP address, port number, protocol, packet length, and more.

The two modes cannot be accessed simultaneously. Only the mode that is currently configured can be accessed.

To enable and configure traffic control, do the following:

1. Navigate to the **Traffic Control** tab under **QoS**.

---

**Note**

A firewall must be enabled before enabling traffic control configuration.

For more information, refer to "Enabling/Disabling a Firewall" (Page 219).

---

2. Configure the following parameter(s) as required:

Parameter	Description
Enable Configuration	Enables/disables traffic control (TC) for the current firewall configuration. The current firewall configuration is the one that is committed. When an active configuration is committed to the system, then an <b>enabled</b> TC configuration will be included. When a work configuration is committed, the <b>enabled</b> TC configuration will be included in the work configuration. <b>A TC configuration needs a firewall configuration to operate.</b>
Basic or Advanced Configuration Mode	<b>Synopsis:</b> [ basic   advanced ] <b>Default:</b> basic  Choose to use either 'simple' or 'advanced' configuration modes. Click again on traffic-control after making a choice.

3. If basic mode is enabled, do the following:

- a. Add traffic control interfaces. For more information, refer to "Adding a Traffic Control Interface" (Page 728).
- b. Add traffic control priorities. For more information, refer to "Adding a Traffic Control Priority" (Page 730).
4. If advanced mode is enabled, do the following:
  - a. Add traffic control classes. For more information, refer to "Adding a Traffic Control Class" (Page 732).
  - b. Add traffic control devices. For more information, refer to "Adding a Traffic Control Device" (Page 735).
  - c. Add traffic control rules. For more information, refer to "Adding a Traffic Control Rule" (Page 737).
5. Commit the changes.

## 15.2.2 Managing Traffic Control Interfaces

Traffic control interfaces define interfaces used for traffic shaping, mainly for outbound bandwidth and the outgoing device.

---

### Note

Traffic control interfaces can only be configured in basic mode. For more information about setting the traffic control mode, refer to "Enabling and Configuring Traffic Control" (Page 726).

---

### 15.2.2.1 Viewing a List of Traffic Control Interfaces

To view a list of traffic control interfaces, do the following:

1. Navigate to the **Basic Configurations** tab under **QoS**.
2. Select **TC Interfaces**. If interfaces have been configured, a list appears.

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Traffic Control Interface" (Page 728).

### 15.2.2.2 Adding a Traffic Control Interface

To add a new traffic control interface, do the following:

1. Navigate to the **Basic Configurations** tab under **QoS**.
2. Select **TC Interfaces**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Interface	<p><b>Synopsis:</b> A string between 1 and 15 characters long</p> <p>An interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.</p>

4. Click **OK** to create the new traffic control interface.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<p><b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ]</p> <p><b>Default:</b> ipv4</p> <p>The type of traffic accepted by the interface. Traffic not accepted will be routed to another interface. Select 'ipv4ipv6' to accept all traffic regardless of IP type.</p>
Type	<p><b>Synopsis:</b> [ internal   external   none ]</p> <p><b>Default:</b> none</p> <p>(optional) 'external' (facing toward the Internet) or 'internal' (facing toward a local network). 'external' causes the traffic generated by each unique source IP address to be treated as a single flow. 'internal' causes the traffic generated by each unique destination IP address to be treated as a single flow. Internal interfaces seldom benefit from simple traffic shaping.</p>
Ingress Speed (numerical value only)	<p><b>Synopsis:</b> An integer</p> <p>(optional) The incoming bandwidth of this interface. If incoming traffic exceeds the given rate, received packets are dropped randomly. When unspecified, maximum speed is assumed. Specify only the number here. The unit (kilobits, megabits) is specified in the in-unit.</p>
Unit for Ingress Speed	<p><b>Synopsis:</b> [ none   kilobits   megabits ]</p> <p><b>Default:</b> none</p> <p>The unit for inbandwidth, per second.</p>
Egress Speed (numerical value only)	<p><b>Synopsis:</b> An integer</p> <p>The outgoing bandwidth for this interface. Specify only the number here. The unit (kilobits, megabits) is specified in the out-unit.</p>
Unit for egress speed	<p><b>Synopsis:</b> [ kilobits   megabits ]</p> <p><b>Default:</b> megabits</p> <p>The unit for outgoing bandwidth, per second.</p>
Description	<p><b>Synopsis:</b> A string</p> <p>A description for this configuration item.</p>

6. Commit the changes.

### 15.2.2.3 Deleting a Traffic Control Interface

To delete a traffic control interface, do the following:

1. Navigate to the **Basic Configurations** tab under **QoS**.
2. Select **TC Interfaces**.
3. Select the traffic control interface to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 15.2.3 Managing Traffic Control Priorities

Traffic control priorities define priorities used for traffic shaping.

---

### Note

Traffic control priorities can only be configured in basic mode. For more information about setting the traffic control mode, refer to "Enabling and Configuring Traffic Control" (Page 726).

---

### 15.2.3.1 Viewing a List of Traffic Control Priorities

To view a list of traffic control interfaces, do the following:

1. Navigate to the **Basic Configurations** tab under **QoS**.
2. Select **TC Priorities**. If priorities have been configured, a list appears.

If no priorities have been configured, add priorities as needed. For more information, refer to "Adding a Traffic Control Priority" (Page 730).

### 15.2.3.2 Adding a Traffic Control Priority

To add a new traffic control priority, do the following:

1. Navigate to the **Basic Configurations** tab under **QoS**.
2. Select **TC Priorities**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string A distinct name for this configuration entry.

4. Click **OK** to create the new traffic control priority.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<p><b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ]</p> <p><b>Default:</b> ipv4</p> <p>Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.</p>
Band	<p><b>Synopsis:</b> [ high   medium   low ]</p> <p><b>Default:</b> medium</p> <p>Priority (band) : high, medium, low... <b>High band includes:</b> Minimize Cost (md) (0x10), md + Minimize Monetary Cost (mmc) (0x12), md + Maximize Reliability (mr) (0x14), mmc+md+mr (0x16). <b>Medium band includes:</b> Normal Service (0x0), mr (0x04), mmc+mr (0x06), md + Maximize Throughput (mt) (0x18), mmc+mt+md (0x1a), mr+mt+md (0x1c), mmc+mr+mt+md (0x1e). <b>Low band includes:</b> mmc (0x02), mt (0x08), mmc+mt (0x0a), mr+mt (0x0c), mmc+mr+mt (0x0e).</p>
Protocol	<p><b>Synopsis:</b> A string or [ tcp   udp   icmp   all ]</p> <p>(choice) A targeted protocol.</p>
Port	<p><b>Synopsis:</b> A string</p> <p>(choice) Source port - can be specified <b>only if</b> protocol is TCP, UDP, DCCP, SCTP or UDPlite</p>
Address	<p><b>Synopsis:</b> A string</p> <p>(choice) The source address. This can be specified <b>only if</b> the protocol, port and interface are not defined.</p>
Interface	<p><b>Synopsis:</b> A string between 1 and 15 characters long</p> <p>(choice) The source interface. This can be specified <b>only if</b> the protocol, port and address are not defined. Lowercase alphanumeric as well as '.' and '-' characters are allowed.</p>
Description	<p><b>Synopsis:</b> A string</p> <p>(optional) A description for this configuration.</p>

6. Commit the changes.

### 15.2.3.3 Deleting a Traffic Control Priority

To delete a traffic control priority, do the following:

1. Navigate to the **Basic Configurations** tab under **QoS**.
2. Select **TC Priorities**.
3. Select the traffic control priority to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 15.2.4 Managing Traffic Control Classes

Traffic control classes define classes for traffic shaping. Optionally, they can also define parameters for Type of Service (ToS), which is an eight-bit field in the IPv4 header. Traffic control can inspect the ToS value of an incoming IP frame and classify traffic to provide preferential service in the outgoing queue. Traffic classification is done based on the ToS value and the ToS options defined for each traffic control class and traffic control rule. IP Traffic matching with the ToS options takes precedence over the mark rules.

---

### Note

One traffic control class must be added for each network interface.

---

### Note

Type of Service (ToS) is defined by the Internet Engineering Task Force (IETF). For more information about ToS, refer to [RFC 1349 \[http://tools.ietf.org/html/rfc1349\]](http://tools.ietf.org/html/rfc1349).

---

### 15.2.4.1 Viewing a List of Traffic Control Classes

To view a list of traffic control classes, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Control Classes**. If classes have been configured, a list appears.

If no classes have been configured, add classes as needed. For more information, refer to "Adding a Traffic Control Class" (Page 732).

### 15.2.4.2 Adding a Traffic Control Class

To add a new traffic control class, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Control Classes**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string The name for this TC class entry.

4. Click **OK** to create the new class.
5. Configure the following parameter(s) as required:

Parameter	Description
ToS Minimize Delay	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Value/mask encoding: 0x10/0x10</p>
ToS Maximize Throughput	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Value/mask encoding: 0x08/0x08</p>
ToS Maximize Reliability	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Value/mask encoding: 0x04/0x04</p>
ToS Minimize Cost	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Value/mask encoding: 0x02/0x02</p>
ToS Normal Service	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Value/mask encoding: 0x00/0x1e</p>
Default	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>One default class per interface must be defined.</p>
TCP Ack	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>All TCP ACK packets into this class. This option should be specified only once per interface.</p>
ToS Value	<p><b>Synopsis:</b> A string</p> <p>A custom classifier for the given value/mask. The values are hexadecimal, prefixed by '0x'. Ex.: 0x56[0x0F]</p>
IP Type	<p><b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ]</p> <p><b>Default:</b> ipv4</p> <p>Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.</p>
Interface	<p><b>Synopsis:</b> A string</p> <p>The interface to which this class applies. Each interface must be listed only once. Lowercase alphanumerical as well as '.' and '-' characters are allowed.</p>



Parameter	Description
Mark	<p><b>Synopsis:</b> An integer between 1 and 255</p> <p>A mark that identifies traffic belonging to this class. This is a unique integer between 1-255. Each class must have its own unique mark.</p>
Min-Bandwidth	<p><b>Synopsis:</b> A string</p> <p>The minimum bandwidth this class should have when the traffic load rises. This can be either a numeric value or a calculated expression based on the bandwidth of the interface. A fixed numerical value must only be a number - its unit is specified in Minbw-unit.</p> <p>A calculated expression is based on a fraction of the 'full' bandwidth, such as:</p> <ol style="list-style-type: none"> <li>'full/3' for a third of the bandwidth and</li> <li>'full*9/10' for nine tenths of the bandwidth.</li> </ol> <p>In such a case, do not specify any minbw-unit.</p>
Minbw-unit	<p><b>Synopsis:</b> [ none   kilobits   megabits ]</p> <p><b>Default:</b> none</p> <p>(per second) Only if the minimum bandwidth is a single numerical value</p>
Max-Bandwidth	<p><b>Synopsis:</b> A string</p> <p>The maximum bandwidth this class is allowed to use when the link is idle. This can be either a numeric value or a calculated expression based on the bandwidth of the interface. A fixed numerical value must only be a number - its unit is specified in Maxbw-unit.</p> <p>A calculated expression is based on a fraction of the 'full' bandwidth, such as:</p> <ol style="list-style-type: none"> <li>'full/3' for a third of the bandwidth and</li> <li>'full*9/10' for nine tenths of the bandwidth.</li> </ol> <p>In such a case, do not specify any maxbw-unit.</p>
Maxbw-unit	<p><b>Synopsis:</b> [ none   kilobits   megabits ]</p> <p><b>Default:</b> none</p> <p>(per second) only if max-bandwidth is a <b>single numerical value</b></p>
Priority	<p><b>Synopsis:</b> An integer between 0 and 7</p> <p><b>Default:</b> 0</p> <p>The priority in which classes will be serviced. Higher priority classes will experience less delay since they are serviced first. Priority values are serviced in ascending order (e.g. 0 is higher priority than 1. Minimum: 7).</p>
Description	<p><b>Synopsis:</b> A string</p> <p>A description for this configuration item.</p>

6. Commit the changes.

### 15.2.4.3 Deleting a Traffic Control Class

To delete a traffic control class, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Control Classes**.
3. Select the class to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 15.2.5 Managing Traffic Control Devices

Traffic control devices define devices used for traffic shaping.

---

### Note

Traffic control devices can only be configured in advanced mode. For more information about setting the traffic control mode, refer to "Enabling and Configuring Traffic Control" (Page 726).

---

### 15.2.5.1 Viewing a List of Traffic Control Devices

To view a list of traffic control devices, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Devices**. If devices have been configured, a list appears.

If no devices have been configured, add devices as needed. For more information, refer to "Adding a Traffic Control Device" (Page 735).

### 15.2.5.2 Adding a Traffic Control Device

To add a new traffic control device, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Devices**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Interface	<b>Synopsis:</b> A string between 1 and 15 characters long An interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.

4. Click **OK** to create the new traffic control device.
5. Configure the following parameter(s) as required:

Parameter	Description
In Bandwidth	<p><b>Synopsis:</b> An integer  <b>Default:</b> 0</p> <p>Incoming bandwidth. Default: 0 = ignore ingress. Defines the maximum traffic allowed for this interface in total. If the rate is exceeded, the packets are dropped.</p>
In Units	<p><b>Synopsis:</b> [ none   kilobits   megabits ]  <b>Default:</b> none</p> <p>Unit for inbandwidth, per second.</p>
Out Bandwidth	<p><b>Synopsis:</b> An integer</p> <p>Maximum outgoing bandwidth... This is the maximum speed that can be handled. Additional packets will be dropped. This is the bandwidth that can be referred-to as 'full' when defining classes.</p>
Out Units	<p><b>Synopsis:</b> [ kilobits   megabits ]  <b>Default:</b> megabits</p> <p>Unit for outgoing bandwidth, per second.</p>
Description	<p><b>Synopsis:</b> A string</p> <p>A description for this configuration item.</p>

6. Commit the changes.

### 15.2.5.3 Deleting a Traffic Control Device

To delete a traffic control device, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Devices**.
3. Select the traffic control device to be deleted, and then click **Delete Entry**.
4. Commit the change.

### 15.2.6 Managing Traffic Control Rules

Traffic control rules define rules for packet marking.

**Note**

Traffic control rules can only be configured in advanced mode. For more information about setting the traffic control mode, refer to "Enabling and Configuring Traffic Control" (Page 726).

**15.2.6.1 Viewing a List of Traffic Control Rules**

To view a list of traffic control rules, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Rules**. If rules have been configured, a list appears.

If no rules have been configured, add rules as needed. For more information, refer to "Adding a Traffic Control Rule" (Page 737).

**15.2.6.2 Adding a Traffic Control Rule**

To add a new traffic control rule, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Rules**, and then click **Add Entry**.
3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string A distinct name for this rule.

4. Click **OK** to create the new traffic control rule.
5. Configure the following parameter(s) as required:

Parameter	Description
IP Type	<b>Synopsis:</b> [ ipv4   ipv6   ipv4ipv6 ] <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Source	<b>Synopsis:</b> A string IF name, comma-separated list of hosts or IPs, MAC addresses, or 'all'. When using MAC addresses, use '~' as prefix and '-' as separator. Ex.: ~00-1a-6b-4a-72-34,~00-1a-6b-4a-71-42
Destination	<b>Synopsis:</b> A string IF name, comma-separated list of hosts or IPs, or 'all'.

Parameter	Description
Protocol	<p><b>Synopsis:</b> A string or [ tcp   udp   icmp   all ]</p> <p><b>Default:</b> all</p> <p>The protocol to match.</p>
Destination Ports	<p><b>Synopsis:</b> A string</p> <p>(Optional) A comma-separated list of port names, port numbers or port ranges.</p>
Source Ports	<p><b>Synopsis:</b> A string</p> <p>(Optional) A comma-separated list of port names, port numbers or port ranges.</p>
Test	<p><b>Synopsis:</b> A string</p> <p>Defines the test criteria for an existing packet or connection mark. The rule will match only if the test returns true.</p> <p>Define the test as follows: [ ! ]{ value }[ / { mask }][ :C ]</p> <p>! - Reverses the test</p> <p>value - The value of the packet or connection mark</p> <p>mask - A mask to be applied to the mark before testing</p> <p>:C - Designates a connection mark. If not present, the test is applied by default to a packet mark.</p> <p>Example:</p> <p>!0:C</p>
Length	<p><b>Synopsis:</b> A string</p> <p>(Optional) Matches the length of a packet against a specific value or range of values... Greater than and lesser than, as well as ranges are supported in the form of min:max. Ex.: Equal to 64 <b>64</b> Greater or equal to 65 <b>65:</b> Lesser or equal to 65 <b>:65</b> In-between 64 and 768 <b>64:768</b></p>
ToS	<p><b>Synopsis:</b> A string or [ minimize-delay   maximize-throughput   maximize-reliability   minimize-cost   normal-service ]</p> <p>(Optional) Type of Service . A pre-defined ToS value or a numerical value. The numerical value is hexadecimal. Ex.: 0x38</p>
Description	<p><b>Synopsis:</b> A string</p> <p>A description for this configuration item.</p>

**Note**

Only one QoS mark is allowed for each traffic control rule.

6. Configure the rules for a QoS mark. For more information, refer to "Configuring QoS Marking" (Page 739).
7. Commit the changes.

### 15.2.6.3 Configuring QoS Marking

Quality of Service (QoS) marking applies a mark to important data packets that should receive preferential treatment as they travel through the network. Only one QoS mark is allowed for each traffic control rule. Options include:

- **Set** – Determines whether the packet or the connection is assigned the QoS mark.
- **Modify** – Changes the QoS mark value using an AND or OR argument.
- **Save/Restore** – Replaces the connection's QoS mark value with an assigned value.
- **Continue** – If the packet matches, no more traffic control rules are checked and the packet is automatically forwarded to the specified chain.
- **DSCP Marking**: Determines whether the packet is assigned the DSCP mark.

To configure the QoS mark for a traffic control rule, do the following:

#### Configuring a Set Mark

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Rules**, and then select a traffic control rule.
3. In the **Mark Choice** column of the table, select **set** from the drop down list.
4. Under **Mark Choice-Set**, configure the following parameter(s) as required:

---

#### Note

The `chain-options` parameter specifies the chain in which the rule will be processed.

- **Pre-Routing - Mark the connection in the PREROUTING chain**  
This can be used with DNAT, SNAT and Masquerading rules in the firewall. An example of such a rule is *Source.IP:192.168.2.101, Chain-option: preroute or default*, but the actual Source.NAT address is 2.2.2.2.
  - **Post-Routing - Mark the connection in the POSTROUTING chain**  
This can be used with DNAT, SNAT and Masquerading rules in the firewall. An example of such rule is *Destination.IP:192.168.3.101, Chain-option: preroute or default*. In this case, the actual destination address is 192.168.3.101, but it will be translated to 192.168.3.33 by DNAT. Another example of a traffic control rule is *Destination.IP:192.168.3.33, Chain-option: postrouting*.
  - **Forward - Mark the connection in the FORWARD chain**  
This is the default chain option and it can be used for normal IP traffic without any address or port translation.
-

Parameter	Description
Object	<b>Synopsis:</b> [ packet   connection ] <b>Default:</b> packet Sets the mark on either a packet or a connection.
Mark	<b>Synopsis:</b> A string A mark that corresponds to a class mark (decimal value).
Mask	<b>Synopsis:</b> A string (optional) A mask to determine which mark bits will be set.
Chain Options	<b>Synopsis:</b> [ forward   postrouting   prerouting ] <b>Default:</b> forward A chain where the set operation will take place.

5. Commit the change.

### Configuring a Modify Mark

1. Select a traffic control rule.
2. In the **Mark Choice** column of the table, select **modify** from the drop down list.
3. Configure the following parameter(s) as required:

Parameter	Description
Logic Options	<b>Synopsis:</b> [ and   or ] A logical operation to perform on the current mark: AND/OR.
Mark Value	<b>Synopsis:</b> A string A mark to perform the operation with (decimal value).
Chain Options	<b>Synopsis:</b> [ forward   postrouting   prerouting ] <b>Default:</b> forward A chain in which the operation will take place.

4. Commit the change.

### Configuring a Save Mark

1. Select a traffic control rule.
2. In the **Mark Choice** column of the table, select **save** from the drop down list.
3. Configure the following parameter(s) as required:

Parameter	Description
Value Mask	<b>Synopsis:</b> A string Mask to process the mark with
Option Chain	<b>Synopsis:</b> [ forward   prerouting ] <b>Default:</b> forward A chain in which the operation will take place.

4. Commit the change.

### Configuring a Restore Mark

1. Select a traffic control rule.
2. In the **Mark Choice** column of the table, select **restore** from the drop down list.
3. Configure the following parameter(s) as required:

Parameter	Description
Value Mask	<b>Synopsis:</b> A string A mask to process the mark with.
Option Chain	<b>Synopsis:</b> [ forward   prerouting ] <b>Default:</b> forward A chain in which the operation will take place.

4. Commit the change.

### Configuring a Continue Mark

1. Select a traffic control rule.
2. In the **Mark Choice** column of the table, select **continue** from the drop down list.
3. Configure the following parameter(s) as required:

Parameter	Description
Continue Chain	<b>Synopsis:</b> [ forward   prerouting ] <b>Default:</b> forward A chain in which the operation will take place.

4. Commit the change.

### Configuring a DSCP Mark

1. Select a traffic control rule.



2. In the **Mark Choice** column of the table, select **dcsp marking** from the drop down list.
3. Configure the following parameter(s) as required:

Parameter	Description
DSCP Mark	<p><b>Synopsis:</b> [ BE   AF11   AF12   AF13   AF21   AF22   AF23   AF31   AF32   AF33   AF41   AF42   AF43   CS1   CS2   CS3   CS4   CS5   CS6   CS7   EF ]</p> <p>A DSCP class value chosen amongst the given list.</p>
DSCP Chain	<p><b>Synopsis:</b> [ forward   postrouting   prerouting ]</p> <p><b>Default:</b> forward</p> <p>A chain where the DSCP marking will take place.</p>

4. Commit the change.

#### 15.2.6.4 Deleting a Traffic Control Rule

To delete a traffic control rule, do the following:

1. Navigate to the **Advanced Configurations** tab under **QoS**.
2. Select **TC Rules**.
3. Select the traffic control rule to be deleted, and then click **Delete Entry**.
4. Commit the change.

### 15.2.7 Managing QoS Mapping for VLANs

Quality of Service (QoS) mapping is used to map QoS traffic. It assigns a traffic control mark to incoming IP traffic based on the priority value of a tagged frame. The incoming traffic is then classified and placed in the priority queues according to the traffic control rules specified for the marked rule. In addition, traffic control can assign the same priority or a different priority value when a frame needs to be egressed with a VLAN tag through a traffic control interface.

QoS maps can be configured for VLAN connections on routable Ethernet ports and virtual switches.

#### 15.2.7.1 Viewing a List of QoS Maps for VLANs

To view a list of QoS maps for a VLAN connection, navigate to either:

- **For Switched Ethernet Ports**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Switch VLANs**.
- **For Routable-Only Ethernet Ports**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Eth VLANs**.

- **For Virtual Switches**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Virtual Switch VLANs**.

If QoS maps have been configured, a list appears.

If no QoS maps have been configured, add maps as needed. For more information, refer to "Adding a QoS Map" (Page 743).

### 15.2.7.2 Adding a QoS Map

To add a QoS map for a VLAN connection, do the following:

1. In the case of a QoS map for a virtual switch, make sure the desired virtual switch has been configured. For more information, refer to "Adding a Virtual Switch" (Page 368).
2. Navigate to either:
  - **For Switched Ethernet Ports**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Switch VLANs**.
  - **For Routable-Only Ethernet Ports**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Eth VLANs**.
  - **For Virtual Switches**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Virtual Switch VLANs**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

Parameter	Description
QoS	<b>Synopsis:</b> An integer between 0 and 7  VLAN QoS, which is the priority in the VLAN header.

5. Click **OK** to create the new QoS Map.
6. Configure the following parameter(s) as required:

Parameter	Description
Ingress	<b>Synopsis:</b> An integer between 0 and 255  Map the ingress to a mark.

7. Add an egress mark for the QoS map. For more information, refer to "Adding an Egress Mark" (Page 745).
8. Commit the changes.

### 15.2.7.3 Deleting a QoS Map

To delete a QoS map for a VLAN connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Switched Ethernet Ports**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Switch VLANs**.
  - **For Routable-Only Ethernet Ports**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Eth VLANs**.
  - **For Virtual Switches**  
The **QoS Map** tab for the selected VLAN under **QoS » QoS Map » Virtual Switch VLANs**.
3. Select the QoS map to be deleted, and then click **Delete Entry**.
4. Commit the change.

## 15.2.8 Managing Egress Markers for QoS Maps

Egress markers for QoS maps are used to assign priority to traffic that shares the same mark as one of the egress marks configured for the device.

### 15.2.8.1 Viewing a List of Egress Marks

Users can view the egress marks for switched Ethernet ports, routable-only Ethernet ports, virtual switches, and WAN interfaces.

#### Switched Ethernet Ports

To view a list of egress marks for a QoS map for switched Ethernet ports, do the following:

1. Navigate to the **VLANs ID** tab under **QoS » QoS Map » Switch VLANs**, and then select a VLAN ID.
2. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**. If egress marks have been configured, a list appears.

#### Routable-Only Ethernet Ports

To view a list of egress marks for a QoS map for routable-only Ethernet ports, do the following:

1. Navigate to the **VLANs ID** tab under **QoS » QoS Map » Eth VLANs**, and then select a VLAN ID.

2. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**. If egress marks have been configured, a list appears.

## Virtual Switches

To view a list of egress marks for a QoS map for virtual switches, do the following:

1. Navigate to the **VLANS ID** tab under **QoS » QoS Map » Virtual Switch VLANs**, and then select a VLAN ID.
2. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**. If egress marks have been configured, a list appears.

If no egress marks have been configured, add egress marks as needed. For more information, refer to "Adding an Egress Mark" (Page 745).

### 15.2.8.2 Adding an Egress Mark

To add an egress mark for a QoS Map, do the following:

1. For Switched Ethernet Ports:
  - a. Navigate to the **VLANS ID** tab under **QoS » QoS Map » Switch VLANs**, and then select a VLAN ID.
  - b. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**.
2. For Routable-Only Ethernet Ports:
  - a. Navigate to the **VLANS ID** tab under **QoS » QoS Map » Eth VLANs**, and then select a VLAN ID.
  - b. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**.
3. For Virtual Switches:
  - a. Navigate to the **VLANS ID** tab under **QoS » QoS Map » Virtual Switch VLANs**, and then select a VLAN ID.
  - b. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**.
4. For WAN Interfaces:
  - a. Navigate to the **Slot/Port** tab under **Interface » WAN**, and then select an interface.
  - b. Under the **Parameters** tab, select a protocol, and then select the **Channel** tab.
  - c. Select a channel, and then click **hdlc-eth**.
  - d. Under **VLAN**, select a VLAN and then click the **QoS Map** tab.
5. Click **Add Entry**.
6. Configure the following parameter(s) as required:

Parameter	Description
Egress	<b>Synopsis:</b> An integer between 0 and 255 The mark value.

7. Click **OK** to create the new egress mark.
8. Commit the changes.

### 15.2.8.3 Deleting an Egress Mark

To delete an egress mark for a QoS map, do the following:

1. For Switched Ethernet Ports:
  - a. Navigate to the **VLANs ID** tab under **QoS » QoS Map » Switch VLANs**, and then select a VLAN ID.
  - b. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**.
2. For Routable-Only Ethernet Ports:
  - a. Navigate to the **VLANs ID** tab under **QoS » QoS Map » Eth VLANs**, and then select a VLAN ID.
  - b. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**.
3. For Virtual Switches:
  - a. Navigate to the **VLANs ID** tab under **QoS » QoS Map » Virtual Switch VLANs**, and then select a VLAN ID.
  - b. Select the **QoS Map** tab, select a QoS entry, and then click **Egress**.
4. For WAN Interfaces:
  - a. Navigate to the **Slot/Port** tab under **Interface » WAN**, and then select an interface.
  - b. Under the **Parameters** tab, select a protocol, and then select the **Channel** tab.
  - c. Select a channel, and then click **hdlc-eth**.
  - d. Under **VLAN**, select a VLAN and then click the **QoS Map** tab.
5. Select the egress mark to be deleted, and then click **Delete Entry**.
6. Commit the change.

## 15.2.9 Viewing QoS Statistics

RUGGEDCOM ROX II provides statistics for traffic going through each class that has been configured. Packets are assigned to classes on the outbound interface based on rules. If a packet matches the specified criteria, it is considered to be a member

of the class and is forwarded to that class. If the packet does not match any rule, it is forwarded to the default class.

For more information about traffic control classes, refer to "Managing Traffic Control Classes" (Page 732).

---

**Note**

Statistics are only available when traffic control is enabled in advanced mode. For more information about enabling traffic control, refer to "Enabling and Configuring Traffic Control" (Page 726).

---

To view the QoS statistics, navigate to the **Statistics** tab under **QoS**.

The following information is provided:

Parameter	Description
Min Bandwidth	<b>Synopsis:</b> A string The minimum guaranteed bandwidth. This is based on the device's defined characteristics.
Max Bandwidth	<b>Synopsis:</b> A string The maximum guaranteed bandwidth in absence of any higher prioritized traffic. This is based on the device's defined characteristics.
Sent Bytes	<b>Synopsis:</b> A string The number of bytes that were sent through this class.
Sent Packets	<b>Synopsis:</b> A string The number of packets that were sent through this class.
Dropped Packets	<b>Synopsis:</b> A string The number of packets that were dropped in this class.
Rate	<b>Synopsis:</b> A string Based on a 10-second average.
Average	<b>Synopsis:</b> A string Based on a 10-second average.

## 15.3 Managing Classes of Service

Classes of Service (CoS) provides the ability to expedite the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High or Critical. By default, RUGGEDCOM ROX II enforces Normal CoS for all traffic.

**⚠ NOTICE**

Use the highest supported CoS with caution, as it is always used by the switch for handling network management traffic, such as RSTP BPDUs.

If this CoS is used for regular network traffic, upon traffic bursts, it may result in the loss of some network management frames, which in turn may result in the loss of connectivity over the network.

The process of controlling traffic based on CoS occurs over two phases:

- **Inspection Phase**

In the inspection phase, the CoS priority of a received frame is determined from:

- A specific CoS based upon the source and destination MAC address (as set in the Static MAC Address Table)
- The priority field in 802.1Q tags
- The Differentiated Services Code Point (DSCP) component of the Type Of Service (TOS) field, if the frame is IP
- The default CoS for the port

Each frame's CoS will be determined once the first examined parameter is found in the frame.

Received frames are first examined to determine if their destination or source MAC address is found in the Static MAC Address Table. If they are, the CoS configured for the static MAC address is used. If neither destination or source MAC address is in the Static MAC Address Table, the frame is then examined for 802.1Q tags and the priority field is mapped to a CoS. If a tag is not present, the frame is examined to determine if it is an IP frame. If the frame is IP and inspecting TOS is enabled, the CoS is determined from the DSCP field. If the frame is not IP or inspecting TOS is disabled, the default CoS for the port is used.

After inspection, the frame is forwarded to the egress port for transmission.

- **Forwarding Phase**

Once the CoS of the frame is determined, the frame is forwarded to the egress port, where it is collected into one of the priority queues according to the assigned CoS.

CoS weighting selects the degree of preferential treatment that is attached to different priority queues. The ratio of the number of higher CoS to lower CoS frames transmitted can be configured. If desired, the user can configure lower CoS frames to be transmitted only after all higher CoS frames have been serviced.

## 15.3.1 Configuring Classes of Service

To configure Classes of Service, do the following:

1. Navigate to the **Global CoS** tab under **Layer 2 » CoS Mapping**.

2. Configure the following parameters as required:

Parameter	Description
CoS Weighting	<p><b>Synopsis:</b> [ 8421   strict ]</p> <p><b>Default:</b> 8421</p> <p>During traffic bursts, frames queued in the switch pending transmission on a port may have different Class of Service (CoS) priorities. This parameter specifies the weighting algorithm for transmitting different priority CoS frames.</p>

3. If necessary, configure CoS mapping based on either the IEEE 802.1p priority or Differentiated Services (DS) field set in the IP header for each packet. For more information, refer to "Adding a Priority-to-CoS Mapping Entry" (Page 749) or "Adding a DSCP-to-CoS Mapping Entry" (Page 750).
4. Commit the change.

## 15.3.2 Managing Priority-to-CoS Mapping

Assigning CoS to different IEEE 802.1p priority values in the frame is done by defining priority-to-CoS mapping table entries.

### 15.3.2.1 Viewing a List of Priority-to-CoS Mapping Entries

To view a list of priority-to-CoS mapping entries, navigate to the **Priority To CoS** tab under **Layer 2 » CoS Mapping**. If priorities have been configured, a list appears.

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Priority-to-CoS Mapping Entry" (Page 749).

### 15.3.2.2 Adding a Priority-to-CoS Mapping Entry


To add a priority-to-CoS mapping entry, do the following:

1. Navigate to the **Priority To CoS** tab under **Layer 2 » CoS Mapping**.
2. Click **Add Entry**, and then configure the following parameter(s) as required:

Parameter	Description
Priority	<p><b>Synopsis:</b> An integer between 0 and 7</p> <p>The value of the IEEE 802.1p priority.</p>

3. Click **OK** to add the priority
4. Configure the following parameter(s) as required:



 <b>NOTICE</b> Since RSTP BPDU's are sent through the critical CoS queue, take extra care when adding a priority with a CoS set to Critical.	
--	--

Parameter	Description
CoS	<b>Synopsis:</b> [ N/A   normal   medium   high   crit ] <b>Default:</b> normal The Class of Service (CoS) assigned to received tagged frames with the specified IEEE 802.1p priority value.

5. Commit the changes.

### 15.3.2.3 Deleting a Priority-to-CoS Mapping Entry

To delete a priority-to-CoS mapping entry, do the following:

---

**Note**

Deleting an entry sets the CoS to Normal.

---

1. Navigate to the **Priority To CoS** tab under **Layer 2 » CoS Mapping**.
2. Select the priority to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 15.3.3 Managing DSCP-to-CoS Mapping

Assigning CoS to different values of the Differentiated Services Code Point (DSCP) field in the IP header of received packets is done by defining DSCP-to-CoS mapping table entries.

### 15.3.3.1 Viewing a List of DSCP-to-CoS Mapping Entries

To view a list of DSCP-to-CoS mapping entries, navigate to the **DSCP To CoS** tab under **Layer 2 » CoS Mapping**. If DSCPs have been configured, a list appears.

If no entries have been configured, add entries as needed. For more information, refer to "Adding a DSCP-to-CoS Mapping Entry" (Page 750).

### 15.3.3.2 Adding a DSCP-to-CoS Mapping Entry

To add a DSCP-to-CoS mapping entry, do the following:

1. Navigate to the **DSCP To CoS** tab under **Layer 2 » CoS Mapping**.

- Click **Add Entry**, and then configure the following parameter(s) as required:

Parameter	Description
DSCP	<p><b>Synopsis:</b> An integer between 0 and 63</p> <p>The Differentiated Services Code Point (DSCP): a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header.</p>

- Click **OK** to add the DSCP.
- Configure the following parameter(s) as required:

Parameter	Description
CoS	<p><b>Synopsis:</b> [ N/A   normal   medium   high   crit ]</p> <p><b>Default:</b> normal</p> <p>The Class of Service (CoS) assigned to the received frames with the specified DSCP.</p>

- Configure the CoS parameters on select switched Ethernet ports and/or trunk interfaces as needed. For more information, refer to "Configuring a Switched Ethernet Port" (Page 276) and/or "Adding an Ethernet Trunk Interface" (Page 290).
- Commit the changes.

### 15.3.3.3 Deleting a DSCP-to-CoS Mapping Entry

To delete a DSCP-to-CoS mapping entry, do the following:

- Navigate to the **DSCP To CoS** tab under **Layer 2 » CoS Mapping**.
- Select the DSCP to be deleted, and then click **Delete Entry**.
- Commit the change.

## 15.4 Managing NetFlow Data Export

RUGGEDCOM ROX II supports the collection and forwarding of flow records to NetFlow-enabled servers, or NetFlow Collectors.

### NOTICE

NetFlow requires additional memory and CPU resources, which may affect device performance when network traffic is high. When enabled, general performance should be monitored to make sure traffic is processed optimally. If needed, NetFlow's resource requirements can be minimized by reducing the NetFlow cache. For more information, refer to "Controlling the NetFlow Cache" (Page 754).

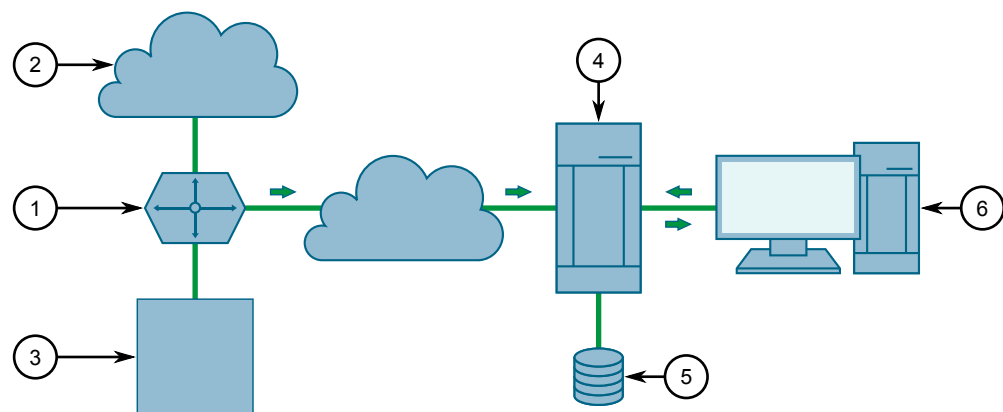
### 15.4.1 Understanding NetFlow Data Export

NetFlow is a traffic analysis tool developed by Cisco that allows network operators to characterize traffic flows across their networks. It provides information that allows operators to identify security vulnerabilities, assess network productivity and resource utilization, determine the causes of congestion, and more.

A basic NetFlow monitoring setup consists of the following components

- **Flow Exporter**  
The exporter aggregates data packets into flows, which are forwarded to one or more flow collectors.
- **Flow Collector**  
The collector receives, stores and pre-processes flow data received from one or more flow exporters.
- **Flow Analyzer**  
The flow analyzer queries one or more flow collectors for flow data and then analyzes the data with a focus on intrusion detection and traffic profiling.

RUGGEDCOM ROX II acts as a *flow exporter*, collecting data from ingress (incoming) and/or egress (outgoing) packets and then forwarding them as flow records to one or more collectors.



- ① NetFlow Exporter (RUGGEDCOM ROX II)
- ② WAN
- ③ LAN
- ④ NetFlow Collector
- ⑤ Flow Storage
- ⑥ Analysis Console

Figure 15.1 NetFlow

#### Note

RUGGEDCOM ROX II supports NetFlow version 5.

### 15.4.1.1 Flow Records

A flow record, as defined by the Cisco standard, is a unidirectional sequence of packets that share the same:

- Ingress interface
- Source and destination IP address
- IP protocol
- Source and destination port for TCP and UDP
- Type of Service (ToS)

Each flow record is exported using the User Datagram Protocol (UDP), which requires each packet to include the IP address of the target NetFlow collector and its designated UDP port.

A flow record is considered ready to export when either of the following conditions are met:

- The flow has been inactive (e.g. no new packets) for a specific period of time
- The flow has been active for longer than allowed by the configuration
- A TCP flag indicates the flow has been terminated

RUGGEDCOM ROX II includes user-configurable timers for inactive and active flows.

---

#### Note

RUGGEDCOM ROX II does not retain a record of flows sent. Therefore, any NetFlow packets dropped due to congestion or packet corruption will be lost permanently.

---

## 15.4.2 Configuring NetFlow Data Export

To configure the device to send flows to a NetFlow collector, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

 <b>NOTICE</b>
---

NetFlow does not support Layer 3 switching functions. Layer 3 switching must be disabled before NetFlow is enabled.
---

2. Make sure Layer 3 switching is disabled by setting the following parameters under **switch » layer3-switching** to **disabled**:

- **Unicast Mode**
- **Multicast Mode**

For more information, refer to "Configuring Layer 3 Switching" (Page 329).

3. Enable the NetFlow service. For more information, refer to "Enabling/Disabling NetFlow" (Page 754).

4. [Optional] Set the engine ID that is assigned to each flow record. For more information, refer to "Setting the NetFlow Engine ID" (Page 754).
5. [Optional] Set the maximum number of active flows tracked by the device. This can help improve performance in some scenarios. For more information, refer to "Controlling the NetFlow Cache" (Page 754).
6. [Optional] Control how RUGGEDCOM ROX II manages active and inactive flows. For more information, refer to "Controlling Active/Inactive Flows" (Page 755).
7. Define one or more interfaces from which to monitor traffic. For more information, refer to "Adding a NetFlow Interface" (Page 756).
8. Define one or more NetFlow collectors to which RUGGEDCOM ROX II can send flows. For more information, refer to "Adding a NetFlow Collector" (Page 757).

### 15.4.3 Enabling/Disabling NetFlow

To enable or disable NetFlow, do the following:

1. Navigate to the **Netflow Parameters** tab under **Layer 3 » Netflow**.
2. Under **NetFlow**, do one of the following:
  - Select **Enabled** to enable NetFlow
  - Clear **Enabled** to disable NetFlow
3. Commit the change.

### 15.4.4 Setting the NetFlow Engine ID

An engine ID can be assigned to flow records to uniquely link them to the device from which they were sent. This can be useful information to network analysts wishing to further categorize NetFlow data by device, region, etc.

The engine ID is defined in the header of the data export.

To set an engine ID for the device, do the following:

1. Navigate to the **Netflow Parameters** tab under **Layer 3 » Netflow**.
2. Under **Engine ID**, enter a number.
3. Commit the change.

### 15.4.5 Controlling the NetFlow Cache

NetFlow consumes memory and CPU resources during operation, which may affect the performance of the device during times of high traffic. To reduce NetFlow's effect on performance, consider reducing the number of active flows tracked by NetFlow. This will reduce the cache and free resources for other processes.

To control the NetFlow cache, do the following:

1. Navigate to the **Netflow Parameters** tab under **Layer 3 » Netflow**.
2. Configure the following parameter:

Parameter	Description
Maximum Flows	<p><b>Synopsis:</b> An integer</p> <p><b>Default:</b> 16384</p> <p>The maximum number of active flows tracked by NetFlow.</p>

3. Commit the change.

## 15.4.6 Controlling Active/Inactive Flows

NetFlow considers a flow to be ready for export when it has been inactive for a specific period of time or the flow has been active (long lived) for too long. By default, a flow is considered inactive if no new packets have been received for 15 seconds. An active flow is considered ready if it has received packets for longer than 30 minutes. Both durations can be adjusted to reduce or increase either the size of the NetFlow packets and/or the speed at which they are delivered.

To control how RUGGEDCOM ROX II manages active and inactive flows, do the following:

1. Navigate to the **Netflow Parameters** tab under **Layer 3 » Netflow**.
2. Configure the following parameters:

Parameter	Description
Active Timeouts	<p><b>Synopsis:</b> An integer equal to or greater than 1</p> <p><b>Default:</b> 1800</p> <p>The time in seconds (s) an active flow remains active.</p>
Inactive Timeout	<p><b>Synopsis:</b> An integer equal to or greater than 1</p> <p><b>Default:</b> 15</p> <p>The time in seconds (s) an inactive flow remains in the cache before it is deleted.</p>

3. Commit the changes.

## 15.4.7 Managing NetFlow Interfaces

RUGGEDCOM ROX II requires an interface from which to collect NetFlow data, but can be configured to monitor multiple interfaces if needed. Each interface can be configured to monitor packets entering (ingress) and/or exiting (egress).

---

**Note**

RUGGEDCOM ROX II does not support Netflow data collection on hardware-accelerated interfaces.

---

#### 15.4.7.1 Viewing a List of NetFlow Interfaces

To view a list of interfaces configured to monitor traffic for NetFlow, navigate to the **Interface** tab under **Layer 3 » Netflow**. If interfaces have been configured, a list appears.

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a NetFlow Interface" (Page 756).

#### 15.4.7.2 Adding a NetFlow Interface

To add a NetFlow interface, do the following:

1. Navigate to the **Interface** tab under **Layer 3 » Netflow**.
2. Click **Add Entry**.
3. Under **Interface Name**, select the desired interface and then click **OK**.
4. In the **Direction** column of the table, select the direction of traffic to be monitored. Options include:
  - **ingress** – Only traffic entering through the interface is monitored
  - **egress** – Only traffic exiting through the interface is monitored
  - **both** – All traffic traversing the interface is monitored
5. Commit the changes.

#### 15.4.7.3 Deleting a NetFlow Interface

To delete a NetFlow interface, do the following:

1. Navigate to the **Interface** tab under **Layer 3 » Netflow**.
2. Select the NetFlow interface to be deleted, and then click **Delete Entry**.
3. Commit the change.

### 15.4.8 Managing NetFlow Collectors

RUGGEDCOM ROX II can be configured to forward flows to up to four NetFlow collectors.

### 15.4.8.1 Viewing a List of NetFlow Collectors

To view a list of NetFlow collectors the device can send flows, navigate to the **Collector** tab under **Layer 3 » Netflow**. If collectors have been configured, a list appears.

If no collectors have been configured, add collectors as needed. For more information, refer to "Adding a NetFlow Collector" (Page 757).

### 15.4.8.2 Adding a NetFlow Collector

To define a NetFlow collector to which RUGGEDCOM ROX II will send flows, do the following:

1. Navigate to the **Collector** tab under **Layer 3 » Netflow**.
2. Click **Add Entry**, and then configure the following parameters:

---

**Note**

A single server can host multiple NetFlow collectors, each monitoring a specific UDP port.

---

Parameter	Description
IP Address	<b>Synopsis:</b> A string The IP address of the NetFlow collector.
Port	<b>Synopsis:</b> An integer between 0 and 65535 The UDP port used by the NetFlow Collector to receive messages.

3. Click **OK**.
4. [Optional] Enable the collector so RUGGEDCOM ROX II can forward NetFlow packets to it. For more information, refer to "Enabling/Disabling a NetFlow Collector" (Page 757).
5. Commit the change.

### 15.4.8.3 Enabling/Disabling a NetFlow Collector

To enable or disable a NetFlow collector defined in RUGGEDCOM ROX II, do the following:

1. Navigate to the **Collector** tab under **Layer 3 » Netflow**.
2. Select a collector.
3. Under **Collector**, do one for the following:
  - Select **Enabled** to enable the collector
  - Clear **Enabled** to disable the collector



4. Commit the change.

#### 15.4.8.4 Deleting a NetFlow Collector

To delete a NetFlow collector, do the following:

1. Navigate to the **Collector** tab under **Layer 3 » Netflow**.
2. Select the NetFlow collector to be deleted, and then click **Delete Entry**.
3. Commit the change.

#### 15.4.9 Viewing the Status of NetFlow

To view the status of NetFlow, navigate to the **Status** tab under **Layer 3 » Netflow**.

The following information is provided:

Parameter	Description
Active Flows	<b>Synopsis:</b> An integer The total number of active flows.
Bits/s	<b>Synopsis:</b> An integer The current rate in bits/s.
Packets/s	<b>Synopsis:</b> An integer The current rate in packets/s.
Minute Average Bits/s	<b>Synopsis:</b> An integer The average rate in bits/s over a minute.
Minute Average Packets/s	<b>Synopsis:</b> An integer The average rate in packets/s over a minute.

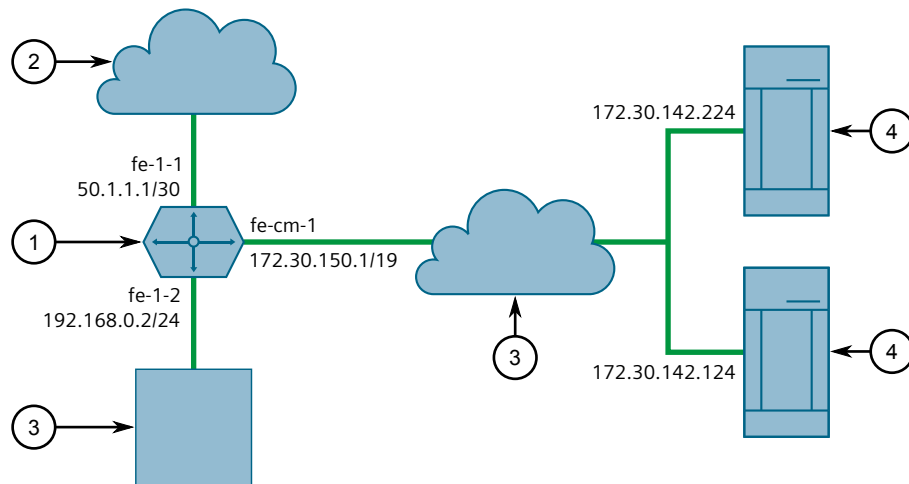
#### 15.4.10 Example: Exporting Flows to Multiple Collectors

This example describes how to configure RUGGEDCOM ROX II to forward NetFlow data to two NetFlow collectors.

In the following topology, the NetFlow exporter (RUGGEDCOM ROX II) is collecting data on packets traversing two interfaces. Packets sharing the same characteristics (i.e. source, destination, port, etc.) are placed into flows. When each flow is either deemed inactive, has exceeded the active timer, or is flagged as terminated, the exporter forwards the flow to the specified collectors.

**Note**

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.



- ① NetFlow Exporter (RUGGEDCOM ROX II)
- ② WAN
- ③ LAN
- ④ NetFlow Collector

Figure 15.2 Topology – Exporting Data to Multiple Collectors

**Configuration**

To configure RUGGEDCOM ROX II to export NetFlow packets to two NetFlow collectors, do the following:

1. Make sure Layer 3 switching is disabled by setting the following parameters under *switch » layer3-switching* to **disabled**:
  - **Unicast Mode**
  - **Multicast Mode**
 For more information, refer to "Configuring Layer 3 Switching" (Page 329).
2. Enable NetFlow. For more information, refer to "Enabling/Disabling NetFlow" (Page 754).
3. Define two NetFlow collectors and make sure they are both enabled. For more information, refer to "Adding a NetFlow Collector" (Page 757).
4. Define the interface that will be monitored by NetFlow. For more information, refer to "Adding a NetFlow Interface" (Page 756).
5. Send traffic to the interface monitored by RUGGEDCOM ROX II.
6. Verify the NetFlow collectors are receiving flows from the device.

## Final Configuration Example

```

services
netflow
  enabled
  engine-id 10
  timeouts active-timeout 1800
  timeouts inactive-timeout 15
  collector 172.30.142.124 2
    enabled
  !
  collector 172.30.142.224 1
    enabled
  !
  interface fe-1-1
  !
!
!
!
!

```

## 15.5 Managing Port Rate Limiting

This section describes how to manage port rate limiting.

### 15.5.1 Understanding Port Rate Limiting

Rate limiting restricts the bandwidth for a specific interface. The restriction can be applied to ingress and/or egress traffic, and to a specific type of traffic (e.g. unicast, multicast, broadcast, etc.). In some applications, controlling bandwidth may be required to maintain quality of service.

Rate limiting also provides a layer of defense against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks exhaust network resources by flooding a device with requests.

### 15.5.2 Configuring Port Rate Limiting

To configure port rate limiting, do the following:

1. Navigate to the **Port Rate Limiting** tab under **Interface » Switch Ports**.
2. Select an interface.
3. Configure the following parameter(s) as required:

Parameter	Description
Ingress Limit	<p><b>Synopsis:</b> An integer between 62 and 256000 or [ disabled ]</p> <p><b>Default:</b> 1000</p> <p>The data rate in kbps at which received frames (of the type described by the ingress frames parameter) will start to be discarded by the switch. The valid range is 62 to 256000 kbps. The default value is 1000 kbps. If not set(cleared), this feature is disabled.</p>

Parameter	Description
Ingress Frames	<p><b>Synopsis:</b> [ broadcast   multicast   mcast-flood-ucast   all ]</p> <p><b>Default:</b> broadcast</p> <p>This parameter specifies the types of frames to rate-limit on this port. It applies only to received frames:</p> <ul style="list-style-type: none"> <li>• BROADCAST : only broadcast frames will be limited.</li> <li>• MULTICAST : all multicast frames (including broadcast) will be limited.</li> <li>• MCAST-FLOOD-UCAST : all multicast frames (including broadcast) will be limited. Unicast will not be limited.</li> <li>• ALL : all frames (both multicast and unicast) will be limited.</li> </ul>
Egress Limit	<p><b>Synopsis:</b> [ disabled ] or An integer between 62 and 256000</p> <p><b>Default:</b> disabled</p> <p>The maximum data rate in kbps at which the switch will transmit (multicast, broadcast and unicast) frames on this port. The switch will discard frames in order to meet this rate if required. The valid range is 62 to 256000 Kbps. If not set, this feature is disabled.</p>

4. Commit the change.



## Time Services

RUGGEDCOM ROX II offers the following time-keeping and time synchronization features:

- Local hardware time keeping and time zone management
- NTP (Network Time Protocol) client and server

### 16.1 Configuring the Time Synchronization Settings

To configure the time synchronization settings, do the following:

1. Configure the system time and date. For more information, refer to "Configuring the System Time and Date" (Page 764).
2. Configure the system time zone. For more information, refer to "Configuring the System Time Zone" (Page 764).
3. Configure the local time settings. For more information, refer to "Configuring the Local Time Settings" (Page 764).
4. If multicast addresses will be configured for the NTP server, enable and configure the NTP multicast client. For more information, refer to "Enabling and Configuring NTP Multicast Clients" (Page 773).
5. If broadcast addresses will be configured for the NTP server, enable and configure the NTP broadcast client. For more information, refer to "Enabling and Configuring NTP Broadcast Clients" (Page 774).
6. Add remote NTP servers. For more information, refer to "Adding an NTP Server" (Page 769).
7. Add broadcast/multicast addresses for the NTP server. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 775).
8. If required, add server authentication keys. For more information, refer to "Adding a Server Key" (Page 771).
9. Add restrictions for the remote NTP servers. For more information, refer to "Adding a Server Restriction" (Page 772).
10. Enable and configure the NTP service. For more information, refer to "Enabling and Configuring the NTP Service" (Page 765).
11. View the status of the NTP service. For more information, refer to "Viewing the NTP Service Status" (Page 766).

## 16.2 Configuring the System Time and Date

To configure the system time and date, do the following:

1. Navigate to the **General** tab under **Administration » System » Time**.
2. Under **Set New Time and Date**, click **Perform** and configure the following parameter(s) as required:

Parameter	Description
Time	<b>Synopsis:</b> A string between 1 and 19 characters long Enter the date and time in the format YYYY-MM-DD HH:MM:SS.

3. Commit the change.

## 16.3 Configuring the System Time Zone

To configure the system time zone, do the following:

1. Navigate to the **General** tab under **Administration » System » Time**.
2. Under **Timezone**, configure the following parameter(s) as required:

Parameter	Description
Timezone	<b>Synopsis:</b> A string  The time zone in which the device resides. Note that UTC/GMT time zones conform to the POSIX style and have their signs reversed from common usage. In POSIX style, zones west of the GMT zone have a negative sign, while zones east of the GMT zone have a positive sign.

3. Commit the change.

## 16.4 Configuring the Local Time Settings

The local time settings configure the local clock on the device as the NTP time source.

To configure the local NTP time settings, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **General**.
2. Under **Local Time Settings**, Configure the following parameter(s) as required:

Parameter	Description
Enable Local Clock	Enables the local clock. The NTP daemon will use the local clock as the NTP source. The stratum number (of 10) indicates the priority relative to other sources.

Parameter	Description
Stratum	<p><b>Synopsis:</b> An integer between 0 and 15</p> <p><b>Default:</b> 10</p> <p>The stratum number of the local clock.</p>

3. Commit the changes.

## 16.5 Enabling and Configuring the NTP Service

To enable and configure the NTP service, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **General**.

### Note

RUGGEDCOM ROX II supports both IPv4 and IPv6 addresses.

### Note

Only a bind interface or a bind IP address can be selected/defined for NTP.

2. Select a bind interface or define a bind IP address.

Parameter	Description
Enable NTP Service	<p><b>Synopsis:</b> [ true   false ]</p> <p><b>Default:</b> false</p> <p>Enables NTP service.</p>
Bind Interface	<p><b>Synopsis:</b> A string</p> <p>Sets the primary/first IP address for the selected interface as the source IP address for outgoing NTP messages. Make sure an IP address is first assigned to the selected interface. The dummy0 interface should be used, unless required otherwise.</p> <p>If the bind interface is down, the source IP address for traffic transmitted by NTP will be the IP address of another egress interface.</p>
Bind IP Address	<p><b>Synopsis:</b> A string</p> <p>The defined IP address is used as the source IP address for all outgoing NTP messages.</p> <p>Make sure the IP address is statically defined for an interface. If the IP address is not assigned to an interface, the source IP address for traffic transmitted by NTP will be the IP address of the egress interface.</p>

3. Select the **Enable NTP Service** check box to enable the NTP service, or clear the check box to disable the service.



4. Commit the change.

## 16.6 Viewing the NTP Service Status

To view the status of the NTP service, do the following:

1. Make sure the NTP service is enabled. For more information, refer to "Enabling and Configuring the NTP Service" (Page 765).
2. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **General**.

The following information is provided under NTP Status:

Parameter	Description
Remote	<b>Synopsis:</b> A string up to 40 characters long Remote address.
Reference ID	<b>Synopsis:</b> A string up to 40 characters long The identification of the reference clock.
Stratum	<b>Synopsis:</b> A string up to 32 characters long The stratum number of the reference clock.
Address Type	<b>Synopsis:</b> A string up to 32 characters long The address type of the remote machine.
When	<b>Synopsis:</b> A string up to 32 characters long The number of seconds since the last poll of the reference clock.
Poll	<b>Synopsis:</b> A string up to 32 characters long The polling interval in seconds.
Reach	<b>Synopsis:</b> A string up to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
Delay	<b>Synopsis:</b> A string up to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
Offset	<b>Synopsis:</b> A string up to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
Jitter	<b>Synopsis:</b> A string up to 32 characters long The observed jitter (in milliseconds).

A character before an address is referred to as a tally code. Tally codes indicate the fate of the peer in the clock selection process. The following describes the meaning of each tally code:

Tally Code	Description
blank	A blank tally code indicates the peer has been discarded either because it is unreachable, it is synchronized to the same server (synch loop) or the synchronization distance is too far.
x	This tally code indicates the peer has been discarded because its clock is not correct. This is referred to as a <i>false ticker</i> .
.	This tally code indicates the peer has been discarded because its synchronization distance is too poor to be considered a candidate.
-	This tally code indicates the peer has been discarded because its offset is too a significant compared to the other peers. This is referred to as an <i>outlier</i> .
+	This tally code indicates the peer is considered a candidate.
#	This tally code indicates the peer is considered a candidate, but it is not among the top six sorted by synchronization distance. If the association is short-lived, it may be demobilized to conserve resources.
*	This tally code indicates the peer is the system peer.
o	This tally code indicates the peer is the system peer, but the synchronization distance is derived from a Pulse-Per-Second (PPS) signal.

## 16.7 Viewing the Status of Reference Clocks

To view the status of reference clocks, navigate to the **NTP** tab under **Administration » System » Time**, and then click **Reference Clock Status**.

The following information is provided:

Parameter	Description
Address	<b>Synopsis:</b> A string up to 40 characters long The IP address of the reference clock.
State	<b>Synopsis:</b> A string up to 32 characters long The state of the clock.
Reference ID	<b>Synopsis:</b> A string up to 40 characters long The identification of the reference clock.
Stratum	<b>Synopsis:</b> A string up to 32 characters long The stratum number of the reference clock.
Address Type	<b>Synopsis:</b> A string up to 32 characters long The address type of the remote machine.
When	<b>Synopsis:</b> A string up to 32 characters long The number of seconds since the last poll of the reference clock.

Parameter	Description
Poll	<b>Synopsis:</b> A string up to 32 characters long The polling interval in seconds.
Reach	<b>Synopsis:</b> A string up to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.

## 16.8 Managing NTP Servers

RUGGEDCOM ROX II can periodically refer to a remote NTP server to correct any accumulated drift in the onboard clock. RUGGEDCOM ROX II can also serve time via SNTP (Simple Network Time Protocol) to hosts that request it.

NTP servers can be added with or without authentication keys. To associate an authentication key with an NTP server, first define a server key. For information about adding server keys, refer to "Adding a Server Key" (Page 771).

### 16.8.1 Viewing a List of NTP Servers

To view a list of NTP servers configured on the device, navigate to the **NTP** tab under **Administration » System » Time**, and then click **Server**. If servers have been configured, a list appears.

If no servers have been configured, add servers as needed. For more information, refer to "Adding an NTP Server" (Page 769).

### 16.8.2 Monitoring Subscribers

RUGGEDCOM ROX II monitors the subscriptions of up to 600 hosts (e.g. clients, servers and peers) that are connected to the NTP server.

To view the list of subscriber hosts, navigate to the **NTP** tab under **Administration » System » Time**, and then click **Monitor List Status**.

The table/list provides the following information:

Parameter	Description
Remote	<b>Synopsis:</b> A string up to 40 characters long Remote address.
Port	<b>Synopsis:</b> An integer UDP port number.

Parameter	Description
Count	<b>Synopsis:</b> An integer Number of packets received.
Mode	<b>Synopsis:</b> An integer Mode of last packet.
Version	<b>Synopsis:</b> An integer Version of last packet.
Restrict	<b>Synopsis:</b> [ ignore   kod   limited   lowpriortrap   nomodify   nopeer   noquery   noserve   notrap   notrust   ntpport   version ] Restrict flags.
Average Interval	<b>Synopsis:</b> An integer Average interval (in seconds) between packets from this address.
Last Interval	<b>Synopsis:</b> An integer Interval (in seconds) between the receipt of the most recent packet from this address and the completion of the retrieval of the status.

### 16.8.3 Adding an NTP Server

To configure an NTP server on the device, do the following:

1. [Optional] If the communications with the server are to be authenticated, add a server authentication key or make sure the required key has been configured. For more information, refer to "Managing Server Keys" (Page 770).
2. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Server**.
3. Click **Add Entry**, and then configure the following parameter(s) as required:

#### Note

RUGGEDCOM ROX II supports both IPv4 and IPv6 addresses.

Parameter	Description
NTP Server	<b>Synopsis:</b> A string between 1 and 253 characters long The Internet address of the remote NTP server to be monitored.

4. Click **OK** to create the server configuration.
5. Configure the following parameter(s) as required:

Parameter	Description
Enabled	Turns on the NTP interface to this server.

Parameter	Description
Peer	Allows you to enter and edit peers. Peers are NTP servers of the same stratum as the router, and are useful when contact is lost with the hosts in the NTP servers menu.
Min Poll	<b>Synopsis:</b> An integer between 4 and 17 <b>Default:</b> 6 The minimum poll interval for NTP messages, in seconds as a power of two.
Max Poll	<b>Synopsis:</b> An integer between 4 and 17 <b>Default:</b> 10 The maximum poll interval for NTP messages, in seconds as a power of two.
Iburst	When the server is unreachable and at each poll interval, a burst of eight packets is sent instead of one.
NTP Version	<b>Synopsis:</b> An integer between 1 and 4 The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
Prefer	Marks this server as preferred.
Key	<b>Synopsis:</b> An integer equal to or greater than 1 An authentication key associated with this host.

6. [Optional] Set restrictions to control which NTP services can be accessed on the server. For more information, refer to "Adding a Server Restriction" (Page 772).
7. Commit the changes.

## 16.8.4 Deleting an NTP Server

To delete an NTP server configured on the device, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Server**.
2. Select the server to be deleted, and then click **Delete Entry**.
3. Commit the changes.

## 16.8.5 Managing Server Keys

Server keys are used to authenticate NTP communications and prevent tampering with NTP timestamps. When using authentication, both the local and remote servers must share the same key and key identifier. Packets sent to and received from the server/peer include authentication fields encrypted using the key.

### 16.8.5.1 Viewing a List of Server Keys

To view a list of server keys, navigate to the **NTP** tab under **Administration » System » Time**, and then click **Key**. If keys have been configured, a list appears.

If no server keys have been configured, add keys as needed. For more information, refer to "Adding a Server Key" (Page 771).

### 16.8.5.2 Adding a Server Key

To add a server key, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Key**.
2. Click **Add Entry**, and then configure the following parameter(s) as required:

Parameter	Description
Key ID	<b>Synopsis:</b> An integer equal to or greater than 1 The name of the key.

3. Click **OK** to create the new key.
4. Configure the following parameter(s) as required:

Parameter	Description
Key	<b>Synopsis:</b> A string between 1 and 1024 characters long The key.
Trusted	Mark this key as trusted for the purposes of authenticating peers with symmetric key cryptography. The authentication procedures require that both the local and remote servers share the same key and key identifier.

5. Commit the changes.

### 16.8.5.3 Deleting a Server Key

To delete a server key, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Key**.
2. Select the key to be deleted, and then click **Delete Entry**.

## 16.8.6 Managing Server Restrictions

Server restrictions control access to the NTP servers.

### 16.8.6.1 Viewing a List of Server Restrictions

To view a list of NTP server restrictions, navigate to the **NTP** tab under **Administration » System » Time**, and then click **Restrict**. If restrictions have been configured, a list appears.

If no server restrictions have been configured, add restrictions as needed. For more information, refer to "Adding a Server Restriction" (Page 772).

### 16.8.6.2 Adding a Server Restriction

To add an NTP server restriction, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Restrict**.
2. Click **Add Entry**, and then configure the following parameter(s) as required:

Parameter	Description
Address	<p><b>Synopsis:</b> A string between 1 and 253 characters long or [ default ]</p> <p>The address to match. The address can be a host or network IP address or a valid host DNS name.</p>
Mask	<p><b>Synopsis:</b> A string or [ default ]</p> <p>The mask used to match the address. Mask 255.255.255.255 means the address is treated as the address of an individual host.</p>

3. Click **OK** to create the new restriction.
4. Configure the following parameter(s) as required:

#### NOTICE

#### Security hazard – risk of unauthorized access and/or exploitation

It is recommended to restrict queries via ntpdc and ntpq, unless the queries come from a local host, or to disable this feature entirely if not required. This prevents DDoS (Distributed Denial of Service) reflection/amplification attacks. Configure the following flags to the restrict default entry: **kod**, **nomodify**, **nopeer**, **noquery** and **notrap**.

Parameter	Description
Flags	<p><b>Synopsis:</b> [ ignore   kod   limited   lowpriortrap   nomodify   nopeer   noquery   noserve   notrap   notrust   ntpport   version ]</p> <p>Flags restrict access to NTP services. An entry with no flags allows free access to the NTP server.</p> <ul style="list-style-type: none"> <li>• Version: Denies packets that do not match the current NTP version.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• ntpport: Matches only if the source port in the packet is the standard NTP UDP port (123).</li> <li>• notrust: Denies service unless the packet is cryptographically authenticated.</li> <li>• notrap: Declines to provide mode 6 control message trap service to matching hosts.</li> <li>• noserve: Denies all packets except ntpq(8) and ntpdc(8) queries.</li> <li>• noquery: Denies ntpq(8) and ntpdc(8) queries.</li> <li>• nopeer: Denies packets which result in mobilizing a new association.</li> <li>• nomodify: Denies ntpq(8) and ntpdc(8) queries attempting to modify the state of the server; queries returning information are permitted.</li> <li>• lowpriortrap: Declares traps set by matching hosts to be low priority.</li> <li>• limited: Denies service if the packet spacing violates the lower limits specified in the NTP discard setting.</li> <li>• kod: Sends a Kiss-o'-Death (KoD) packet when an access violation occurs.</li> <li>• ignore: Denies all packets.</li> </ul>

5. Commit the changes.

### 16.8.6.3 Deleting a Server Restriction

To delete an NTP server restriction, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Restrict**.
2. Select the restriction to be deleted, and then click **Delete Entry**.
3. Commit the change.

## 16.9 Managing NTP Broadcast/Multicast Clients

Set the device to NTP broadcast or multicast client mode if the NTP server issues regular time-of-day advertisements.

### 16.9.1 Enabling and Configuring NTP Multicast Clients

The NTP multicast client enables the NTP server to receive advertisements from other NTP servers.



To enable and configure the NTP multicast client, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **General**.
2. Under **NTP Multicast Clients**, configure the following parameter(s) as required:

Parameter	Description
Enable Multicast Clients	Enables the multicast message mode.
Address	<p><b>Synopsis:</b> A string between 1 and 253 characters long</p> <p><b>Default:</b> 224.0.1.1</p> <p>The multicast address on which the NTP client listens for NTP messages.</p>

3. Add a multicast address for a known NTP server. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 775).
4. Commit the changes.

## 16.9.2 Enabling and Configuring NTP Broadcast Clients

The NTP broadcast client enables the NTP server to receive advertisements from other NTP servers and send advertisements of its own.

To enable and configure the NTP broadcast client, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **General**.
2. Under **NTP**, configure the following parameters as required:

Parameter	Description
Enable Broadcast Client	Enables/disables the broadcast client.

3. Add a broadcast address for a known NTP server. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 775).
4. Commit the changes.

## 16.9.3 Managing NTP Broadcast/Multicast Addresses

When broadcast or multicast addresses for known NTP servers are configured, the NTP daemon monitors advertisements from each address and chooses the server with the lowest stratum to use as the NTP time source. This is opposed to manually configuring a list of servers or peers.

### 16.9.3.1 Viewing a List of Broadcast/Multicast Addresses

To view a list of broadcast/multicast addresses for an NTP server, navigate to the **NTP** tab under **Administration » System » Time**, and then click **Broadcast**. If addresses have been configured, a list appears.

If no broadcast/multicast addresses have been configured, add addresses as needed. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 775).

### 16.9.3.2 Adding a Broadcast/Multicast Address

To add a broadcast/multicast address for an NTP server, do the following:

 **NOTICE**

It is strongly recommended to enable NTP authentication, unless all hosts on the network are trusted.

1. If necessary, make sure a server authentication key has been configured with the broadcast/multicast setting to enable NTP authentication. For more information, refer to "Adding a Server Key" (Page 771).
2. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Broadcast**.
3. Click **Add Entry**.
4. Configure the following parameter(s) as required:

 **NOTICE**

The broadcast/multicast address must be the same as the address for the NTP multicast client.

Parameter	Description
Broadcast/Multicast IP Address	<b>Synopsis:</b> A string between 7 and 15 characters long or A string between 6 and 40 characters long  The broadcast or multicast address.

5. Click **OK** to create the new address.
6. Configure the following parameter(s) as required:

Parameter	Description
Enabled	Enables sending broadcast or multicast NTP messages to this address.
Key	<b>Synopsis:</b> An integer equal to or greater than 1  Authentication key.

Parameter	Description
NTP Version	<b>Synopsis:</b> An integer between 1 and 4  The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
Time To Live	<b>Synopsis:</b> An integer between 1 and 127 <b>Default:</b> 1  Time to live.

7. Commit the changes.

### 16.9.3.3 Deleting a Broadcast/Multicast Address

To delete a broadcast/multicast address for an NTP server, do the following:

1. Navigate to the **NTP** tab under **Administration » System » Time**, and then click **Broadcast**.
2. Select the address to be deleted, and then click **Delete Entry**.
3. Commit the change.

## Applications

Applications are special add-ons that extend the functionality of RUGGEDCOM ROX II, such as enhanced support for other RUGGEDCOM products (e.g. RUGGEDCOM CROSSBOW). They are installed and upgraded the same as the RUGGEDCOM ROX II operating system, in that they are first installed on the inactive partition and are only activated after a reboot. This makes it possible to decline or undo the installation if the application creates undesirable results. The currently active partition is also unaffected when an application is being installed or upgraded.

All RUGGEDCOM ROX II applications are released as repositories and must be hosted by an upgrade server. For more information about configuring an upgrade server, refer to "Configuring the Upgrade Server" (Page 81).

---

### Note

Some applications are only compatible with specific versions of RUGGEDCOM ROX II. Check the application's requirements before installing, or before upgrading/downgrading RUGGEDCOM ROX II.

---

## 17.1 Viewing a List of Installed Applications

To view a list of RUGGEDCOM ROX II applications installed on the device, navigate to the **Installed Apps** tab under **Administration » Apps**. If applications have been installed, the **Installed Apps** table appears.

If no applications have been installed, install applications as needed. For more information, refer to "Installing an Application" (Page 777).

## 17.2 Installing an Application

To install an application, do the following:

1. Navigate to the **App Management** tab under **Administration » Apps**. The **Install App** form appears.
2. On the **Install App** form, configure the following parameters:

Parameter	Description
URL	<p><b>Synopsis:</b> A string up to 256 characters long</p> <p>The URL of the app image to download. Supported URIs are HTTP, HTTPS, FTP, FTPS, SFTP, USB and SD.</p>

Parameter	Description
	<p>To flash from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". The device name is displayed under "chassis" in the Web UI or using the "show chassis" command in the CLI. Note that only one single partition is supported for either data medium.</p> <p>For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".</p>

3. Click **Perform**.

## 17.3 Upgrading an Application

To upgrade an application, do the following:

1. Navigate to the **App Management** tab under **Administration » Apps**. The **Upgrade App** form appears.
2. On the **Upgrade App** form, configure the following parameters:

Parameter	Description
App Name	<p><b>Synopsis:</b> A string up to 256 characters long</p> <p>The URL of the app image to download. Supported URIs are HTTP, HTTPS, FTP, FTPS, SFTP, USB and SD.</p> <p>To flash from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". The device name is displayed under "chassis" in the Web UI or using the "show chassis" command in the CLI. Note that only one single partition is supported for either data medium.</p> <p>For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".</p>

3. Click **Perform**.

## 17.4 Uninstalling an Application

To uninstall an application, do the following:

1. Navigate to the **App Management** tab under **Administration » Apps**. The **Uninstall App** form appears.
2. On the **Uninstall App** form, configure the following parameters:

Parameter	Description
App Name	<b>Synopsis:</b> A string between 1 and 256 characters long The name of the app to uninstall.

3. Click **Perform**.



## Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM ROX II or designing a network. It describes the following tasks:

For further assistance, contact Siemens Customer Support.

---

### Note

For a description of pre-configured alarms, refer to "Pre-Configured Alarms" (Page 110).

---

## 18.1 Management Access

The following describes common problems related to management access.

Problem	Solution
<p>Mozilla Firefox displays an error message related to PKCS #11 when attempting to access the RUGGEDCOM ROX II Web UI.</p>	<p>Some versions of Mozilla Firefox may produce an error message similar to the following when attempting to access the RUGGEDCOM ROX II Web User Interface:</p> <pre data-bbox="715 1176 1410 1326">An error occurred during a connection to 192.168.0.2. A PKCS #11 module returned CKR_DE VICE_ERROR, indicating that a problem has occurred with the token or slot. (Error code: sec_error_pkcs11_device_error)</pre> <p>To resolve this issue, download the latest version of Mozilla Firefox, then verify if connectivity to RUGGEDCOM ROX II is successful.</p> <p>If the error persists, specific encryption ciphers must be disabled. To disable the ciphers, do the following:</p> <hr/> <p><b>Note</b></p> <p>The following steps were tested using Mozilla Firefox v91.6.0esr.</p> <hr/> <ol style="list-style-type: none"> <li>1. Open Mozilla Firefox, type <b>about:config</b> in the address bar, and then press <b>Enter</b>. A confirmation message appears.</li> <li>2. Click <b>Accept the Risk and Continue</b> to proceed. A list of preferences appears.</li> <li>3. In the <b>Search</b> box at the top of the window, type <b>security.ssl3.dhe_rsa_aes</b>. The following preferences appear: <ul style="list-style-type: none"> <li>• security.ssl3.dhe_rsa_aes_128_sha</li> <li>• security.ssl3.dhe_rsa_aes_256_sha</li> </ul> </li> <li>4. Double-click each preference. The <b>Value</b> setting changes from <b>true</b> to <b>false</b>.</li> </ol>



## 18.2 Feature Keys

The following describes common problems related to feature keys.

Problem	Solution
A file-based feature key does not match the hardware	<p>Each file-based feature key is licensed to a particular device. When transferring a feature key from one device to another, such as when configuring a backup unit to replace a malfunctioning device, the device will detect a hardware mismatch with the key and trigger an alarm.</p> <p>Do not transfer file-based feature keys between devices. Contact a Siemens Canada Ltd. sales representative to order a feature key matching the serial numbers of the hardware in the destination device.</p>

## 18.3 Ethernet Ports

The following describes common problems related to Ethernet ports.

Problem	Solution
A link seems fine when traffic levels are low, but fails as traffic rates increase OR a link can be pinged but has problems with FTP/SQL/HTTP/etc.	<p>A possible cause of intermittent operation is that of a <i>duplex mismatch</i>. If one end of the link is fixed to full-duplex and the peer auto-negotiates, the auto-negotiating end falls back to half-duplex operation.</p> <p>At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable.</p> <p>The ping command with flood options is a useful tool for testing commissioned links. The command <code>ping 192.168.0.1 500 2</code> can be used to issue 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.</p>
Links are inaccessible, even when using the Link Fault Indication (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.

## 18.4 Multicast Filtering

The following describes common problems related to multicast filtering.

Problem	Solution
When started, a multicast traffic feed is always distributed to all members of the VLAN.	Is IGMP enabled for the VLAN? Multicasts will be distributed to all members of the VLAN unless IGMP is enabled.
Computers connected to the switch receive multicast traffic, but not when they are connected to a router.	<p>Is the port used to connect the router included in the Router Ports list?</p> <p>To determine whether the multicast stream is being delivered to the router, view the statistics collected for switched Ethernet ports.</p>

Problem	Solution
	<p>For more information, refer to "Viewing Switched Ethernet Port Statistics" (Page 283).</p> <p>Verify the traffic count transmitted to the router is the same as the traffic count received from the multicasting source.</p>
The video stream at an end station is of poor quality.	<p>Video serving is a resource-intensive application. Because it uses isochronous workload, data must be fed at a prescribed rate or end users will see glitches in the video. Networks that carry data from the server to the client must be engineered to handle this heavy, isochronous workload. Video streams can consume large amounts of bandwidth. Features and capacity of both server and network (including routers, bridges, switches and interfaces) impact the streams.</p> <p>Do not exceed 60% of the maximum interface bandwidth. For example, if using a 10 Mbps Ethernet, run a single multicasting source at no more than 6 Mbps, or two sources at 3 Mbps. It is important to consider these ports in the network design, as router ports will carry the traffic of all multicast groups.</p> <hr/> <p><b>Note</b></p> <p>Multicasting will introduce latency in all traffic on the network. Plan the network carefully to account for capacity and latency concerns.</p> <hr/>
Multicast streams of some groups are not forwarded properly. Some segments without subscribers receive the traffic, while some segments with subscribers do not.	Make sure different multicast groups do not have multicast IP addresses that map to the same multicast MAC address. The switch forwarding operation is MAC address-based and will not work properly for several groups mapping to the same MAC address.
Computers on the switch issue join requests, but do not receive multicast streams from a router.	Is the multicast route running IGMP version 2? It must run IGMP version 2 in order for IGMP Snooping to operate properly.
Unable to connect or disconnect some switch ports, and multicast goes everywhere. Is IGMP broken?	<p>IGMP is not broken. This may in fact be proper switch behavior.</p> <p>When the switch detects a change in the network topology through RSTP, it acts to avoid loss of multicast traffic. If configured to do so, it starts forwarding all multicast traffic to all ports that are not RSTP Edge ports (because they may potentially link to routers). This may result in some undesired flooding of multicast traffic, which will stop after a few minutes. However, it guarantees that all devices interested in the traffic will keep receiving it without interruption.</p> <p>The same behavior will be observed when the switch resets or when IGMP Snooping is being disabled for the VLAN.</p>

## 18.5 Spanning Tree

The following describes common problems related to the Spanning Tree Protocol (STP).

Problem	Solution
The network locks up when a new port is connected and the	Is it possible that one of the switches in the network or one of the ports on a switch in the network has STP disabled and accidentally

Problem	Solution
port status LEDs are flashing rapidly.	connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	<p>If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to The network becomes unstable when a specific application is started (Page 785).</p> <p>Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.</p>
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	<p>Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up.</p> <p>Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port's point-to-point setting to true.</p> <p>Either one will allow the Proposal-Agreement protocol to be used.</p>
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	<p>Is it possible that some ports participating in the topology have been configured to STP mode or that the port's point-to-point parameter is set to false? STP and multi-point ports converge slowly after failures occur.</p> <p>Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow.</p> <p>Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst</p>

Problem	Solution
	of all possible designs occurs when the secondary root bridge is located at the farthest edge of the network from the root. In this case, a configuration message will have to propagate out to the edge and then back in order to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An IED/controller does not work with the device.	Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port.  If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller's bridge to STP.
Polls to other devices are occasionally lost.	Review the network statistics to determine whether the root bridge is receiving TCNs around the time of observed frame loss. It may be possible there are problems with intermittent links in the network.
The root is receiving a number of TCNs. Where are they coming from?	Examine the RSTP port statistics to determine the port from which the TCNs are arriving. Sign-on to the switch at the other end of the link attached to that port. Repeat this step until the switch generating the TCNs is found (i.e. the switch that is itself not receiving a large number of TCNs). Determine the problem at that switch.

## 18.6 VLANs

The following describes common problems related to the VLANs.

Problem	Solution
VLANs are not needed on the network. Can they be turned off?	Yes. Simply leave all ports set to type <i>edge</i> and leave the native VLAN set to 1. This is the default configuration for the switch.
Two VLANs were created and a number of ports were made members of them. Now some of the devices in one VLAN need to	If the devices need to communicate at the physical address layer, they must be members of the same VLAN. If they can communicate in a Layer 3 fashion (i.e. using a protocol such as IP or IPX), use a router. The router will treat each VLAN as a separate interface, which will have its own associated IP address space.

<b>Problem</b>	<b>Solution</b>
send messages to devices in the other VLAN.	

This chapter provides additional information that may be required to understand and/or configure related features in RUGGEDCOM ROX II.

## 19.1 Supported MIBs

The current MIB files supported by RUGGEDCOM ROX II can be downloaded from the <https://www.siemens.com>.

RUGGEDCOM ROX II supports the following MIBs:

### NOTICE

This section lists all MIBs supported by RUGGEDCOM ROX II, and is intended for reference purposes only. Individual device support may vary.

- **BRIDGE-MIB**  
For more information, refer to "BRIDGE-MIB" (Page 788).
- **IF-MIB**  
For more information, refer to "IF-MIB" (Page 794).
- **IP-MIB**  
For more information, refer to "IP-MIB" (Page 801).
- **TCP-MIB**  
For more information, refer to "TCP-MIB" (Page 806).
- **UDP-MIB**  
For more information, refer to "UDP-MIB" (Page 809).
- **LLDP-MIB**  
For more information, refer to "LLDP-MIB" (Page 809).
- **Q-BRIDGE-MIB**  
For more information, refer to "Q-BRIDGE-MIB" (Page 817).
- **RUGGEDCOM-SYS-INFO-MIB**  
For more information, refer to "RUGGEDCOM-SYS-INFO-MIB" (Page 822).
- **RC-IEC-62439-3-MIB**  
For more information, refer to "RC-IEC-62439-3-MIB" (Page 826).
- **SNMP-FRAMEWORK-MIB**  
For more information, refer to "SNMP-FRAMEWORK-MIB" (Page 829).
- **SNMP-USER-BASED-SM-MIB**  
For more information, refer to "SNMP-USER-BASED-SM-MIB" (Page 829).

- **SNMPv2-MIB**  
For more information, refer to "SNMPv2-MIB" (Page 834).
- **SNMP-VIEW-BASED-ACM-MIB**  
For more information, refer to "SNMP-VIEW-BASED-ACM-MIB" (Page 836).
- **BGP4-MIB**  
For more information, refer to "BGP4-MIB" (Page 839).
- **IP-FORWARD-MIB**  
For more information, refer to "IP-FORWARD-MIB" (Page 839).
- **RFC1213-MIB**  
For more information, refer to "RFC1213-MIB" (Page 842).
- **PIM-STD-MIB**  
For more information, refer to "PIM-STD-MIB" (Page 845).
- **MPLS-LDP-STD-MIB**  
For more information, refer to "MPLS-LDP-STD-MIB" (Page 845).
- **MPLS-LDP-GENERIC-STD-MIB**  
For more information, refer to "MPLS-LDP-GENERIC-STD-MIB" (Page 845).
- **IEC-62439-2-MIB**  
For more information, refer to "IEC-62439-2-MIB" (Page 846).

**BRIDGE-MIB**

Object	Description
dot1dBaseBridgeAddress	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.1.1</p> <p><b>Description:</b> The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However, it is only required to be unique. When concatenated with dot1dStpPriority, a unique BridgIdentifier is formed, which is used in the Spanning Tree Protocol.</p>
dot1dBaseNumPorts	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.1.2</p> <p><b>Description:</b> The number of ports controlled by this bridging entity.</p>
dot1dBaseType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.1.3</p> <p><b>Description:</b> Indicates what type of bridging this bridge can perform. If a bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type.</p>
dot1dBasePort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.1.4.1.1</p>

Object	Description
	<b>Description:</b> The port number of the port for which this entry contains bridge management information.
dot1dBasePortIfIndex	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.1.4.1.2 <b>Description:</b> The value of the instance of the ifIndex object, defined in IF-MIB, for the interface corresponding to this port.
dot1dBasePortCircuit	<b>Syntax:</b> OID <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.1.4.1.3 <b>Description:</b> For a port that (potentially) has the same value of dot1dBasePortIfIndex as another port on the same bridge. This object contains the name of an object instance unique to this port. For example, in the case where multiple ports correspond one-to-one with multiple X.25 virtual circuits, this value might identify an (e.g., the first) object instance associated with the X.25 virtual circuit corresponding to this port. For a port which has a unique value of dot1dBasePortIfIndex, this object can have the value { 0 0 }.
dot1dBasePortDelayExceededDiscards	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.1.4.1.4 <b>Description:</b> The number of frames discarded by this port due to excessive transit delay through the bridge. It is incremented by both transparent and source route bridges.
dot1dBasePortMtuExceededDiscards	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.1.4.1.5 <b>Description:</b> The number of frames discarded by this port due to an excessive size. It is incremented by both transparent and source route bridges.
dot1dStpProtocolSpecification	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.2.1 <b>Description:</b> An indication of what version of the Spanning Tree Protocol is being run. The value 'decLb100(2)' indicates the DEC LANbridge 100 Spanning Tree protocol. IEEE 802.1D implementations will return 'ieee8021d(3)'. If future versions of the IEEE Spanning Tree Protocol that are incompatible with the current version are released a new value will be defined.
dot1dStpPriority	<b>Syntax:</b> Integer <b>Access:</b> Read-Write <b>OID:</b> .1.3.6.1.2.1.17.2.2 <b>Description:</b> The value of the write-able portion of the Bridge ID (i.e., the first two octets of the (8 octet long) Bridge ID). The other (last) 6 octets of the Bridge ID are given by the value of dot1dBaseBridgeAddress. On bridges supporting IEEE 802.1t or IEEE 802.1w, permissible values are 0-61440, in steps of 4096.
dot1dStpTimeSinceTopologyChange	<b>Syntax:</b> Timeticks



## 19.1 Supported MIBs

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.3</p> <p><b>Description:</b> The time (in hundredths of a second) since the last time a topology change was detected by the bridge entity. For RSTP, this reports the time since the tcWhile timer for any port on this Bridge was nonzero.</p>
dot1dStpTopChanges	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.4</p> <p><b>Description:</b> The total number of topology changes detected by this bridge since the management entity was last reset or initialized.</p>
dot1dStpDesignatedRoot	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.5</p> <p><b>Description:</b> The bridge identifier of the root of the spanning tree, as determined by the Spanning Tree Protocol, as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.</p>
dot1dStpRootCost	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.6</p> <p><b>Description:</b> The cost of the path to the root as seen from this bridge.</p>
dot1dStpRootPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.7</p> <p><b>Description:</b> The port number of the port that offers the lowest cost path from this bridge to the root bridge.</p>
dot1dStpMaxAge	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.8</p> <p><b>Description:</b> The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.</p>
dot1dStpHelloTime	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.9</p> <p><b>Description:</b> The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree, or trying to become so, in units of hundredths of a second. This is the actual value that this bridge is currently using.</p>
dot1dStpHoldTime	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.10</p> <p><b>Description:</b> This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of hundredths of a second.</p>

Object	Description
dot1dStpForwardDelay	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.11</p> <p><b>Description:</b> This time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. Note that this value is the one that this bridge is currently using, in contrast to dot1dStpBridgeForwardDelay, which is the value that this bridge and all others would start using if/when this bridge were to become the root.</p>
dot1dStpBridgeMaxAge	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.12</p> <p><b>Description:</b> The value that all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1998 specifies that the range for this parameter is related to the value of dot1dStpBridgeHelloTime. The granularity of this timer is specified by 802.1D-1998 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.</p>
dot1dStpBridgeHelloTime	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.13</p> <p><b>Description:</b> The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1998 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.</p>
dot1dStpBridgeForwardDelay	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.14</p> <p><b>Description:</b> The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1998 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1998 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.</p>
dot1dStpPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.1</p> <p><b>Description:</b> The port number of the port for which this entry contains Spanning Tree Protocol management information.</p>
dot1dStpPortPriority	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.2</p> <p><b>Description:</b> The value of the priority field that is contained in the first (in network byte order) octet of the (2 octet long) Port ID. The other octet of the Port ID is given by the value of dot1dStpPort. On bridges supporting IEEE 802.1t or IEEE 802.1w, permissible values are 0-240, in steps of 16.</p>

## 19.1 Supported MIBs

Object	Description
dot1dStpPortState	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.3</p> <p><b>Description:</b> The port's current state, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning, it will place that port into the broken(6) state. For ports that are disabled (see dot1dStpPortEnable), this object will have a value of disabled(1).</p>
dot1dStpPortEnable	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.4</p> <p><b>Description:</b> The enabled/disabled status of the port.</p>
dot1dStpPortPathCost	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.5</p> <p><b>Description:</b> The contribution of this port to the path cost of paths towards the spanning tree root which include this port. 802.1D-1998 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. New implementations should support dot1dStpPortPathCost32. If the port path costs exceeds the maximum value of this object then this object should report the maximum value, namely 65535. Applications should try to read the dot1dStpPortPathCost32 object if this object reports the maximum value.</p>
dot1dStpPortDesignatedRoot	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.6</p> <p><b>Description:</b> The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.</p>
dot1dStpPortDesignatedCost	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.7</p> <p><b>Description:</b> The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.</p>
dot1dStpPortDesignatedBridge	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.8</p> <p><b>Description:</b> The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.</p>
dot1dStpPortDesignatedPort	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.9</p> <p><b>Description:</b> The Port Identifier of the port on the Designated Bridge for this port's segment.</p>
dot1dStpPortForwardTransitions	<p><b>Syntax:</b> Counter32</p>

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.2.15.1.10</p> <p><b>Description:</b> The number of times this port has transitioned from the Learning state to the Forwarding state.</p>
dot1dTpLearnedEntryDiscards	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.1</p> <p><b>Description:</b> The contribution of this port to the path cost of paths towards the spanning tree root which include this port. 802.1D-1998 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. This object replaces dot1dStpPortPathCost to support IEEE 802.1t.</p>
dot1dTpAgingTime	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.2</p> <p><b>Description:</b> The timeout period in seconds for aging out dynamically-learned forwarding information. 802.1D-1998 recommends a default of 300 seconds.</p>
dot1dTpPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.4.1.1</p> <p><b>Description:</b> The port number of the port for which this entry contains Transparent bridging management information.</p>
dot1dTpPortMaxInfo	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.4.1.2</p> <p><b>Description:</b> The maximum size of the INFO (non-MAC) field that this port will receive or transmit.</p>
dot1dTpPortInFrames	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.4.1.3</p> <p><b>Description:</b> The number of frames that have been received by this port from its segment. Note that a frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.</p>
dot1dTpPortOutFrames	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.4.1.4</p> <p><b>Description:</b> The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.</p>
dot1dTpPortInDiscards	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.4.4.1.5</p>

Object	Description
	<b>Description:</b> Count of received valid frames that were discarded (i.e., filtered) by the Forwarding Process.

## IF-MIB

Object	Description
ifIndex	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.1</p> <p><b>Description:</b> A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.</p>
ifDescr	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.2</p> <p><b>Description:</b> A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software.</p>
ifType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.3</p> <p><b>Description:</b> The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention.</p>
ifSpeed	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.5</p> <p><b>Description:</b> An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interface's speed. For a sub-layer which has no concept of bandwidth, this object should be zero.</p>
ifAdminStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.7</p> <p><b>Description:</b> The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state).</p>
ifOperStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p>

Object	Description
	<p><b>OID:</b> .1.3.6.1.2.1.2.2.1.8</p> <p><b>Description:</b> The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components.</p>
ifLastChange	<p><b>Syntax:</b> Timeticks</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.9</p> <p><b>Description:</b> The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value.</p>
ifLinkUpDownTrapEnable	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.14</p> <p><b>Description:</b> Indicates whether linkUp/linkDown traps should be generated for this interface. By default, this object should have the value enabled(1) for interfaces which do not operate on 'top' of any other interface (as defined in the ifStackTable), and disabled(2) otherwise.</p>
ifConnectorPresent	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.17</p> <p><b>Description:</b> This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise.</p>
ifHighSpeed	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.15</p> <p><b>Description:</b> An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of `n' then the speed of the interface is somewhere in the range of `n-500,000' to `n+499,999'. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object should be zero.</p>
ifName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.1</p> <p><b>Description:</b> The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name, such as `le0' or a simple port number, such as `1', depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. Note that for an</p>

Object	Description
	agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of ifName for such an interface is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string.
ifNumber	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.1</p> <p><b>Description:</b> The number of network interfaces (regardless of their current state) present on this system.</p>
ifAlias	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.18</p> <p><b>Description:</b> This object is an 'alias' name for the interface as specified by a network manager, and provides a non-volatile 'handle' for the interface. On the first instantiation of an interface, the value of ifAlias associated with that interface is the zero-length string. As and when a value is written into an instance of ifAlias through a network management set operation, then the agent must retain the supplied value in the ifAlias instance associated with the same interface for as long as that interface remains instantiated, including across all re- initializations/reboots of the network management system, including those which result in a change of the interface's ifIndex value. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface. Some agents may support write-access only for interfaces having particular values of ifType. An agent which supports write access to this object is required to keep the value in non-volatile storage, but it may limit the length of new values depending on how much storage is already occupied by the current values for other interfaces.</p>
ifTableLastChange	<p><b>Syntax:</b> Timeticks</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.5</p> <p><b>Description:</b> The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value.</p>
ifHCInUcastPkts	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.7</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifHCInBroadcastPkts	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.9</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts.</p>

Object	Description
	Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCOutMulticastPkts	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.12</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifHCInOctets	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.6</p> <p><b>Description:</b> The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifInOctets	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.10</p> <p><b>Description:</b> The total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifInErrors	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.14</p> <p><b>Description:</b> For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifMtu	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.4</p> <p><b>Description:</b> The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.</p>
ifInBroadcastPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.3</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.</p>



## 19.1 Supported MIBs

Object	Description
	Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifOutUcastPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.17</p> <p><b>Description:</b> The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifOutBroadcastPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.5</p> <p><b>Description:</b> The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifPromiscuousMode	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.16</p> <p><b>Description:</b> This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. The value true(1) is only legal on certain types of media. If legal, setting this object to a value of true(1) may require the interface to be reset before becoming effective. The value of ifPromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface.</p>
ifHCInMulticastPkts	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.8</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifHCOUcastPkts	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.11</p> <p><b>Description:</b> The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>

Object	Description
ifHCOutBroadcastPkts	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.13</p> <p><b>Description:</b>The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifHCOutOctets	<p><b>Syntax:</b> Counter64</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.10</p> <p><b>Description:</b> The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifOutOctets	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.16</p> <p><b>Description:</b> The total number of octets transmitted out of the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifOutErrors	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.20</p> <p><b>Description:</b> For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifInUcastPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.11</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifInDiscards	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.13</p> <p><b>Description:</b> The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of</p>

## 19.1 Supported MIBs

Object	Description
	this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifOutMulticastPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.4</p> <p><b>Description:</b> The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifOutDiscards	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.19</p> <p><b>Description:</b> The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifInUnknownProtos	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.2.2.1.15</p> <p><b>Description:</b> For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifInMulticastPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.2</p> <p><b>Description:</b> The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
ifCounterDiscontinuityTime	<p><b>Syntax:</b> Timeticks</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.31.1.1.1.19</p> <p><b>Description:</b> The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity. The relevant counters are the specific instances associated with this interface of any Counter32 or Counter64 object contained in the ifTable or ifXTable. If no</p>

Object	Description
	such discontinuities have occurred since the last re- initialization of the local management subsystem, then this object contains a zero value.
linkUp	<b>OID:</b> .1.3.6.1.6.3.1.1.5.4 <b>Description:</b> A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkDown	<b>OID:</b> .1.3.6.1.6.3.1.1.5.3 <b>Description:</b> A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.

## IP-MIB

Object	Description
ipForwarding	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.4.1 <b>Description:</b> The indication of whether this entity is acting as an IPv4 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv4 routers forward datagrams. IPv4 hosts do not (except those source-routed via the host). When this object is written, the entity should save the change to non-volatile storage and restore the object from non-volatile storage upon re-initialization of the system. Note: a stronger requirement is not used because this object was previously defined.
ipInHdrErrors	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.4.4 <b>Description:</b> The number of input datagrams discarded due to errors in their IPv4 headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IPv4 options, etc. This object has been deprecated as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInHdrErrors.
ipForwDatagrams	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.4.6 <b>Description:</b> The number of input datagrams for which this entity was not their final IPv4 destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IPv4 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInForwDatagrams.
ipInDiscards	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only

## 19.1 Supported MIBs

Object	Description
	<p><b>OID:</b> .1.3.6.1.2.1.4.8</p> <p><b>Description:</b> The number of input IPv4 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInDiscards.</p>
ipOutDiscards	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.11</p> <p><b>Description:</b> The number of output IPv4 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsOutDiscards.</p>
ipReasmTimeout	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.13</p> <p><b>Description:</b> The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.</p>
ipReasmFails	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.16</p> <p><b>Description:</b> The number of failures detected by the IPv4 re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IPv4 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsReasmFails.</p>
ipFragFails	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.18</p> <p><b>Description:</b> The number of IPv4 datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsOutFragFails.</p>
ipAdEntAddr	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.20.1.1</p> <p><b>Description:</b> The IPv4 address to which this entry's addressing information pertains.</p>
ipAdEntBcastAddr	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.20.1.4</p>

Object	Description
	<p><b>Description:</b> The value of the least-significant bit in the IPv4 broadcast address used for sending datagrams on the (logical) interface associated with the IPv4 address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcast addresses used by the entity on this (logical) interface.</p>
ipNetToMediaIfIndex	<p><b>Syntax:</b> Integer  <b>Access:</b> Read-Only  <b>OID:</b> .1.3.6.1.2.1.4.22.1.1</p> <p><b>Description:</b> The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB's ifIndex. This object predates the rule limiting index objects to a max access value of 'not-accessible' and so continues to use a value of 'read-create'.</p>
ipNetToMediaNetAddress	<p><b>Syntax:</b> IpAddress  <b>Access:</b> Read-Only  <b>OID:</b> .1.3.6.1.2.1.4.22.1.3</p> <p><b>Description:</b> The IpAddress corresponding to the media-dependent 'physical' address. This object predates the rule limiting index objects to a max access value of 'not-accessible' and so continues to use a value of 'read-create'.</p>
ipRoutingDiscards	<p><b>OID:</b> .1.3.6.1.2.1.4.23</p>
ipDefaultTTL	<p><b>Syntax:</b> Integer  <b>Access:</b> Read-Write  <b>OID:</b> .1.3.6.1.2.1.4.2</p> <p><b>Description:</b> The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries. This object was defined in pre-IPv6 versions of the IP MIB. It was implicitly IPv4 only, but the original specifications did not indicate this protocol restriction. In order to clarify the specifications, this object has been deprecated and a similar, but more thoroughly clarified, object has been added to the IP-FORWARD-MIB.</p>
ipInAddrErrors	<p><b>Syntax:</b> Counter32  <b>Access:</b> Read-Only  <b>OID:</b> .1.3.6.1.2.1.4.5</p> <p><b>Description:</b> The number of input datagrams discarded because the IPv4 address in their IPv4 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IPv4 routers, and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInAddrErrors.</p>
ipInUnknownProtos	<p><b>Syntax:</b> Counter32  <b>Access:</b> Read-Only  <b>OID:</b> .1.3.6.1.2.1.4.7</p> <p><b>Description:</b> The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.</p>

Object	Description
	This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInUnknownProtos.
ipInDelivers	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.9</p> <p><b>Description:</b> The total number of input datagrams successfully delivered to IPv4 user-protocols (including ICMP). This object has been deprecated as a new IP version neutral table has been added. It is loosely replaced by ipSystemStatsInDelivers.</p>
ipOutNoRoutes	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.12</p> <p><b>Description:</b> The number of IPv4 datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default routers are down. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsOutNoRoutes.</p>
ipReasmReqds	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.14</p> <p><b>Description:</b> The number of IPv4 fragments received which needed to be reassembled at this entity. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsReasmReqds.</p>
ipFragOKs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.17</p> <p><b>Description:</b> The number of IPv4 datagrams that have been successfully fragmented at this entity. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsOutFragOKs.</p>
ipFragCreates	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.19</p> <p><b>Description:</b> The number of IPv4 datagram fragments that have been generated as a result of fragmentation at this entity. This object has been deprecated as a new IP version neutral table has been added. It is loosely replaced by ipSystemStatsOutFragCreates.</p>
ipAdEntIfIndex	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.20.1.2</p> <p><b>Description:</b> The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB's ifIndex.</p>
ipAdEntReasmMaxSize	<p><b>Syntax:</b> Integer</p>

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.20.1.5</p> <p><b>Description:</b> The size of the largest IPv4 datagram which this entity can re-assemble from incoming IPv4 fragmented datagrams received on this interface.</p>
ipNetToMediaPhysAddress	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.22.1.2</p> <p><b>Description:</b> The media-dependent `physical' address. This object should return 0 when this entry is in the 'incomplete' state. As the entries in this table are typically not persistent when this object is written the entity should not save the change to non-volatile storage. Note: a stronger requirement is not used because this object was previously defined.</p>
ipNetToMediaType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.22.1.4</p> <p><b>Description:</b> The type of mapping. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively dis-associates the interface identified with said entry from the mapping identified with said entry. It is an implementation- specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object. As the entries in this table are typically not persistent when this object is written the entity should not save the change to non-volatile storage. Note: a stronger requirement is not used because this object was previously defined.</p>
ipInReceives	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.3</p> <p><b>Description:</b> The total number of input datagrams received from interfaces, including those received in error. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInReceives.</p>
ipOutRequests	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.10</p> <p><b>Description:</b> The total number of IPv4 datagrams which local IPv4 user protocols (including ICMP) supplied to IPv4 in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsOutRequests.</p>
ipReasmOKs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.4.15</p>



## 19.1 Supported MIBs

Object	Description
	<b>Description:</b> The number of IPv4 datagrams successfully re-assembled. This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsReasmOKs.
ipAdEntNetMask	<b>Syntax:</b> IpAddress <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.4.20.1.3 <b>Description:</b> The subnet mask associated with the IPv4 address of this entry. The value of the mask is an IPv4 address with all the network bits set to 1 and all the hosts bits set to 0.

## TCP-MIB

Object	Description
tcpRtoAlgorithm	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.6.1 <b>Description:</b> The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.6.2 <b>Description:</b> The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend on the algorithm used to determine the retransmission timeout; in particular, the IETF standard algorithm rfc2988(5) provides a minimum value.
tcpMaxConn	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.6.4 <b>Description:</b> The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpPassiveOpens	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.6.6 <b>Description:</b> The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.
tcpEstabResets	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.6.8 <b>Description:</b> The number of times that TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.
tcpOutSegs	<b>Syntax:</b> Counter32

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.11</p> <p><b>Description:</b> The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpConnLocalAddress	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.13.1.2</p> <p><b>Description:</b> The local IP address for this TCP connection. In the case of a connection in the listen state willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.</p>
tcpConnRemAddress	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.13.1.4</p> <p><b>Description:</b> The remote IP address for this TCP connection.</p>
tcpInErrs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.14</p> <p><b>Description:</b> The total number of segments received in error (e.g., bad TCP checksums). Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpRtoMax	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.3</p> <p><b>Description:</b> The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend on the algorithm used to determine the retransmission timeout; in particular, the IETF standard algorithm rfc2988(5) provides an upper bound (as part of an adaptive backoff algorithm).</p>
tcpActiveOpens	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.5</p> <p><b>Description:</b> The number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpAttemptFails	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.7</p> <p><b>Description:</b> The number of times that TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times that TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpCurrEstab	<p><b>Syntax:</b> Gauge32</p>

## 19.1 Supported MIBs

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.9</p> <p><b>Description:</b> The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.</p>
tcpRetransSegs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.12</p> <p><b>Description:</b> The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpConnLocalPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.13.1.3</p> <p><b>Description:</b> The local port number for this TCP connection.</p>
tcpConnRemPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.13.1.5</p> <p><b>Description:</b> The remote port number for this TCP connection.</p>
tcpOutRsts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.15</p> <p><b>Description:</b> The number of TCP segments sent containing the RST flag. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpInSegs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.17</p> <p><b>Description:</b> The total number of segments received, including those received in error. This count includes segments received on currently established connections. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.</p>
tcpConnState	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.6.13.1.1</p> <p><b>Description:</b> The state of this TCP connection. The only value that may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then the TCB (as defined in [RFC793]) of the corresponding connection on the managed node is deleted, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note, however, that RST segments are not sent reliably).</p>

## UDP-MIB

Object	Description
udpInDatagrams	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.7.1</p> <p><b>Description:</b> The total number of UDP datagrams delivered to UDP users. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.</p>
udpNoPorts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.7.2</p> <p><b>Description:</b> The total number of received UDP datagrams for which there was no application at the destination port. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.</p>
udpInErrors	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.7.3</p> <p><b>Description:</b> The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.</p>
udpLocalAddress	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.7.5.1.1</p> <p><b>Description:</b> The local IP address for this UDP listener. In the case of a UDP listener that is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.</p>
udpOutDatagrams	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.7.4</p> <p><b>Description:</b> The total number of UDP datagrams sent from this entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.</p>
udpLocalPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.7.5.1.2</p> <p><b>Description:</b> The local port number for this UDP listener.</p>

## LLDP-MIB

Object	Description
lldpPortConfigAdminStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p>

Object	Description
	<p><b>OID:</b> .1.0.8802.1.1.2.1.1.6.1.2</p> <p><b>Description:</b> The administratively desired status of the local LLDP agent. If the associated IldpPortConfigAdminStatus object has a value of 'txOnly(1)', then LLDP agent will transmit LLDP frames on this port and it will not store any information about the remote systems connected. If the associated IldpPortConfigAdminStatus object has a value of 'rxOnly(2)', then the LLDP agent will receive, but it will not transmit LLDP frames on this port. If the associated IldpPortConfigAdminStatus object has a value of 'txAndRx(3)', then the LLDP agent will transmit and receive LLDP frames on this port. If the associated IldpPortConfigAdminStatus object has a value of 'disabled(4)', then LLDP agent will not transmit or receive LLDP frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port's IldpPortConfigAdminStatus becomes disabled, then the information will naturally age out.</p>
IldpNotificationInterval	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.1.5</p> <p><b>Description:</b> This object controls the transmission of LLDP notifications. the agent must not generate more than one IldpRemTablesChange notification-event in the indicated period, where a 'notification-event' is the transmission of a single notification PDU type to a list of notification destinations. If additional changes in IldpRemoteSystemsData object groups occur within the indicated throttling period, then these trap-events must be suppressed by the agent. An NMS should periodically check the value of IldpStatsRemTableLastChangeTime to detect any missed IldpRemTablesChange notification-events, e.g. due to throttling or transmission loss. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.</p>
IldpPortConfigNotificationEnable	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.1.6.1.3</p> <p><b>Description:</b> The IldpPortConfigNotificationEnable controls, on a per port basis, whether or not notifications from the agent are enabled. The value true(1) means that notifications are enabled; the value false(2) means that they are not.</p>
IldpMessageTxInterval	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.1.1</p> <p><b>Description:</b> The interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value for IldpMessageTxInterval object is 30 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.</p>
IldpMessageTxHoldMultiplier	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.1.2</p> <p><b>Description:</b> The time-to-live value expressed as a multiple of the IldpMessageTxInterval object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula: <math>TTL = \min(65535, (IldpMessageTxInterval * IldpMessageTxHoldMultiplier))</math> For example, if the value of</p>

Object	Description
	<p>lldpMessageTxInterval is '30', and the value of lldpMessageTxHoldMultiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header. The default value for lldpMessageTxHoldMultiplier object is 4. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.</p>
lldpReinitDelay	<p><b>Syntax:</b> Integer  <b>Access:</b> Read-Write  <b>OID:</b> .1.0.8802.1.1.2.1.1.3  <b>Description:</b> The lldpReinitDelay indicates the delay (in units of seconds) from when lldpPortConfigAdminStatus object of a particular port becomes 'disabled' until re-initialization will be attempted. The default value for lldpReinitDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.</p>
lldpTxDelay	<p><b>Syntax:</b> Integer  <b>Access:</b> Read-Write  <b>OID:</b> .1.0.8802.1.1.2.1.1.4  <b>Description:</b> The lldpTxDelay indicates the delay (in units of seconds) between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula:</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <math display="block">1 \leq \text{lldpTxDelay} \leq (0.25 * \text{lldpMessageTxInterval})</math> </div> <p>The default value for lldpTxDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.</p>
lldpPortConfigTLVsTxEnable	<p><b>Syntax:</b> Hex-String  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.1.6.1.4  <b>Description:</b> The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The value of this object is used as a port index to the lldpPortConfigTable.</p>
lldpConfigManAddrPortsTxEnable	<p><b>Syntax:</b> Hex-String  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.1.7.1.1  <b>Description:</b> A set of ports that are identified by a PortList, in which each port is represented as a bit. The corresponding local system management address instance will be transmitted on the member ports of the lldpManAddrPortsTxEnable. The default value for lldpConfigManAddrPortsTxEnable object is empty binary string, which means no ports are specified for advertising indicated management address instance.</p>
lldpStatsRemTablesLastChangeTime	<p><b>Syntax:</b> Timeticks  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.2.1  <b>Description:</b> The value of sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in the in tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects</p>

Object	Description
	associated with remote systems. An NMS can use this object to reduce polling of the IldpRemoteSystemsData objects.
IldpStatsRemTablesInserts	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.2.2</p> <p><b>Description:</b> The number of times the complete set of information advertised by a particular MSAP has been inserted into tables contained in IldpRemoteSystemsData and IldpExtensions objects. The complete set of information received from a particular MSAP should be inserted into related tables. If partial information cannot be inserted for a reason such as lack of resources, all of the complete set of information should be removed. This counter should be incremented only once after the complete set of information is successfully recorded in all related tables. Any failures during inserting information set which result in deletion of previously inserted information should not trigger any changes in IldpStatsRemTablesInserts since the insert is not completed yet or or in IldpStatsRemTablesDeletes, since the deletion would only be a partial deletion. If the failure was the result of lack of resources, the IldpStatsRemTablesDrops counter should be incremented once.</p>
IldpStatsRemTablesDeletes	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.2.3</p> <p><b>Description:</b> The number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in IldpRemoteSystemsData and IldpExtensions objects. This counter should be incremented only once when the complete set of information is completely deleted from all related tables. Partial deletions, such as deletion of rows associated with a particular MSAP from some tables, but not from all tables are not allowed, thus should not change the value of this counter.</p>
IldpStatsRemTablesDrops	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.2.4</p> <p><b>Description:</b> The number of times the complete set of information advertised by a particular MSAP could not be entered into tables contained in IldpRemoteSystemsData and IldpExtensions objects because of insufficient resources.</p>
IldpStatsRemTablesAgeouts	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.2.5</p> <p><b>Description:</b> The number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in IldpRemoteSystemsData and IldpExtensions objects because the information timeliness interval has expired. This counter should be incremented only once when the complete set of information is completely invalidated (aged out) from all related tables. Partial aging, similar to deletion case, is not allowed, and thus, should not change the value of this counter.</p>
IldpStatsRxPortFramesDiscardedTotal	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.2.7.1.2</p>

Object	Description
	<p><b>Description:</b> The number of LLDP frames received by this LLDP agent on the indicated port, and then discarded for any reason. This counter can provide an indication that LLDP header formatting problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system.</p>
lldpStatsRxPortFramesErrors	<p><b>Syntax:</b> Counter32  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.2.7.1.3  <b>Description:</b> The number of invalid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.</p>
lldpStatsRxPortFramesTotal	<p><b>Syntax:</b> Counter32  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.2.7.1.4  <b>Description:</b> The number of valid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.</p>
lldpStatsRxPortTLVsDiscardedTotal	<p><b>Syntax:</b> Counter32  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.2.7.1.5  <b>Description:</b> The number of LLDP TLVs discarded for any reason by this LLDP agent on the indicated port.</p>
lldpStatsRxPortTLVsUnrecognizedTotal	<p><b>Syntax:</b> Counter32  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.2.7.1.6  <b>Description:</b> The number of LLDP TLVs received on the given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE Std 802.1AB-2005. An unrecognized TLV may be a basic management TLV from a later LLDP version.</p>
lldpStatsRxPortAgeoutsTotal	<p><b>Syntax:</b> Gauge32  <b>Access:</b> Read-Only  <b>OID:</b> .1.0.8802.1.1.2.1.2.7.1.7  <b>Description:</b> The counter that represents the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired. This counter is similar to lldpStatsRemTablesAgeouts, except that the counter is on a per port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter should be set to zero during agent initialization and its value should not be saved in non-volatile storage. When a port's admin status changes from 'disabled' to 'rxOnly', 'txOnly' or 'txAndRx', the counter associated with the same port should reset to 0. The agent should also flush all remote system information associated with the same port. This counter should be incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, should not change the value of this counter.</p>
lldpStatsTxPortFramesTotal	<p><b>Syntax:</b> Counter32</p>



## 19.1 Supported MIBs

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.2.6.1.2</p> <p><b>Description:</b> The collection of objects which are used to represent LLDP transmission statistics. This group is mandatory for agents which implement the LLDP and have the capability of transmitting LLDP frames.</p>
lldpLocChassisIdSubtype	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.1</p> <p><b>Description:</b> The type of encoding used to identify the chassis associated with the local system.</p>
lldpLocChassisId	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.2</p> <p><b>Description:</b> The string value used to identify the chassis component associated with the local system.</p>
lldpLocPortIdSubtype	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.7.1.2</p> <p><b>Description:</b> The type of port identifier encoding used in the associated 'lldpLocPortId' object.</p>
lldpLocPortId	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.7.1.3</p> <p><b>Description:</b> The string value used to identify the port component associated with a given port in the local system.</p>
lldpLocPortDesc	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.7.1.4</p> <p><b>Description:</b> The string value used to identify the 802 LAN station's port description associated with the local system. If the local agent supports IETF RFC 2863, lldpLocPortDesc object should have the same value of ifDescr object.</p>
lldpLocSysDesc	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.4</p> <p><b>Description:</b> The string value used to identify the system description of the local system. If the local agent supports IETF RFC 3418, lldpLocSysDesc object should have the same value of sysDesc object.</p>
lldpLocSysName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.3</p> <p><b>Description:</b> The string value used to identify the system name of the local system. If the local agent supports IETF RFC 3418, lldpLocSysName object should have the same value of sysName object.</p>
lldpLocSysCapSupported	<p><b>Syntax:</b> Hex-String</p>

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.5</p> <p><b>Description:</b> The bitmap value used to identify which system capabilities are supported on the local system.</p>
lldpLocSysCapEnabled	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.6</p> <p><b>Description:</b> The bitmap value used to identify which system capabilities are enabled on the local system.</p>
lldpLocManAddrLen	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.8.1.3</p> <p><b>Description:</b> The total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP will not be required to implement an iana family numbers/address length equivalency table in order to decode the management address.</p>
lldpLocManAddrIfSubtype	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.8.1.4</p> <p><b>Description:</b> The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the local system.</p>
lldpLocManAddrIfId	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.3.8.1.5</p> <p><b>Description:</b> The integer value used to identify the interface number regarding the management address component associated with the local system.</p>
lldpLocManAddrOID	<p><b>Syntax:</b> OID</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.8802.1.1.2.1.3.8.1.6</p> <p><b>Description:</b> The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.</p>
lldpRemChassisIdSubtype	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.4</p> <p><b>Description:</b> The type of encoding used to identify the chassis associated with the remote system.</p>
lldpRemChassisId	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.5</p> <p><b>Description:</b> The string value used to identify the chassis component associated with the remote system.</p>

## 19.1 Supported MIBs

Object	Description
IldpRemPortIdSubtype	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.6</p> <p><b>Description:</b> The type of port identifier encoding used in the associated 'IldpRemPortId' object.</p>
IldpRemPortId	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.7</p> <p><b>Description:</b> The string value used to identify the port component associated with the remote system.</p>
IldpRemPortDesc	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.8</p> <p><b>Description:</b> The string value used to identify the description of the given port associated with the remote system.</p>
IldpRemSysName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.9</p> <p><b>Description:</b> The string value used to identify the system name of the remote system.</p>
IldpRemSysDesc	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.10</p> <p><b>Description:</b> The string value used to identify the system description of the remote system.</p>
IldpRemSysCapSupported	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.11</p> <p><b>Description:</b> The bitmap value used to identify which system capabilities are supported on the remote system.</p>
IldpRemSysCapEnabled	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.1.1.12</p> <p><b>Description:</b> The bitmap value used to identify which system capabilities are enabled on the remote system.</p>
IldpRemManAddrIfSubtype	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.2.1.3</p> <p><b>Description:</b> The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system.</p>
IldpRemManAddrIfId	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.0.8802.1.1.2.1.4.2.1.4</p>

Object	Description
	<b>Description:</b> The integer value used to identify the interface number regarding the management address component associated with the remote system.
IldpRemManAddrOID	<b>Syntax:</b> OID <b>Access:</b> Read-Only <b>OID:</b> .1.0.8802.1.1.2.1.4.2.1.5 <b>Description:</b> The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.
IldpRemUnknownTLVInfo	<b>OID:</b> .1.0.8802.1.1.2.1.4.3.1.2 <b>Description:</b> This object represents the value extracted from the value field of the TLV.
IldpRemOrgDefInfo	<b>OID:</b> .1.0.8802.1.1.2.1.4.4.1.4 <b>Description:</b> The string value used to identify the organizationally defined information of the remote system. The encoding for this object should be as defined for SnmpAdminString TC.

## Q-BRIDGE-MIB

Object	Description
dot1qVlanVersionNumber	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.7.1.1.1 <b>Description:</b> The version number of IEEE 802.1Q that this device supports.
dot1qMaxVlanId	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.7.1.1.2 <b>Description:</b> The maximum IEEE 802.1Q VLAN-ID that this device supports.
dot1qMaxSupportedVlans	<b>Syntax:</b> Gauge32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.7.1.1.3 <b>Description:</b> The maximum number of IEEE 802.1Q VLANs that this device supports.
dot1qNumVlans	<b>Syntax:</b> Gauge32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.7.1.1.4 <b>Description:</b> The current number of IEEE 802.1Q VLANs that are configured in this device.
dot1qGvrpStatus	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.17.7.1.1.5 <b>Description:</b> The administrative status requested by management for GVRP. The value enabled(1) indicates that GVRP should be enabled on this device, on all ports for which it has not been specifically disabled. When disabled(2), GVRP is disabled on all ports, and all GVRP packets will be forwarded transparently. This object affects all GVRP Applicant and Registrar

## 19.1 Supported MIBs

Object	Description
	state machines. A transition from disabled(2) to enabled(1) will cause a reset of all GVRP state machines on all ports. The value of this object MUST be retained across reinitializations of the management system.
dot1qVlanNumDeletes	<p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.1</p> <p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>Description:</b> The number of times a VLAN entry has been deleted from the dot1qVlanCurrentTable (for any reason). If an entry is deleted, then inserted, and then deleted, this counter will be incremented by 2.</p>
dot1qVlanFdbld	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.2.1.3</p> <p><b>Description:</b> The number of times a VLAN entry has been deleted from the dot1qVlanCurrentTable (for any reason). If an entry is deleted, then inserted, and then deleted, this counter will be incremented by 2.</p>
dot1qVlanCurrentEgressPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.2.1.4</p> <p><b>Description:</b> The set of ports that are transmitting traffic for this VLAN as either tagged or untagged frames.</p>
dot1qVlanCurrentUntaggedPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.2.1.5</p> <p><b>Description:</b> The set of ports that are transmitting traffic for this VLAN as untagged frames.</p>
dot1qVlanStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.2.1.6</p> <p><b>Description:</b> This object indicates the status of this entry. other(1) - this entry is currently in use, but the conditions under which it will remain so differ from the following values. permanent(2) - this entry, corresponding to an entry in dot1qVlanStaticTable, is currently in use and will remain so after the next reset of the device. The port lists for this entry include ports from the equivalent dot1qVlanStaticTable entry and ports learned dynamically. dynamicGvrp(3) - this entry is currently in use and will remain so until removed by GVRP. There is no static entry for this VLAN, and it will be removed when the last port leaves the VLAN.</p>
dot1qVlanCreationTime	<p><b>Syntax:</b> Timeticks</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.2.1.7</p> <p><b>Description:</b> The value of sysUpTime when this VLAN was created.</p>
dot1qVlanStaticName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.3.1.1</p> <p><b>Description:</b> An administratively assigned string, which may be used to identify the VLAN.</p>
dot1qVlanStaticEgressPorts	<p><b>Syntax:</b> Hex-String</p>

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.3.1.2</p> <p><b>Description:</b> The set of ports that are permanently assigned to the egress list for this VLAN by management. Changes to a bit in this object affect the per-port, per-VLAN Registrar control for Registration Fixed for the relevant GVRP state machine on each port. A port may not be added in this set if it is already a member of the set of ports in dot1qVlanForbiddenEgressPorts. The default value of this object is a string of zeros of appropriate length, indicating not fixed.</p>
dot1qVlanForbiddenEgressPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.3.1.3</p> <p><b>Description:</b> The set of ports that are prohibited by management from being included in the egress list for this VLAN. Changes to this object that cause a port to be included or excluded affect the per-port, per-VLAN Registrar control for Registration Forbidden for the relevant GVRP state machine on each port. A port may not be added in this set if it is already a member of the set of ports in dot1qVlanStaticEgressPorts. The default value of this object is a string of zeros of appropriate length, excluding all ports from the forbidden set.</p>
dot1qVlanStaticUntaggedPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.3.1.4</p> <p><b>Description:</b> The set of ports that should transmit egress packets for this VLAN as untagged. The default value of this object for the default VLAN (dot1qVlanIndex = 1) is a string of appropriate length including all ports. There is no specified default for other VLANs. If a device agent cannot support the set of ports being set, then it will reject the set operation with an error. For example, a manager might attempt to set more than one VLAN to be untagged on egress where the device does not support this IEEE 802.1Q option.</p>
dot1qVlanStaticRowStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.3.1.5</p> <p><b>Description:</b> This object indicates the status of this entry.</p>
dot1qNextFreeLocalVlanIndex	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.4</p> <p><b>Description:</b> The next available value for dot1qVlanIndex of a local VLAN entry in dot1qVlanStaticTable. This will report values <math>\geq 4096</math> if a new Local VLAN may be created or else the value 0 if this is not possible. A row creation operation in this table for an entry with a local VlanIndex value may fail if the current value of this object is not used as the index. Even if the value read is used, there is no guarantee that it will still be the valid index when the create operation is attempted; another manager may have already got in during the intervening time interval. In this case, dot1qNextFreeLocalVlanIndex should be re-read and the creation re-tried with the new value. This value will automatically change when the current value is used to create a new row.</p>
dot1qPvid	<p><b>Syntax:</b> Gauge32</p>

Object	Description
	<p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.5.1.1</p> <p><b>Description:</b> The PVID, the VLAN-ID assigned to untagged frames or Priority-Tagged frames received on this port. The value of this object MUST be retained across reinitializations of the management system.</p>
dot1qPortAcceptableFrameTypes	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.5.1.2</p> <p><b>Description:</b> When this is admitOnlyVlanTagged(2), the device will discard untagged frames or Priority-Tagged frames received on this port. When admitAll(1), untagged frames or Priority-Tagged frames received on this port will be accepted and assigned to a VID based on the PVID and VID Set for this port. This control does not affect VLAN-independent Bridge Protocol Data Unit (BPDU) frames, such as GVRP and Spanning Tree Protocol (STP). It does affect VLAN-dependent BPDU frames, such as GMRP. The value of this object MUST be retained across reinitializations of the management system.</p>
dot1qPortIngressFiltering	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.5.1.3</p> <p><b>Description:</b> When this is true(1), the device will discard incoming frames for VLANs that do not include this Port in its Member set. When false(2), the port will accept all incoming frames. This control does not affect VLAN-independent BPDU frames, such as GVRP and STP. It does affect VLAN-dependent BPDU frames, such as GMRP. The value of this object MUST be retained across reinitializations of the management system.</p>
dot1qPortGvrpStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.4.5.1.4</p> <p><b>Description:</b> The state of GVRP operation on this port. The value enabled(1) indicates that GVRP is enabled on this port, as long as dot1qGvrpStatus is also enabled for this device. When disabled(2) but dot1qGvrpStatus is still enabled for the device, GVRP is disabled on this port: any GVRP packets received will be silently discarded, and no GVRP registrations will be propagated from other ports. This object affects all GVRP Applicant and Registrar state machines on this port. A transition from disabled(2) to enabled(1) will cause a reset of all GVRP state machines on this port. The value of this object MUST be retained across reinitializations of the management system.</p>
dot1qFdbDynamicCount	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.1.1.2</p> <p><b>Description:</b> A collection of objects providing information about all unicast addresses, learned dynamically or statically configured by management, in each Filtering Database.</p>
dot1qTpFdbPort	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.2.1.2</p> <p><b>Description:</b> Either the value '0', or the port number of the port on which a frame having a source address equal to the value of the corresponding instance of dot1qTpFdbAddress has been seen. A value of '0' indicates</p>

Object	Description
	that the port number has not been learned but that the device does have some forwarding/filtering information about this address (e.g., in the dot1qStaticUnicastTable). Implementors are encouraged to assign the port value to this object whenever it is learned, even for addresses for which the corresponding value of dot1qTpFdbStatus is not learned(3).
dot1qTpFdbStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.2.1.3</p> <p><b>Description:</b> The status of this entry. The meanings of the values are:</p> <ul style="list-style-type: none"> <li>• other(1) - none of the following. This may include the case where some other MIB object (not the corresponding instance of dot1qTpFdbPort, nor an entry in the dot1qStaticUnicastTable) is being used to determine if and how frames addressed to the value of the corresponding instance of dot1qTpFdbAddress are being forwarded.</li> <li>• invalid(2) - this entry is no longer valid (e.g., it was learned but has since aged out), but has not yet been flushed from the table.</li> <li>• learned(3) - the value of the corresponding instance of dot1qTpFdbPort was learned and is being used.</li> <li>• self(4) - the value of the corresponding instance of dot1qTpFdbAddress represents one of the device's addresses. The corresponding instance of dot1qTpFdbPort indicates which of the device's ports has this address.</li> <li>• mgmt(5) - the value of the corresponding instance of dot1qTpFdbAddress is also the value of an existing instance of dot1qStaticAddress.</li> </ul>
dot1qTpGroupEgressPorts	<p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.3.1.2</p> <p><b>Description:</b> The complete set of ports, in this VLAN, to which frames destined for this Group MAC address are currently being explicitly forwarded. This does not include ports for which this address is only implicitly forwarded, in the dot1qForwardAllPorts list.</p>
dot1qTpGroupLearnt	<p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.3.1.3</p> <p><b>Description:</b> The subset of ports in dot1qTpGroupEgressPorts that were learned by GMRP or some other dynamic mechanism, in this Filtering database.</p>
dot1qForwardAllPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.4.1.1</p> <p><b>Description:</b> The complete set of ports in this VLAN to which all multicast group-addressed frames are to be forwarded. This includes ports for which this need has been determined dynamically by GMRP, or configured statically by management.</p>
dot1qForwardAllStaticPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.4.1.2</p> <p><b>Description:</b> The set of ports configured by management in this VLAN to which all multicast group-addressed frames are to be forwarded. Ports entered in this list will also appear in the complete set shown by dot1qForwardAllPorts. This value will be restored after the device is reset. This only applies to ports that are members of the VLAN, defined by dot1qVlanCurrentEgressPorts. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardAllForbiddenPorts. The default value is a string of ones of appropriate length, to indicate</p>



## 19.1 Supported MIBs

Object	Description
	the standard behaviour of using basic filtering services, i.e., forward all multicasts to all ports. The value of this object MUST be retained across reinitializations of the management system.
dot1qForwardAllForbiddenPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.4.1.3</p> <p><b>Description:</b> The set of ports configured by management in this VLAN for which the Service Requirement attribute Forward All Multicast Groups may not be dynamically registered by GMRP. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardAllStaticPorts. The default value is a string of zeros of appropriate length. The value of this object MUST be retained across reinitializations of the management system.</p>
dot1qForwardUnregisteredPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.5.1.1</p> <p><b>Description:</b> The complete set of ports in this VLAN to which multicast group-addressed frames for which there is no more specific forwarding information will be forwarded. This includes ports for which this need has been determined dynamically by GMRP, or configured statically by management.</p>
dot1qForwardUnregisteredStaticPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.5.1.2</p> <p><b>Description:</b> The set of ports configured by management, in this VLAN, to which multicast group-addressed frames for which there is no more specific forwarding information are to be forwarded. Ports entered in this list will also appear in the complete set shown by dot1qForwardUnregisteredPorts. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardUnregisteredForbiddenPorts. The default value is a string of zeros of appropriate length, although this has no effect with the default value of dot1qForwardAllStaticPorts. The value of this object MUST be retained across reinitializations of the management system.</p>
dot1qForwardUnregisteredForbiddenPorts	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.17.7.1.2.5.1.3</p> <p><b>Description:</b> The set of ports configured by management in this VLAN for which the Service Requirement attribute Forward Unregistered Multicast Groups may not be dynamically registered by GMRP. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardUnregisteredStaticPorts. The default value is a string of zeros of appropriate length. The value of this object MUST be retained across reinitializations of the management system.</p>

## RUGGEDCOM-SYS-INFO-MIB

Object	Description
rcDeviceErrBootupError	<b>Syntax:</b> String

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.1</p> <p><b>Description:</b> The error discovered during bootup process. If there was no error during device bootup, zero length string will be retrieved.</p>
rcDeviceErrWatchdogReset	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.2</p> <p><b>Description:</b> Indicates whether the last device reboot was caused by watchdog.</p>
rcDeviceErrConfigurationFailure	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.3</p> <p><b>Description:</b> Indicates whether errors were detected while applying configuration settings from configuration file. Configuration is updated from the configuration file at bootup time when file is loaded from nonvolatile memory, or when new file is downloaded to the device. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.</p>
rcDeviceErrCrashLogCreated	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.4</p> <p><b>Description:</b> Indicates whether the device error that caused creation of an entry in crashlog.txt file was detected. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.</p>
rcDeviceErrStackOverflow	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.5</p> <p><b>Description:</b> Indicates whether the stack of any of the system tasks is used over the system threshold. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.</p>
rcDeviceErrHeapError	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.6</p> <p><b>Description:</b> Indicates whether the system memory corruption was detected. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.</p>
rcDeviceErrDateAndTimeSetFailed	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.7</p> <p><b>Description:</b> Indicates whether the date and time setting in the device failed. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.</p>
rcDeviceErrNtpServerUnreachable	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.8</p>

## 19.1 Supported MIBs

Object	Description
	<b>Description:</b> Indicates whether the NTP server (if required) can be reached. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.
rcDeviceErrBootPTftpTrFailed	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.9 <b>Description:</b> Indicates whether the the file was transferred properly after obtaining IP address from the BootP server. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.
rcDeviceErrRadiusServerUnreachable	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.10 <b>Description:</b> Indicates whether the RADIUS server (if required) can be reached. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.
rcDeviceErrTacacsServerUnreachable	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.1.11 <b>Description:</b> Indicates whether the TACACS+ server (if required) can be reached. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.
rcDeviceStsTemperature	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.2.3 <b>Description:</b> The temperature measured in the device.
rcDeviceStsPowerSupply1	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.2.4 <b>Description:</b> Indicates the status of Power Supply Module 1. Whenever the value of this object changes from functional(2) to notFunctional(3), or from notFunctional(3) to functional(2), the device will generate powerSupplyTrap notification.
rcDeviceStsPowerSupply2	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.2.5 <b>Description:</b> Indicates the status of Power Supply Module 2. Whenever the value of this object changes from functional(2) to notFunctional(3), or from notFunctional(3) to functional(2), the device will generate powerSupplyTrap notification.
rcDeviceInfoMainBoardType	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.4 <b>Description:</b> The identification code of the device main board.
rcDeviceInfoTotalRam	<b>Syntax:</b> Integer <b>Access:</b> Read-Only

Object	Description
	<b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.5 <b>Description:</b> The total number of bytes of RAM in the system control CPU.
rcDeviceInfoBootSwVersion	<b>Syntax:</b> String <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.2 <b>Description:</b> The version and the build date of the boot loader software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length string to any string of non-zero length, the device will generate swUpgradeTrap notification.
rcDeviceInfoMainSwVersion	<b>Syntax:</b> String <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.3 <b>Description:</b> The version and the build date of the main operating system software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length string to any string of non-zero length, the device will generate swUpgradeTrap notification.
rcDeviceInfoPendingBootSwVersion	<b>Syntax:</b> String <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.6 <b>Description:</b> The version and the build date of the boot loader software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length string to any string of non-zero length, the device will generate swUpgradeTrap notification.
rcDeviceInfoPendingMainSwVersion	<b>Syntax:</b> String <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.7 <b>Description:</b> The version and the build date of the main operating system software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length string to any string of non-zero length, the device will generate swUpgradeTrap notification.
rcDeviceInfoCfgRevision	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.8 <b>Description:</b> The configuration file revision. The revision number will be updated whenever file is saved to the flash memory. This number is recorded in config.csv at the time file is uploaded from the device. Whenever the value of this object changes the device will generate cfgChangeTrap notification.
rcDeviceInfoSerialNumber	<b>Syntax:</b> String <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.1 <b>Description:</b> The manufacturing serial number of the device.
rcDeviceCommReset	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.4.1

## 19.1 Supported MIBs

Object	Description
	<b>Description:</b> Setting the value of this object to 'true(1)' will cause device to reboot. As a result of Read request the agent will return value 'false(2)'.
rcDeviceCommLoadDefaultCfg	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.4.1.15004.4.2.4.2 <b>Description:</b> Setting the value of this object to 'true(1)' will force device to load default configuration to all tables. As a result of Read request the agent will return value 'false(2)'.
rcDeviceCommClearAlarms	<b>Syntax:</b> Integer <b>Access:</b> Read-Write <b>OID:</b> 1.3.6.1.4.1.15004.4.2.4.3 <b>Description:</b> Setting the value of this object to 'true(1)' will cause device to clear all alarms. As a result of Read request the agent will return value 'false(2)'.
rcDeviceCommClearSyslog	<b>Syntax:</b> Integer <b>Access:</b> Read-Write <b>OID:</b> 1.3.6.1.4.1.15004.4.2.4.4 <b>Description:</b> Setting the value of this object to 'true(1)' will cause device to clear syslog.txt file. As a result of Read request the agent will return value 'false(2)'.
rcDeviceCommClearLogs	<b>Syntax:</b> Integer <b>Access:</b> Read-Write <b>OID:</b> 1.3.6.1.4.1.15004.4.2.4.5 <b>Description:</b> Setting the value of this object to 'true(1)' will cause device to clear syslog.txt and crashlog.txt files. As a result of Read request the agent will return value 'false(2)'.

## RC-IEC-62439-3-MIB

Object	Description
lreInterfaceConfigIndex	<b>Syntax:</b> Gauge32 <b>Access:</b> Read-Only <b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.1 <b>Description:</b> A unique value for each LRE.
lreRowStatus	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.2 <b>Description:</b> Indicates the status of the LRE table entry.
lreNodeType	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.3 <b>Description:</b> Specifies the operation mode of the LRE: <ul style="list-style-type: none"> <li>• PRP mode 1 (1).</li> <li>• HSR mode (2).</li> </ul>

Object	Description
	<p><b>Note</b></p> <p>PRP mode 0 is considered deprecated and is not supported by this revision of the MIB.</p>
IreNodeName	<p><b>Syntax:</b> Octets</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.4</p> <p><b>Description:</b> Specifies this LRE's node name.</p>
IreVersionName	<p><b>Syntax:</b> Octets</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.5</p> <p><b>Description:</b> Specifies the version of this LRE's software.</p>
IreMacAddress	<p><b>Syntax:</b> Octets</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.6</p> <p><b>Description:</b> Specifies the MAC address to be used by this LRE. MAC addresses are identical for all ports of a single LRE.</p>
IrePortAdminStateA	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.7</p> <p><b>Description:</b> Specifies whether the port A shall be active or not Active through administrative action (Default: active).</p>
IrePortAdminStateB	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.8</p> <p><b>Description:</b> Specifies whether the port B shall be active or not Active through administrative action (Default: active).</p>
IreLinkStatusA	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.9</p> <p><b>Description:</b> Shows the actual link status of the LRE's port A.</p>
IreLinkStatusB	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.10</p> <p><b>Description:</b> Shows the actual link status of the LRE's port B.</p>
IreDuplicateDiscard	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.11</p> <p><b>Description:</b> Specifies whether a duplicate discard algorithm is used at reception (Default: discard).</p>
IreTransparentReception	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.12</p>

Object	Description
	<p><b>Description:</b> If removeRCT is configured, the RCT is removed when forwarding to the upper layers, only applicable for PRP LRE (Default: removeRCT).</p>
IreHsrLREMode	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.13</p> <p><b>Description:</b> This enumeration is only applicable if the LRE is an HSR bridging node or RedBox. It shows the mode of the HSR LRE:</p> <ul style="list-style-type: none"> <li>• (1) Default mode: The HSR LRE is in mode h and bridges tagged HSR traffic.</li> <li>• (2) Optional mode: The HSR LRE is in mode n and bridging between its HSR ports is disabled. Traffic is HSR tagged.</li> <li>• (3) Optional mode: The HSR LRE is in mode t and bridges non-tagged HSR traffic between its HSR ports.</li> <li>• (4) Optional mode: The HSR LRE is in mode u and behaves like in mode h, except it does not remove unicast messages.</li> <li>• (5) Optional mode: The HSR LRE is configured in mixed mode. HSR frames are handled according to mode h. Non-HSR frames are handled according to 802.1D bridging rules.</li> </ul>
IreSwitchingEndNode	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.14</p> <p><b>Description:</b> This enumeration shows which feature is enabled in this particular LRE:</p> <ul style="list-style-type: none"> <li>• (1): an unspecified non-bridging node, e.g. SRP.</li> <li>• (2): an unspecified bridging node, e.g. RSTP.</li> <li>• (3): a PRP node/RedBox.</li> <li>• (4): an HSR RedBox with regular Ethernet traffic on its interlink.</li> <li>• (5): an HSR switching node.</li> <li>• (6): an HSR RedBox with HSR tagged traffic on its interlink.</li> <li>• (7): an HSR RedBox with PRP traffic for LAN A on its interlink.</li> <li>• (8): an HSR RedBox with PRP traffic for LAN B on its interlink.</li> </ul>
IreRedBoxIdentity	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.15</p> <p><b>Description:</b> Applicable to RedBox HSR-PRP A and RedBox HSR-PRP B. One ID is used by one pair of RedBoxes (one configured to A and one configured to B) coupling an HSR ring to a PRP network. The integer value states the value of the path field a RedBox inserts into each frame it receives from its interlink and injects into the HSR ring. When interpreted as binary values, the LSB denotes the configuration of the RedBox (A or B), and the following 3 bits denote the identifier of a RedBox pair.</p>
IreEvaluateSupervision	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.16</p> <p><b>Description:</b> True if the LRE evaluates received supervision frames. False if it drops the supervision frames without evaluating. Note: LREs are required</p>

Object	Description
	to send supervision frames, but reception is optional. Default value is dependent on implementation.
IreNodesTableClear	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.17 <b>Description:</b> Specifies that the Node Table is to be cleared.
IreProxyNodeTableClear	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.0.62439.2.21.0.1.0.1.1.18 <b>Description:</b> Specifies that the Proxy Node Table is to be cleared.

### SNMP-FRAMEWORK-MIB

Object	Description
snmpEngineID	<b>Syntax:</b> Hex-String <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.6.3.10.2.1.1 <b>Description:</b> An SNMP engine's administratively-unique identifier. This information SHOULD be stored in non-volatile storage so that it remains constant across re-initializations of the SNMP engine.
snmpEngineBoots	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.6.3.10.2.1.2 <b>Description:</b> The number of times that the SNMP engine has (re-)initialized itself since snmpEngineID was last configured.
snmpEngineTime	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.6.3.10.2.1.3 <b>Description:</b> The number of seconds since the value of the snmpEngineBoots object last changed. When incrementing this object's value would cause it to exceed its maximum, snmpEngineBoots is incremented as if a re-initialization had occurred, and this object's value consequently reverts to zero.
snmpEngineMaxMessageSize	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.6.3.10.2.1.4 <b>Description:</b> The maximum length in octets of an SNMP message which this SNMP engine can send or receive and process, determined as the minimum of the maximum message size values supported among all of the transports available to and supported by the engine.

### SNMP-USER-BASED-SM-MIB

Object	Description
usmStatsUnsupportedSecLevels	<b>Syntax:</b> Counter32



## 19.1 Supported MIBs

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.1.1</p> <p><b>Description:</b> The total number of packets received by the SNMP engine which were dropped because they requested a securityLevel that was unknown to the SNMP engine or otherwise unavailable.</p>
usmStatsNotInTimeWindows	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.1.2</p> <p><b>Description:</b> The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.</p>
usmStatsUnknownUserNames	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.1.3</p> <p><b>Description:</b> The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.</p>
usmStatsUnknownEngineIDs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.1.4</p> <p><b>Description:</b> The total number of packets received by the SNMP engine which were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.</p>
usmStatsWrongDigests	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.1.5</p> <p><b>Description:</b> The total number of packets received by the SNMP engine which were dropped because they didn't contain the expected digest value.</p>
usmStatsDecryptionErrors	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.1.6</p> <p><b>Description:</b> The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.</p>
usmUserSpinLock	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.1</p> <p><b>Description:</b> An advisory lock used to allow several cooperating Command Generator Applications to coordinate their use of facilities to alter secrets in the usmUserTable.</p>
usmUserSecurityName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.3</p> <p><b>Description:</b> A human readable string representing the user in Security Model independent format. The default transformation of the User-based Security Model dependent security ID to the securityName and vice versa is the identity function so that the securityName is the same as the userName.</p>

Object	Description
usmUserCloneFrom	<p><b>Syntax:</b> OID</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.4</p> <p><b>Description:</b> A pointer to another conceptual row in this usmUserTable. The user in this other conceptual row is called the clone-from user. When a new user is created (i.e., a new conceptual row is instantiated in this table), the privacy and authentication parameters of the new user must be cloned from its clone-from user. These parameters are: - authentication protocol (usmUserAuthProtocol) - privacy protocol (usmUserPrivProtocol) They will be copied regardless of what the current value is. Cloning also causes the initial values of the secret authentication key (authKey) and the secret encryption key (privKey) of the new user to be set to the same values as the corresponding secrets of the clone-from user to allow the KeyChange process to occur as required during user creation. The first time an instance of this object is set by a management operation (either at or after its instantiation), the cloning process is invoked. Subsequent writes are successful but invoke no action to be taken by the receiver. The cloning process fails with an 'inconsistentName' error if the conceptual row representing the clone-from user does not exist or is not in an active state when the cloning process is invoked. When this object is read, the ZeroDotZero OID is returned.</p>
usmUserAuthProtocol	<p><b>Syntax:</b> OID</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.5</p> <p><b>Description:</b> An indication of whether messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, can be authenticated, and if so, the type of authentication protocol which is used. An instance of this object is created concurrently with the creation of any other object instance for the same user (i.e., as part of the processing of the set operation which creates the first object instance in the same conceptual row). If an initial set operation (i.e. at row creation time) tries to set a value for an unknown or unsupported protocol, then a 'wrongValue' error must be returned. The value will be overwritten/set when a set operation is performed on the corresponding instance of usmUserCloneFrom. Once instantiated, the value of such an instance of this object can only be changed via a set operation to the value of the usmNoAuthProtocol. If a set operation tries to change the value of an existing instance of this object to any value other than usmNoAuthProtocol, then an 'inconsistentValue' error must be returned. If a set operation tries to set the value to the usmNoAuthProtocol while the usmUserPrivProtocol value in the same row is not equal to usmNoPrivProtocol, then an 'inconsistentValue' error must be returned. That means that an SNMP command generator application must first ensure that the usmUserPrivProtocol is set to the usmNoPrivProtocol value before it can set the usmUserAuthProtocol value to usmNoAuthProtocol.</p>
usmUserAuthKeyChange	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.6</p> <p><b>Description:</b> An object, which when modified, causes the secret authentication key used for messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, to be modified via a one-way function. The associated protocol is the usmUserAuthProtocol. The associated secret key is the user's secret authentication key (authKey). The associated hash algorithm is the algorithm used by the user's</p>

Object	Description
	<p>usmUserAuthProtocol. When creating a new user, it is an 'inconsistentName' error for a set operation to refer to this object unless it is previously or concurrently initialized through a set operation on the corresponding instance of usmUserCloneFrom. When the value of the corresponding usmUserAuthProtocol is usmNoAuthProtocol, then a set is successful, but effectively is a no-op. When this object is read, the zero-length (empty) string is returned. The recommended way to do a key change is as follows: 1) GET(usmUserSpinLock.0) and save in sValue. 2) generate the keyChange value based on the old (existing) secret key and the new secret key, let us call this kcValue. If you do the key change on behalf of another user: 3) SET(usmUserSpinLock.0=sValue, usmUserAuthKeyChange=kcValue usmUserPublic=randomValue) If you do the key change for yourself: 4) SET(usmUserSpinLock.0=sValue, usmUserOwnAuthKeyChange=kcValue usmUserPublic=randomValue) If you get a response with error-status of noError, then the SET succeeded and the new key is active. If you do not get a response, then you can issue a GET(usmUserPublic) and check if the value is equal to the randomValue you did send in the SET. If so, then the key change succeeded and the new key is active (probably the response got lost). If not, then the SET request probably never reached the target and so you can start over with the procedure above.</p>
usmUserOwnAuthKeyChange	<p><b>Syntax:</b> String  <b>Access:</b> Read-Only  <b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.7  <b>Description:</b> Behaves exactly as usmUserAuthKeyChange, with one notable difference: in order for the set operation to succeed, the usmUserName of the operation requester must match the usmUserName that indexes the row which is targeted by this operation. In addition, the USM security model must be used for this operation. The idea here is that access to this column can be public, since it will only allow a user to change his own secret authentication key (authKey). Note that this can only be done once the row is active. When a set is received and the usmUserName of the requester is not the same as the usmUserName that indexes the row which is targeted by this operation, then a 'noAccess' error must be returned. When a set is received and the security model in use is not USM, then a 'noAccess' error must be returned.</p>
usmUserPrivProtocol	<p><b>Syntax:</b> OID  <b>Access:</b> Read-Only  <b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.8  <b>Description:</b> An indication of whether messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, can be protected from disclosure, and if so, the type of privacy protocol which is used. An instance of this object is created concurrently with the creation of any other object instance for the same user (i.e., as part of the processing of the set operation which creates the first object instance in the same conceptual row). If an initial set operation (i.e. at row creation time) tries to set a value for an unknown or unsupported protocol, then a 'wrongValue' error must be returned. The value will be overwritten/set when a set operation is performed on the corresponding instance of usmUserCloneFrom. Once instantiated, the value of such an instance of this object can only be changed via a set operation to the value of the usmNoPrivProtocol. If a set operation tries to change the value of an existing instance of this object to any value other than usmNoPrivProtocol, then an 'inconsistentValue' error must be returned. Note that if any privacy protocol is used, then you must also use an authentication protocol. In other words, if usmUserPrivProtocol is set to anything else than usmNoPrivProtocol, then</p>

Object	Description
	the corresponding instance of usmUserAuthProtocol cannot have a value of usmNoAuthProtocol. If it does, then an 'inconsistentValue' error must be returned.
usmUserPrivKeyChange	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.9</p> <p><b>Description:</b> An object, which when modified, causes the secret encryption key used for messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, to be modified via a one-way function. The associated protocol is the usmUserPrivProtocol. The associated secret key is the user's secret privacy key (privKey). The associated hash algorithm is the algorithm used by the user's usmUserAuthProtocol. When creating a new user, it is an 'inconsistentName' error for a set operation to refer to this object unless it is previously or concurrently initialized through a set operation on the corresponding instance of usmUserCloneFrom. When the value of the corresponding usmUserPrivProtocol is usmNoPrivProtocol, then a set is successful, but effectively is a no-op. When this object is read, the zero-length (empty) string is returned. See the description clause of usmUserAuthKeyChange for a recommended procedure to do a key change.</p>
usmUserOwnPrivKeyChange	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.10</p> <p><b>Description:</b> Behaves exactly as usmUserPrivKeyChange, with one notable difference: in order for the Set operation to succeed, the usmUserName of the operation requester must match the usmUserName that indexes the row which is targeted by this operation. In addition, the USM security model must be used for this operation. The idea here is that access to this column can be public, since it will only allow a user to change his own secret privacy key (privKey). Note that this can only be done once the row is active. When a set is received and the usmUserName of the requester is not the same as the usmUserName that indexes the row which is targeted by this operation, then a 'noAccess' error must be returned. When a set is received and the security model in use is not USM, then a 'noAccess' error must be returned.</p>
usmUserPublic	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.11</p> <p><b>Description:</b> A publicly-readable value which can be written as part of the procedure for changing a user's secret authentication and/or privacy key, and later read to determine whether the change of the secret was effected.</p>
usmUserStorageType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.12</p> <p><b>Description:</b> The storage type for this conceptual row. Conceptual rows having the value 'permanent' must allow write-access at a minimum to: - usmUserAuthKeyChange, usmUserOwnAuthKeyChange and usmUserPublic for a user who employs authentication, and - usmUserPrivKeyChange, usmUserOwnPrivKeyChange and usmUserPublic for a user who employs privacy. Note that any user who employs authentication or privacy must allow its secret(s) to be updated and thus cannot be 'readOnly'. If an initial set operation tries to set the value to 'readOnly' for a user who employs authentication or privacy, then an 'inconsistentValue' error must be returned. Note that if the value has been previously set (implicit or</p>

## 19.1 Supported MIBs

Object	Description
	explicit) to any value, then the rules as defined in the StorageType Textual Convention apply. It is an implementation issue to decide if a SET for a readOnly or permanent row is accepted at all. In some contexts this may make sense, in others it may not. If a SET for a readOnly or permanent row is not accepted at all, then a 'wrongValue' error must be returned.
usmUserStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.15.1.2.2.1.13</p> <p><b>Description:</b> The status of this conceptual row. Until instances of all corresponding columns are appropriately configured, the value of the corresponding instance of the usmUserStatus column is 'notReady'. In particular, a newly created row for a user who employs authentication, cannot be made active until the corresponding usmUserCloneFrom and usmUserAuthKeyChange have been set. Further, a newly created row for a user who also employs privacy, cannot be made active until the usmUserPrivKeyChange has been set. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified, except for usmUserOwnAuthKeyChange and usmUserOwnPrivKeyChange. For these 2 objects, the value of usmUserStatus MUST be active.</p>

## SNMPv2-MIB

Object	Description
snmplnPkts	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.1</p> <p><b>Description:</b> The total number of messages delivered to the SNMP entity from the transport service.</p>
snmplnBadVersions	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.3</p> <p><b>Description:</b> The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.</p>
snmplnASNParseErrs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.6</p> <p><b>Description:</b> The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.</p>
snmpSilentDrops	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.31</p> <p><b>Description:</b> The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response Class PDU (such as a Response-PDU) with an empty variable-bindings field</p>

Object	Description
	was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.32</p> <p><b>Description:</b> The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response Class PDU (such as a Response-PDU) could be returned.</p>
snmpEnableAuthenTraps	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Write</p> <p><b>OID:</b> 1.3.6.1.2.1.11.30</p> <p><b>Description:</b> Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant across re-initializations of the network management system.</p>
snmpInBadCommunityNames	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.4</p> <p><b>Description:</b> The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which used an SNMP community name not known to said entity. Also, implementations which authenticate community-based SNMP messages using check(s) in addition to matching the community name (for example, by also checking whether the message originated from a transport address allowed to use a specified community name) MAY include in this value the number of messages which failed the additional check(s). It is strongly recommended that the documentation for any security model which is used to authenticate community-based SNMP messages specify the precise conditions that contribute to this value.</p>
snmpInBadCommunityUses	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.11.5</p> <p><b>Description:</b> A collection of objects providing basic instrumentation of a SNMP entity which supports community-based authentication.</p>
snmpSetSerialNo	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.1.1.6.1</p> <p><b>Description:</b> An advisory lock used to allow several cooperating command generator applications to coordinate their use of the SNMP set operation. This object is used for coarse-grain coordination. To achieve fine-grain coordination, one or more similar objects might be defined within each MIB group, as appropriate.</p>

## SNMP-VIEW-BASED-ACM-MIB

Object	Description
vacmContextName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.1.1.1</p> <p><b>Description:</b> A human readable name identifying a particular context at a particular SNMP entity. The empty contextName (zero length) represents the default context.</p>
vacmGroupName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.2.1.3</p> <p><b>Description:</b> The name of the group to which this entry (e.g., the combination of securityModel and securityName) belongs. This groupName is used as index into the vacmAccessTable to select an access control policy. However, a value in this table does not imply that an instance with the value exists in table vacmAccessTable.</p>
vacmSecurityToGroupStorageType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.2.1.4</p> <p><b>Description:</b> The storage type for this conceptual row. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row.</p>
vacmSecurityToGroupStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.2.1.5</p> <p><b>Description:</b> The status of this conceptual row. Until instances of all corresponding columns are appropriately configured, the value of the corresponding instance of the vacmSecurityToGroupStatus column is 'notReady'. In particular, a newly created row cannot be made active until a value has been set for vacmGroupName. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified.</p>
vacmAccessContextMatch	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.4.1.4</p> <p><b>Description:</b> If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected. If the value of this object is prefix(2), then all rows where the contextName whose starting octets exactly match vacmAccessContextPrefix are selected. This allows for a simple form of wildcarding.</p>
vacmAccessReadViewName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.4.1.5</p> <p><b>Description:</b> The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes read access. The identified MIB view is that one for which the vacmViewTreeFamilyViewName has the same value as the instance of this</p>

Object	Description
	object; if the value is the empty string or if there is no active MIB view having this value of vacmViewTreeFamilyViewName, then no access is granted.
vacmAccessWriteViewName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.4.1.6</p> <p><b>Description:</b> The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes write access. The identified MIB view is that one for which the vacmViewTreeFamilyViewName has the same value as the instance of this object; if the value is the empty string or if there is no active MIB view having this value of vacmViewTreeFamilyViewName, then no access is granted.</p>
vacmAccessNotifyViewName	<p><b>Syntax:</b> String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.4.1.7</p> <p><b>Description:</b> The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes access for notifications. The identified MIB view is that one for which the vacmViewTreeFamilyViewName has the same value as the instance of this object; if the value is the empty string or if there is no active MIB view having this value of vacmViewTreeFamilyViewName, then no access is granted.</p>
vacmAccessStorageType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.4.1.8</p> <p><b>Description:</b> The storage type for this conceptual row. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row.</p>
vacmAccessStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.4.1.9</p> <p><b>Description:</b> The status of this conceptual row. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified.</p>
vacmViewSpinLock	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.5.1</p> <p><b>Description:</b> An advisory lock used to allow cooperating SNMP Command Generator applications to coordinate their use of the Set operation in creating or modifying views. When creating a new view or altering an existing view, it is important to understand the potential interactions with other uses of the view. The vacmViewSpinLock should be retrieved. The name of the view to be created should be determined to be unique by the SNMP Command Generator application by consulting the vacmViewTreeFamilyTable. Finally, the named view may be created (Set), including the advisory lock. If another SNMP Command Generator application has altered the views in the meantime, then the spin lock's value will have changed, and so this creation will fail because it will specify the wrong value for the spin lock. Since this is an advisory lock, the use of this lock is not enforced.</p>
vacmViewTreeFamilyMask	<p><b>Syntax:</b> String</p>



Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.5.2.1.3</p> <p><b>Description:</b> Locally held information about families of subtrees within MIB views. Each MIB view is defined by two sets of view subtrees: - the included view subtrees, and - the excluded view subtrees. Every such view subtree, both the included and the excluded ones, is defined in this table. To determine if a particular object instance is in a particular MIB view, compare the object instance's OBJECT IDENTIFIER with each of the MIB view's active entries in this table. If none match, then the object instance is not in the MIB view. If one or more match, then the object instance is included in, or excluded from, the MIB view according to the value of vacmViewTreeFamilyType in the entry whose value of vacmViewTreeFamilySubtree has the most sub-identifiers. If multiple entries match and have the same number of sub-identifiers (when wildcarding is specified with the value of vacmViewTreeFamilyMask), then the lexicographically greatest instance of vacmViewTreeFamilyType determines the inclusion or exclusion. An object instance's OBJECT IDENTIFIER X matches an active entry in this table when the number of sub-identifiers in X is at least as many as in the value of vacmViewTreeFamilySubtree for the entry, and each sub-identifier in the value of vacmViewTreeFamilySubtree matches its corresponding sub-identifier in X. Two sub-identifiers match either if the corresponding bit of the value of vacmViewTreeFamilyMask for the entry is zero (the 'wild card' value), or if they are equal. A 'family' of subtrees is the set of subtrees defined by a particular combination of values of vacmViewTreeFamilySubtree and vacmViewTreeFamilyMask. In the case where no 'wild card' is defined in the vacmViewTreeFamilyMask, the family of subtrees reduces to a single subtree. When creating or changing MIB views, an SNMP Command Generator application should utilize the vacmViewSpinLock to try to avoid collisions. See DESCRIPTION clause of vacmViewSpinLock. When creating MIB views, it is strongly advised that first the 'excluded' vacmViewTreeFamilyEntries are created and then the 'included' entries. When deleting MIB views, it is strongly advised that first the 'included' vacmViewTreeFamilyEntries are deleted and then the 'excluded' entries. If a create for an entry for instance-level access control is received and the implementation does not support instance-level granularity, then an inconsistentName error must be returned.</p>
vacmViewTreeFamilyType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.5.2.1.4</p> <p><b>Description:</b> Indicates whether the corresponding instances of vacmViewTreeFamilySubtree and vacmViewTreeFamilyMask define a family of view subtrees which is included in or excluded from the MIB view.</p>
vacmViewTreeFamilyStorageType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.5.2.1.5</p> <p><b>Description:</b> The storage type for this conceptual row. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row.</p>
vacmViewTreeFamilyStatus	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.6.3.16.1.5.2.1.6</p> <p><b>Description:</b> The status of this conceptual row. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances</p>

Object	Description
	other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified.

**BGP4-MIB**

Object	Description
bgpVersion	<p><b>Syntax:</b> Hex-String</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.15.1</p> <p><b>Description:</b> Vector of supported BGP protocol version numbers. Each peer negotiates the version from this vector. Versions are identified via the string of bits contained within this object. The first octet contains bits 0 to 7, the second octet contains bits 8 to 15, and so on, with the most significant bit referring to the lowest bit number in the octet (e.g., the MSB of the first octet refers to bit 0). If a bit, <i>i</i>, is present and set, then the version (<i>i</i>+1) of the BGP is supported.</p>
bgpLocalAs	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.15.2</p> <p><b>Description:</b> The local autonomous system number.</p>
bgpIdentifier	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.15.4</p> <p><b>Description:</b> The BGP Identifier of the local system.</p>

**IP-FORWARD-MIB**

Object	Description
ipCidrRouteNumber	<p><b>Syntax:</b> Gauge32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.3</p> <p><b>Description:</b> The number of current ipCidrRouteTable entries that are not invalid. This object is deprecated in favor of inetCidrRouteNumber and the inetCidrRouteTable.</p>
ipCidrRouteDest	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.1</p> <p><b>Description:</b> The destination IP address of this route. This object may not take a Multicast (Class D) address value. Any assignment (implicit or otherwise) of an instance of this object to a value <i>x</i> must be rejected if the bitwise logical-AND of <i>x</i> with the value of the corresponding instance of the ipCidrRouteMask object is not equal to <i>x</i>.</p>
ipCidrRouteNextHop	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.4</p>

Object	Description
	<b>Description:</b> On remote routes, the address of the next system en route; Otherwise, 0.0.0.0.
ipCidrRouteType	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.6 <b>Description:</b> The type of route. Note that local(3) refers to a route for which the next hop is the final destination; remote(4) refers to a route for which the next hop is not the final destination. Routes that do not result in traffic forwarding or rejection should not be displayed, even if the implementation keeps them stored internally. reject (2) refers to a route that, if matched, discards the message as unreachable. This is used in some protocols as a means of correctly aggregating routes.
ipCidrRouteInfo	<b>Syntax:</b> OID <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.9 <b>Description:</b> A reference to MIB definitions specific to the particular routing protocol that is responsible for this route, as determined by the value specified in the route's ipCidrRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntactically valid object identifier, and any implementation conforming to ASN.1 and the Basic Encoding Rules must be able to generate and recognize this value.
ipCidrRouteMetric1	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.11 <b>Description:</b> The primary routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1.
ipCidrRouteMetric3	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.13 <b>Description:</b> An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1.
ipCidrRouteMetric5	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.15 <b>Description:</b> An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1.
ipCidrRouteMask	<b>Syntax:</b> IpAddress <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.2 <b>Description:</b> Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipCidrRouteDest field. For those systems that do not support arbitrary subnet masks, an agent

Object	Description
	constructs the value of the ipCidrRouteMask by reference to the IP Address Class. Any assignment (implicit or otherwise) of an instance of this object to a value x must be rejected if the bitwise logical-AND of x with the value of the corresponding instance of the ipCidrRouteDest object is not equal to ipCidrRouteDest.
ipCidrRouteTos	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.3</p> <p><b>Description:</b> The policy specifier is the IP TOS Field. The encoding of IP TOS is as specified by the following convention. Zero indicates the default path if no more specific policy applies.</p>
ipCidrRouteIfIndex	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.5</p> <p><b>Description:</b> The ifIndex value that identifies the local interface through which the next hop of this route should be reached.</p>
ipCidrRouteProto	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.7</p> <p><b>Description:</b> The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols.</p>
ipCidrRouteAge	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.8</p> <p><b>Description:</b> The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of 'too old' can be implied, except through knowledge of the routing protocol by which the route was learned.</p>
ipCidrRouteNextHopAS	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.10</p> <p><b>Description:</b> The Autonomous System Number of the Next Hop. The semantics of this object are determined by the routing- protocol specified in the route's ipCidrRouteProto value. When this object is unknown or not relevant, its value should be set to zero.</p>
ipCidrRouteMetric2	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.12</p> <p><b>Description:</b> An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1.</p>
ipCidrRouteMetric4	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.4.24.4.1.14</p>

## 19.1 Supported MIBs

Object	Description
	<b>Description:</b> An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1.
ipCidrRouteStatus	<b>Syntax:</b> Integer <b>Access:</b> Read-Only <b>OID:</b> 1.3.6.1.2.1.4.24.4.1.16 <b>Description:</b> The row status variable, used according to row installation and removal conventions.

## RFC1213-MIB

Object	Description
icmplnMsgs	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.1 <b>Description:</b> The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmplnErrors.
icmplnDestUnreachs	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.3 <b>Description:</b> The number of ICMP Destination Unreachable messages received.
icmplnParmProbs	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.5 <b>Description:</b> The number of ICMP Parameter Problem messages received.
icmplnRedirects	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.7 <b>Description:</b> The number of ICMP Redirect messages received.
icmplnEchoReps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.9 <b>Description:</b> The number of ICMP Echo Reply messages received.
icmplnTimestampReps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.11 <b>Description:</b> The number of ICMP Timestamp Reply messages received.
icmplnAddrMaskReps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.13 <b>Description:</b> The number of ICMP Address Mask Reply messages received.
icmpOutErrors	<b>Syntax:</b> Counter32

Object	Description
	<p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.15</p> <p><b>Description:</b> The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.</p>
icmpOutTimeExcds	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.17</p> <p><b>Description:</b> The number of ICMP Time Exceeded messages sent.</p>
icmpOutSrcQuenchs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.19</p> <p><b>Description:</b> The number of ICMP Source Quench messages sent.</p>
icmpOutEchos	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.21</p> <p><b>Description:</b> The number of ICMP Echo (request) messages sent.</p>
icmpOutTimestamps	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.23</p> <p><b>Description:</b> The number of ICMP Timestamp (request) messages sent.</p>
icmpOutAddrMaskReps	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.26</p> <p><b>Description:</b> The number of ICMP Address Mask Reply messages sent.</p>
icmpInErrors	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.2</p> <p><b>Description:</b> The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).</p>
icmpInTimeExcds	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.4</p> <p><b>Description:</b> The number of ICMP Time Exceeded messages received.</p>
icmpInSrcQuenchs	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> .1.3.6.1.2.1.5.6</p> <p><b>Description:</b> The number of ICMP Source Quench messages received.</p>
icmpInEchos	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> Read-Only</p>

## 19.1 Supported MIBs

Object	Description
	<b>OID:</b> .1.3.6.1.2.1.5.8 <b>Description:</b> The number of ICMP Echo (request) messages received.
icmpInTimestamps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.10 <b>Description:</b> The number of ICMP Timestamp (request) messages received.
icmpInAddrMasks	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.12 <b>Description:</b> The number of ICMP Address Mask Request messages received.
icmpOutMsgs	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.14 <b>Description:</b> The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
icmpOutDestUnreachs	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.16 <b>Description:</b> The number of ICMP Destination Unreachable messages sent.
icmpOutParmProbs	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.18 <b>Description:</b> The number of ICMP Parameter Problem messages sent.
icmpOutRedirects	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.20 <b>Description:</b> The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchoReps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5 <b>Description:</b> The number of ICMP Echo Reply messages sent.
icmpOutTimestampReps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.24 <b>Description:</b> The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMaskReps	<b>Syntax:</b> Counter32 <b>Access:</b> Read-Only <b>OID:</b> .1.3.6.1.2.1.5.26 <b>Description:</b> The number of ICMP Address Mask Reply messages sent.

**PIM-STD-MIB**

Object	Description
pimInterfaceAddressType	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.157.1.1.1.3</p> <p><b>Description:</b> The address type of this PIM interface.</p>
pimInterfaceAddress	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.157.1.1.1.4</p> <p><b>Description:</b> The primary IP address of this router on this PIM interface. The InetAddressType is given by the pimInterfaceAddressType object.</p>
pimInterfaceStorageType	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.157.1.1.1.28</p> <p><b>Description:</b> The storage type for this row. Rows having the value 'permanent' need not allow write-access to any columnar objects in the row.</p>

**MPLS-LDP-STD-MIB**

Object	Description
mplsLdpLsrId	<p><b>Syntax:</b> IpAddress</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.10.166.4.1.1.1</p> <p><b>Description:</b> A indication of whether this Label Switching Router supports loop detection.</p> <ul style="list-style-type: none"> <li>• none(1) -- Loop Detection is not supported on this LSR.</li> <li>• other(2) -- Loop Detection is supported but by a method other than those listed below.</li> <li>• hopCount(3) -- Loop Detection is supported by Hop Count only.</li> <li>• pathVector(4) -- Loop Detection is supported by Path Vector only.</li> <li>• hopCountAndPathVector(5) -- Loop Detection is supported by both Hop Count And Path Vector.</li> </ul> <p>Since Loop Detection is determined during Session Initialization, an individual session may not be running with loop detection. This object simply gives an indication of whether or not the LSR has the ability to support Loop Detection and which types.</p>

**MPLS-LDP-GENERIC-STD-MIB**

Object	Description
mplsLdpEntityGenericLabelSpace	<p><b>Syntax:</b> Integer</p> <p><b>Access:</b> Read-Only</p> <p><b>OID:</b> 1.3.6.1.2.1.10.166.7.1.1.1.3</p> <p><b>Description:</b> This value of this object is perPlatform(1), then this means that the label space type is per platform. If this object is perInterface(2), then this means that the label space type is per Interface.</p>



## IEC-62439-2-MIB

Object	Description
mrpDomainIndex	<p><b>Syntax:</b> Unsigned32</p> <p><b>Access:</b> not-accessible</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.1</p> <p><b>Description:</b> The index of the entry.</p>
mrpDomainID	<p><b>Syntax:</b> IEC62439UuidType</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.2</p> <p><b>Description:</b> Universally unique identifier belongs to the MRP domain, which represents a ring.</p>
mrpDomainName	<p><b>Syntax:</b> DisplayString</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.3</p> <p><b>Description:</b> A logical name for the MRP domain to ease the management of MRP domains.</p>
mrpDomainAdminRole	<p><b>Syntax:</b> INTEGER</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.4</p> <p><b>Description:</b> Control the MRP behavior of the system per domain. If the value is set to disable(0) the MRP entity of this domain shall be disabled.</p> <p>If the value is set to client(1) the entity shall be set to the role of a Media Redundancy Client (MRC).</p> <p>If the value is set to manager(2) the entity shall be set to the role of a Media Redundancy Manager (MRM).</p> <p>If the value is set to managerAutoComp(3) the entity shall be set to the role of a Media Redundancy Manager Auto (MRA) complying to Annex A.</p> <p>If the value is set to managerAuto(4) the entity shall be set to the role of a Media Redundancy Manager Auto (MRA) not supporting Annex A.</p> <p>The factory settings are recommended to adjust the value of this object to the client(1) capability of the component, or, if supported, to the managerAutoComp(3) or managerAuto(4) capability, in order to prevent multiple managers are in ring (the order of the capabilities are not necessarily conform to the order of the object values here).</p> <p>If the agent restricts the write access, no matter what reason, it shall reject write requests by responding with 'badValue'.</p>
mrpDomainOperRole	<p><b>Syntax:</b> INTEGER</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.5</p> <p><b>Description:</b> The operational role of an MRP entity per domain.</p> <p>A value of disabled(0) signals that the entity doesn't work (whatever reason).</p> <p>A value of client(1) signals that the entity is in a client role.</p> <p>A value of manager(2) signals that the entity is the manager of this MRP domain.</p> <p>A value of managerAutoComp(3) signals that the entity is in automanager role complying to Annex A.</p>

Object	Description
	A value of managerAuto(4) signals that the entity is in automanager role not supporting Annex A.
mrpDomainRingPort1	<b>Syntax:</b> Integer32 <b>Access:</b> read-only <b>OID:</b> 1.0.62439.1.1.1.1.6 <b>Description:</b> The ifIndex of the layer 2 interface which is used as ring port 1.
mrpDomainRingPort1State	<b>Syntax:</b> INTEGER <b>Access:</b> read-only <b>OID:</b> 1.0.62439.1.1.1.1.7 <b>Description:</b> Operational state of the first Ring-Port. <ul style="list-style-type: none"> <li>• disabled(1) indicates that all frames are dropped</li> <li>• blocked(2) indicates that all frames are dropped except               <ul style="list-style-type: none"> <li>• MRP topology change frames and MRP test frames from a MRM,</li> <li>• MRP link change frames from an MRC,</li> <li>• MRP interconnection topology change from a MIM,</li> <li>• MRP interconnection link change from a MIC,</li> <li>• frames from other protocols that also define to pass blocked(2) ports.</li> </ul> </li> <li>• forwarding(3) indicates that all frames are passed through according to the forwarding behavior of IEEE 802.1D</li> <li>• not-connected(4) indicates that the port has no link</li> </ul>
mrpDomainRingPort2	<b>Syntax:</b> Integer32 <b>Access:</b> read-only <b>OID:</b> 1.0.62439.1.1.1.1.8 <b>Description:</b> The ifIndex of the layer 2 interface, which is used as ring port 2.
mrpDomainRingPort2State	<b>Syntax:</b> INTEGER <b>Access:</b> read-only <b>OID:</b> 1.0.62439.1.1.1.1.9 <b>Description:</b> Operational state of the second Ring-Port. <ul style="list-style-type: none"> <li>• disabled(1) indicates that all frames are dropped</li> <li>• blocked(2) indicates that all frames are dropped except               <ul style="list-style-type: none"> <li>• MRP topology change frames and MRP test frames from a MRM,</li> <li>• MRP link change frames from an MRC,</li> <li>• MRP interconnection topology change from a MIM,</li> <li>• MRP interconnection link change from a MIC,</li> <li>• frames from other protocols that also define to pass blocked(2) ports.</li> </ul> </li> <li>• forwarding(3) indicates that all frames are passed through according to the forwarding behavior of IEEE 802.1D</li> <li>• not-connected(4) indicates that the port has no link</li> </ul>
mrpDomainState	<b>Syntax:</b> BITS <b>Access:</b> read-only <b>OID:</b> 1.0.62439.1.1.1.1.10 <b>Description:</b> Operational status of the MRP entity.

## 19.1 Supported MIBs

Object	Description
	<ul style="list-style-type: none"> <li>• disabled(0) – MRP switched off. All higher bits are invalid and shall be reset.</li> <li>• undefined(1) – Value is not valid. All higher bits are invalid and shall be reset.</li> <li>• ringOpen(2) – MRP ring redundancy lost. All higher bits are invalid and shall be reset.</li> <li>• reserved(3) – reserved for further extensions.</li> </ul>
mrpDomainError	<p><b>Syntax:</b> BITS</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.11</p> <p><b>Description:</b> If the device couldn't switch to the desired administrative state (thus the value of 'mrpDomainState' is not the expected one), this value provides the reason. Otherwise the bit noError(0) is set.</p> <ul style="list-style-type: none"> <li>• noError(0) – the operational state of the device is conform to administrative state. All higher bits are invalid and shall be reset.</li> <li>• invalidVlanId(1) – the assigned VLAN ID is not permitted.</li> <li>• invalid (2) – Value is not valid. All higher bits are invalid and shall be reset.</li> <li>• multipleMRM(3) – multiple active managers in ring domain.</li> <li>• singleSideReceive(4) – the test frames of an MRM have been seen, but only on one port.</li> </ul>
mrpDomainBlocked	<p><b>Syntax:</b> INTEGER</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.12</p> <p><b>Description:</b> The entity supports blocked ring ports.</p> <p>Shows whether a mrp domain requires the support of the BLOCKED port state at ring ports. The manager of a mrp domain decides whether this support is required.</p> <p>Set to enabled the manager demands that all clients shall support the blocked attribute also set to enabled.</p> <p>If mrpDomainBlocked is set disabled at the manager, then the value of mrpDomainBlocked can be arbitrary at the clients.</p> <ul style="list-style-type: none"> <li>• enabled(1) client: supports ring ports whose port state can be blocked.</li> <li>• manager: works only with clients supporting blocked ring ports.</li> <li>• disabled(2) client: no support of blocked ring ports.</li> <li>• manager: Work with clients supporting blocked ring ports and with clients not supporting blocked ring ports.</li> </ul>
mrpDomainVlanId	<p><b>Syntax:</b> Unsigned32</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.13</p> <p><b>Description:</b> The VLAN ID assigned to the MRP protocol.</p> <p>The VLAN ID only is in use when the bit invalidVlanId is not set in mrpDomainError.</p> <p>If value is set to 0 no VLAN is assigned.</p> <p>The invalidVlanId shall be set to 0 (no Error).</p>
mrpDomainManagerPriority	<p><b>Syntax:</b> INTEGER</p> <p><b>Access:</b> read-only</p>

Object	Description
	<p><b>OID:</b> 1.0.62439.1.1.1.1.14</p> <p><b>Description:</b> The priority of this MRP entity. If the device is client only, the value of this object shall be ignored by the MRP entity. Only the four most significant bits shall be used, the bits 0 to 11 are reserved. The smaller value has the higher priority.</p>
mrpDomainRingOpenCount	<p><b>Syntax:</b> Counter32</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.15</p> <p><b>Description:</b> Counter for ring-state changes to open.</p>
mrpDomainLastRingOpenChange	<p><b>Syntax:</b> TimeTicks</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.16</p> <p><b>Description:</b> Timeticks since last change of ring-state to ring open.</p>
mrpDomainRoundTripDelayMax	<p><b>Syntax:</b> Unsigned32</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.17</p> <p><b>Description:</b> The max. Round-Trip-Delay (in milliseconds), which was measured since startup.</p>
mrpDomainRoundTripDelayMin	<p><b>Syntax:</b> Unsigned32</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.18</p> <p><b>Description:</b> The min. Round-Trip-Delay (in milliseconds), which was measured since startup.</p>
mrpDomainResetRoundTripDelays	<p><b>Syntax:</b> INTEGER</p> <p><b>Access:</b> not-accessible</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.19</p> <p><b>Description:</b> A write request with resetDelays(1) shall reset the values of mrpDomainRoundTripDelayMax and mrpDomainRoundTripDelayMin to zero at the same time.</p>
mrpDomainMRMReactOnLinkChange	<p><b>Syntax:</b> INTEGER</p> <p><b>Access:</b> read-only</p> <p><b>OID:</b> 1.0.62439.1.1.1.1.20</p> <p><b>Description:</b> Tells whether the MRM reacts on link down MRP link change frames.</p> <ul style="list-style-type: none"> <li>• enabled(1) indicates that the MRM reacts immediately on link down MRP link change frames</li> <li>• disabled(2) indicates that the MRM does not react on link down MRP link change frames</li> </ul>

## 19.2 Standard SNMP Traps

The current MIB files supported by RUGGEDCOM ROX II can be downloaded from the <https://www.siemens.com>.

**Note**

SNMP traps are not configurable in RUGGEDCOM ROX II.

The following table lists all standard traps in RUGGEDCOM ROX II:

Variable	Description
authenticationFailure	<p><b>MIB:</b> SNMPv2-MIB  <b>Standard:</b> RFC 3418  <b>OID:</b> 1.3.6.1.6.3.1.1.5.5</p> <p><b>Definition:</b> An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.</p>
coldStart	<p><b>MIB:</b> SNMPv2-MIB  <b>Standard:</b> RFC 3418  <b>OID:</b> 1.3.6.1.6.3.1.1.5.1</p> <p><b>Definition:</b> A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.</p>
warmStart	<p><b>MIB:</b> SNMPv2-MIB  <b>Standard:</b> RFC 3418  <b>OID:</b> 1.3.6.1.6.3.1.1.5.2</p> <p><b>Definition:</b> A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.</p>
newRoot	<p><b>MIB:</b> BRIDGE-MIB  <b>Standard:</b> RFC 4188  <b>OID:</b> 1.3.6.1.2.1.17.0.1</p> <p><b>Definition:</b> The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree. The trap is sent by a bridge soon after its election as the new root (e.g. upon expiration of the Topology Change Timer) immediately subsequent to its election. Implementation of this trap is optional.</p>
topologyChange	<p><b>MIB:</b> BRIDGE-MIB  <b>Standard:</b> RFC 4188  <b>OID:</b> 1.3.6.1.2.1.17.0.2</p> <p><b>Definition:</b> A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.</p>

Variable	Description
lldpRemTablesChange	<p><b>MIB:</b> LLDP-MIB</p> <p><b>Standard:</b> IEEE Std 802.1AB-2005</p> <p><b>OID:</b> 1.0.8802.1.1.2.0.0.1</p> <p><b>Definition:</b> An lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by a Network Management System (NMS) to trigger LLDP remote systems table maintenance polls. Note that transmission of lldpRemTablesChange notifications are throttled by the agent, as specified by the lldpNotificationInterval object.</p>
linkUp	<p><b>MIB:</b> IF-MIB</p> <p><b>Standard:</b> RFC 1229, 2863, 2233, 1573</p> <p><b>OID:</b> 1.3.6.1.6.3.1.1.5.4</p> <p><b>Definition:</b> A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.</p>
linkDown	<p><b>MIB:</b> IF-MIB</p> <p><b>Standard:</b> RFC 1229, 2863, 2233, 1573</p> <p><b>OID:</b> 1.3.6.1.6.3.1.1.5.3</p> <p><b>Definition:</b> A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.</p>
dsx1LineStatusChange	<p><b>MIB:</b> DS1-MIB</p> <p><b>Standard:</b> RFC 3895</p> <p><b>OID:</b> 1.3.6.1.2.1.10.18.15.0.1</p> <p><b>Definition:</b> A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes. It can be utilized by an Network Management Station (NMS) to trigger polls. When the line status change results from a higher-level line status change (i.e. DS3), then no traps for the DS1 are sent.</p>

## 19.3 Proprietary SNMP Traps

The current MIB files supported by RUGGEDCOM ROX II can be downloaded from the <https://www.siemens.com>.

**Note**

SNMP traps are not configurable in RUGGEDCOM ROX II.

The following table lists all proprietary traps in RUGGEDCOM ROX II:

Variable	Description
ruggedcomMgmt	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4 <b>Definition:</b> The main subtree for new MIB development where specific RUGGEDCOM proprietary MIBs can be placed.
ruggedcomTrapsModule	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1 <b>Definition:</b> The RUGGEDCOM MIB providing traps information.
ruggedcomTrapsModuleObjects	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1 <b>Definition:</b> A group of objects that define the RUGGEDCOM traps module.
trapGenericTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.1 <b>Definition:</b> The main subtree for the RUGGEDCOM generic traps.
genericTrapSeverity	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.1.1 <b>Syntax:</b> Integer <b>Definition:</b> The severity level of the generic trap.
genericTrapDescription	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.1.2 <b>Syntax:</b> String <b>Definition:</b> A description of a generic trap.
trapPowerSupplyTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.2 <b>Definition:</b> The main subtree for the RUGGEDCOM power supply trap.
powerSupplyDescription	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.2.1 <b>Syntax:</b> String <b>Definition:</b> A description of a power supply that fails.
powerSupplyIdentifier	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.2.2 <b>Syntax:</b> Integer <b>Definition:</b> The identified power supply (e.g. power supply 1).

Variable	Description
trapSwUpgradeTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.3 <b>Definition:</b> The main subtree for the RUGGEDCOM software upgrade trap.
trapFanBankTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.5 <b>Definition:</b> The main subtree for the RUGGEDCOM fan bank trap.
fanBankDescription	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.5.1 <b>Syntax:</b> String <b>Definition:</b> A description of a fan bank failure.
fanBankIdentifier	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.5.2 <b>Syntax:</b> Integer <b>Definition:</b> The identified fan bank (e.g. Fan Bank 1).
trapHotswapModuleStateChangeTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.6 <b>Definition:</b> The main subtree for the RUGGEDCOM hotswap module state change trap.
hotswapModuleSlot	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.6.1 <b>Syntax:</b> RcHotswapModuleSlot <b>Definition:</b> The physical slot where the module is located.
hotswapModulePreviousState	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.6.2 <b>Syntax:</b> RcHotswapModuleState <b>Definition:</b> The previous state of the module.
trapModuleTypeMismatchTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.8 <b>Definition:</b> The main subtree for the RUGGEDCOM module type mismatch trap.
trapRTCBatteryLowTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.11 <b>Definition:</b> The main subtree for the RUGGEDCOM RTC battery low trap.
trapSecurityCertificateExpiryTrap	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.12 <b>Definition:</b> The main subtree for the RUGGEDCOM security certificate expiration trap.
trapUserAuthFailure	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.14



Variable	Description
	<b>Syntax:</b> String <b>Definition:</b> The main subtree for the RUGGEDCOM login failure trap.
userAuthFailureMessage	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.14.1 <b>Syntax:</b> String <b>Definition:</b> The login failure message. The message contains the name, reason, IP address, context, and protocol.
trapSuccessUsrChgPwd	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.15 <b>Syntax:</b> String <b>Definition:</b> The main subtree for the RUGGEDCOM successful user changed password trap.
successUsrChgPwd	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.15.1 <b>Syntax:</b> String <b>Definition:</b> The username of the user whose password was successfully changed.
trapRmonThresholdRise	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.16 <b>Definition:</b> The main subtree for the RUGGEDCOM RMON threshold rising alarm trap.
rmonThresholdRiseInterface	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.16.1 <b>Syntax:</b> String <b>Definition:</b> The name of the interface that crossed an RMON threshold value.
rmonThresholdRiseStatistic	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.16.2 <b>Syntax:</b> String <b>Definition:</b> The specific statistic for which an RMON threshold was crossed.
rmonThresholdRiseThroughput	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.16.3 <b>Syntax:</b> String <b>Definition:</b> The current throughput value when this trap is sent.
trapExtDeviceAction	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.17 <b>Syntax:</b> String <b>Definition:</b> The main subtree for the RUGGEDCOM USB status trap.
extDeviceActionMessage	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB

Variable	Description
	<b>OID:</b> 1.3.6.1.4.1.15004.4.1.1.17.1 <b>Syntax:</b> String <b>Definition:</b> The USB status message. The message notifies if a USB is inserted.
ruggedcomTrapsModuleConformance	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5 <b>Definition:</b> A group of objects that define the RUGGEDCOM module conformance trap.
ruggedcomTrapsModuleGroups	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2 <b>Definition:</b> A group of objects that define the RUGGEDCOM traps module.
ruggedcomGenericTrapGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.1 <b>Definition:</b> A group of objects that define the generic trap.
ruggedcomPowerSupplyGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.2 <b>Definition:</b> A group of objects that define the RUGGEDCOM power supply failure trap.
ruggedcomNotificationsGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.3 <b>Definition:</b> The RUGGEDCOM notifications group.
ruggedcomPowerSupplyIdentGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.5 <b>Definition:</b> A group of objects that define RUGGEDCOM power supply identification.
ruggedcomFanBankNotiGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.6 <b>Definition:</b> The RUGGEDCOM notifications group.
ruggedcomHotswapModuleSCNotifGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.7 <b>Definition:</b> The RUGGEDCOM Hotswap Module notifications group.
ruggedcomFanBankGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.8 <b>Definition:</b> A group of objects that define the RUGGEDCOM fan bank failure trap.
ruggedcomModuleStateChangeGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.9 <b>Definition:</b> A group of objects that define the RUGGEDCOM Module State Change trap.
ruggedcomHotswapModuleSCNotifGroup01	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.11

## 19.3 Proprietary SNMP Traps

Variable	Description
	<b>Definition:</b> The RUGGEDCOM Hotswap Module notifications group.
ruggedcomRTCBatteryLowGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.13 <b>Definition:</b> A group of objects for RTC battery low indication.
ruggedcomSecurityGroup02	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.14 <b>Definition:</b> A group of objects to indicate security certificate expiry.
rcPswdChgTrapNotifyGroup	<b>MIB:</b> RUGGEDCOM-TRAPS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.1.5.2.25 <b>Definition:</b> A group of trap objects to notify the password was successfully changed.
rcSysInfo	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.2 <b>Definition:</b> RUGGEDCOM system information MIB.
rcDeviceInfo	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3 <b>Definition:</b> The main subtree for the RUGGEDCOM device info trap.
rcDeviceInfoBootSwVersion	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.2 <b>Definition:</b> The version and the build date of the boot loader software
rcDeviceInfoMainSwVersion	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.3 <b>Definition:</b> The version and the build date of the main operating system software.
rcDeviceInfoPendingBootSwVersion	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.6 <b>Definition:</b> The version and the build date of the boot loader software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length string to any string of non-zero length, the device will generate a swUpgradeTrap notification.
rcDeviceInfoPendingMainSwVersion	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.7 <b>Definition:</b> The version and the build date of the main operating system software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length string to any string of non-zero length, the device will generate a swUpgradeTrap notification.
rcDeviceInfoCfgRevision	<b>MIB:</b> RUGGEDCOM-SYS-INFO-MIB

Variable	Description
	<p><b>OID:</b> 1.3.6.1.4.1.15004.4.2.3.8</p> <p><b>Syntax:</b> Integer</p> <p><b>Definition:</b> The configuration file revision. The revision number will be updated whenever file is saved to the flash memory. This number is recorded in config.csv at the time file is uploaded from the device. Whenever the value of this object changes the device will generate a <code>cfgChangeTrap</code> notification.</p>
<code>ruggedcomTraps</code>	<p><b>MIB:</b> RUGGEDCOM-MIB.mib</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5</p> <p><b>Definition:</b> The root of the subtree where RUGGEDCOM traps can be placed.</p>
<code>genericTrap</code>	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.1</p> <p><b>Definition:</b> A generic trap generated by RUGGEDCOM devices.</p>
<code>powerSupplyTrap</code>	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.2</p> <p><b>Definition:</b> A trap generated when a power supply fails or comes up. The first trap is generated on first power supply failure. The state of the power supply (failed or restored ) is retrieved via object <code>powerSupplyDescription</code> at the time the trap is generated. The status of power supply units in the device can be retrieved via objects <code>rcDeviceStsPowerSupply1</code> and <code>rcDeviceStsPowerSupply2</code>. <code>powerSupplyIdentifier</code> object is recommended to be added as an optional parameter to the list of objects.</p>
<code>swUpgradeTrap</code>	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.3</p> <p><b>Definition:</b> A generic trap generated upon software upgrade. The rate at which this notification is provided is 60 seconds.</p>
<code>cfgChangeTrap</code>	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.4</p> <p><b>Definition:</b> A generic trap generated upon configuration change. The rate at which this notification is provided is 60 seconds.</p>
<code>fanBankTrap</code>	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.6</p> <p><b>Definition:</b> A trap generated when a fan bank fails or fails to comes up. The first trap is generated on first fan bank failure. The state of the fan bank (failed or restored ) is retrieved via object <code>fanBankDescription</code> at the time the trap is generated. The status of power supply units in the device can be retrieved via objects <code>rcDeviceStsFanBank1</code> and <code>rcDeviceStsFanBank2</code>.</p>

## 19.3 Proprietary SNMP Traps

Variable	Description
hotswapModuleStateChangeTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.7</p> <p><b>Definition:</b> A trap generated when a RUGGEDCOM ROX II module changes state. The first traps are generated during initial startup.</p>
moduleTypeMismatchTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.9</p> <p><b>Definition:</b> A trap generated when RUGGEDCOM ROX II sees that, for a given slot, the configured module type does not match the detected module type. The first traps are generated during initial startup.</p>
securityCertificateExpiryTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.16</p> <p><b>Definition:</b> A trap indicating that at least one security certificate on the device is within 30 days of expiration. It is generated by RUGGEDCOM devices.</p>
rcSuccessUsrChgPwdTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.20</p> <p><b>Definition:</b> A trap generated when a user's password is successfully changed.</p>
rcUserLoginFailureTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.46</p> <p><b>Definition:</b> A trap generated when a user login failure occurs.</p>
rcExtDeviceActionTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.47</p> <p><b>Definition:</b> A trap generated when a USB Device is inserted.</p>
rcRmonThresholdRiseTrap	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.48</p> <p><b>Definition:</b> A trap generated when a threshold value has been crossed for an interface.</p>
rcMrpManagerRingClosed	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.50</p> <p><b>Definition:</b> A trap indicating the closed state of the MRP Manager ring. The Manager is identified by its MRP instance ID.</p>
rcMrpManagerRingOpen	<p><b>MIB:</b> RUGGEDCOM-TRAPS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.5.51</p> <p><b>Definition:</b> A trap indicating the open state of the MRP Manager ring. The Manager is identified by its MRP instance ID.</p>
rcTunnels	<p><b>MIB:</b> RUGGEDCOM-TUNNELS-MIB</p> <p><b>OID:</b> 1.3.6.1.4.1.15004.4.16</p>

Variable	Description
	<b>Definition:</b> The RUGGEDCOM MIB providing tunnel status and traps.
rcIpsecTunnelObjects	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1 <b>Definition:</b> The main subtree for all IPsec tunnel objects.
rcIpsecTunnelTable	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1.1 <b>Syntax:</b> SEQUENCE OF RclpsecTunnelEntry <b>Definition:</b> The IPsec Connections Tunnel Table. There is one entry in this table for each IPsec Tunnel.
rcIpsecTunnelEntry	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1.1.1 <b>Syntax:</b> RclpsecTunnelEntry <b>Definition:</b> Each entry contains the attributes associated with an IPsec Tunnel.
rcIpsecConnIndex	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1.1.1.1 <b>Syntax:</b> Integer <b>Definition:</b> The table index number of the IPsec connection.
rcIpsecConnName	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1.1.1.2 <b>Syntax:</b> String <b>Definition:</b> The name of the IPsec connection. The name is unique so it can be used as an index into the connection table.
rcIpsecConnStatus	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1.1.1.3 <b>Syntax:</b> RcTunnelStatus <b>Definition:</b> The status of the IPsec connection. Refer to the TunnelStatus object for definitions of states.
rcIpsecConnNumPeers	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.1.1.1.4 <b>Syntax:</b> Integer <b>Definition:</b> The number of active peers on the IPsec connection.
rcGreTunnelObjects	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.2 <b>Definition:</b> The main subtree for all the various GRE tunnel objects.
rcGreTunnelTable	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.2.1

Variable	Description
	<b>Syntax:</b> SEQUENCE OF RcGreTunnelEntry <b>Definition:</b> The GRE Tunnels Table. There is one entry in this table for each GRE Tunnel.
rcGreTunnelEntry	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.2.1.1 <b>Syntax:</b> RcGreTunnelEntry <b>Definition:</b> Each entry contains the attributes associated with a GRE Tunnel.
rcGreTunnelIndex	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.2.1.1.1 <b>Syntax:</b> Integer <b>Definition:</b> The table index number of the GRE tunnel.
rcGreTunnelName	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.2.1.1.2 <b>Syntax:</b> String <b>Definition:</b> The name of the GRE tunnel.
rcGreTunnelStatus	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.2.1.1.3 <b>Syntax:</b> RcTunnelStatus <b>Definition:</b> The status of the GRE tunnel. Refer to the <i>TunnelStatus</i> object for definitions of states.
rcTunnelTraps	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5 <b>Definition:</b> The main subtree for the RUGGEDCOM tunnel traps.
rcTunnellpsecTraps	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5.1 <b>Definition:</b> The main subtree for the RUGGEDCOM IPsec tunnel traps.
rcIpsecTunnelUpTrap (Notifications)	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5.1.1 <b>Definition:</b> A trap generated when IPsec tunnel connections are established (come up).
rcIpsecTunnelDownTrap (Notifications)	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5.1.2 <b>Definition:</b> A trap generated when IPsec tunnel connections are disconnected (go down).
rcTunnelGreTraps	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5.2 <b>Definition:</b> The main subtree for the RUGGEDCOM GRE tunnel traps.
rcGreTunnelDownTrap (Notifications)	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5.2.2

Variable	Description
	<b>Definition:</b> A trap generated when GRE tunnels are disconnected (go down).
rcGreTunnelUpTrap (Notifications)	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.5.2.1 <b>Definition:</b> A trap generated when GRE tunnels are established (come up).
rcTunnelsConformance	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6 <b>Definition:</b> The main subtree for the RUGGEDCOM tunnels conformance traps.
rcTunnelsIpsecGroups	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.1 <b>Definition:</b> A group of objects that define RUGGEDCOM IPsec tunnels.
rcTunIpsecObjectsGroup	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.1.1 <b>Definition:</b> A group of objects providing information for IPsec tunnels.
rcTunIpsecTrapsGroup	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.1.2 <b>Definition:</b> A group of objects that define RUGGEDCOM Ipsec tunnel traps.
rcTunIpsecNotificationsGroup	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.1.3 <b>Definition:</b> The RUGGEDCOM notifications group for IPsec tunnel traps.
rcTunnelsGreGroups	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.2 <b>Definition:</b> A group of objects that define RUGGEDCOM GRE tunnels.
rcTunGreObjectsGroup	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.2.1 <b>Definition:</b> A group of objects providing information for GRE tunnels.
rcTunGreTrapsGroup	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.2.2 <b>Definition:</b> A group of objects that define RUGGEDCOM GRE tunnel traps.
rcTunGreNotificationsGroup	<b>MIB:</b> RUGGEDCOM-TUNNELS-MIB <b>OID:</b> 1.3.6.1.4.1.15004.4.16.6.2.3 <b>Definition:</b> The RUGGEDCOM notifications group for GRE tunnel traps.



## 19.4 Supported Cipher Suites

### Note

Grade 4 ciphers and above are enabled by default.

### Service: SSH (TCP/22), NETCONF (TCP/830)

Cipher/Algorithm	Grade	Enabled by Default	Configurable
<i>Server Host Key Algorithms</i>			
ssh-ed25519	4	✓	✓
ssh-rsa	3		✓
<i>KEX Algorithms</i>			
diffie-hellman-group18-sha512	4	✓	✓
diffie-hellman-group14-sha1	3		✓
diffie-hellman-group14-sha256	3		✓
<i>MAC Algorithms</i>			
hmac-sha2-256	4	✓	✓
hmac-sha2-512	4	✓	✓
hmac-sha1	1		✓
<i>Encryption Algorithms</i>			
aes128-ctr	4	✓	✓
aes192-ctr	4	✓	✓
aes256-ctr	4	✓	✓

### Service: HTTPS Server (TCP/443)

Cipher Suite/Protocol	Grade	Enabled by Default	Configurable
<i>Protocols</i>			
TLS v1.2	5	✓	✓
TLS v1.0	2		✓
<i>Cipher Suites</i>			
DHE-DSS-AES128-GCM-SHA256	5	✓	✓
DHE-DSS-AES256-GCM-SHA384	5	✓	✓
DHE-RSA-AES128-GCM-SHA256	5	✓	✓
DHE-RSA-AES256-GCM-SHA384	5	✓	✓
DHE-RSA-AES128-SHA256	5	✓	✓
DHE-RSA-AES256-SHA256	5	✓	✓
ECDHE-RSA-AES128-SHA256	5	✓	✓
ECDHE-RSA-AES256-SHA384	5	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	5	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	5	✓	✓

Cipher Suite/Protocol	Grade	Enabled by Default	Configurable
AES128-SHA	2		✓
AES256-SHA	2		✓
DHE-RSA-AES128-SHA	3		✓
DHE-RSA-AES256-SHA	3		✓
<i>Elliptic Curve</i>			
sect571r1	5	✓	✓
sect571k1	5	✓	✓
secp521r1	5	✓	✓
brainpoolP512r1	5	✓	✓
sect409k1	5	✓	✓
sect409r1	5	✓	✓
brainpoolP384r1	5	✓	✓
secp384r1	5	✓	✓
sect283k1	5	✓	✓
sect283r1	5	✓	✓
brainpoolP256r1	5	✓	✓
secp256k1	5	✓	✓
secp256r1	5	✓	✓

## Service: SSH Client

Cipher/Algorithm	Grade	Enabled by Default	Configurable
<i>Server Host Key</i>			
ssh-ed25519	4	✓	✓
ssh-ed25519-cert-v01@openssh.com	4	✓	✓
ecdsa-sha2-nistp256	4	✓	✓
ecdsa-sha2-nistp384	4	✓	✓
ecdsa-sha2-nistp521	4	✓	✓
ecdsa-sha2-nistp256-cert-v01@openssh.com	4	✓	✓
ecdsa-sha2-nistp384-cert-v01@openssh.com	4	✓	✓
ecdsa-sha2-nistp521-cert-v01@openssh.com	4	✓	✓
ssh-rsa	3		✓
ssh-rsa-cert-v01@openssh.com	3		✓
ssh-dss	1		✓
ssh-dss-cert-v01@openssh.com	0		✓
<i>KEX Algorithm</i>			
diffie-hellman-group16-sha512	4	✓	✓
diffie-hellman-group18-sha512	4	✓	✓
ecdh-sha2-nistp256	4	✓	✓
ecdh-sha2-nistp384	4	✓	✓

## 19.4 Supported Cipher Suites

Cipher/Algorithm	Grade	Enabled by Default	Configurable
ecdh-sha2-nistp521	4	✓	✓
curve25519-sha256	4	✓	✓
curve25519-sha256@libssh.org	4	✓	✓
diffie-hellman-group14-sha1	3		✓
diffie-hellman-group14-sha256	3		✓
diffie-hellman-group-exchange-sha1	1		✓
diffie-hellman-group-exchange-sha256	1		✓
diffie-hellman-group1-sha1	0		✓
<i>MAC Algorithm</i>			
hmac-sha1	1		✓
hmac-sha1-96	0		✓
hmac-sha2-256	4	✓	✓
hmac-sha2-512	4	✓	✓
hmac-md5	0		✓
hmac-md5-96	0		✓
umac-64@openssh.com	1		✓
umac-128@openssh.com	4	✓	✓
hmac-sha1-etm@openssh.com	1		✓
hmac-sha1-96-etm@openssh.com	0		✓
hmac-sha2-256-etm@openssh.com	4	✓	✓
hmac-sha2-512-etm@openssh.com	4	✓	✓
hmac-md5-etm@openssh.com	0		✓
hmac-md5-96-etm@openssh.com	0		✓
umac-64-etm@openssh.com	3		✓
umac-128-etm@openssh.com	4	✓	✓
<i>Encryption Algorithm</i>			
aes128-ctr	4	✓	✓
aes192-ctr	4	✓	✓
aes256-ctr	4	✓	✓
aes128-gcm@openssh.com	4	✓	✓
aes256-gcm@openssh.com	4	✓	✓
chacha20-poly1305@openssh.com	4	✓	✓
3des-cbc	1		✓
aes128-cbc	1		✓
aes192-cbc	1		✓
aes256-cbc	1		✓
rijndael-cbc@lysator.liu.se	1		✓

## For more information

Siemens RUGGEDCOM

<https://www.siemens.com/ruggedcom>

Industry Online Support (service and support)

<https://support.industry.siemens.com>

Industry Mall

<https://mall.industry.siemens.com>

Siemens Canada Ltd.

Digital Industries

Process Automation

300 Applewood Crescent

Concord, Ontario, L4K 4E5

Canada

© 2023 Siemens Canada Ltd.

Subject to change