SIEMENS

Edition 11/2023

Configuration Manual

SIMATIC NET

Rugged multi service platforms

RUGGEDCOM ROX II v2.16 CLI

For RX1500, RX1501, RX1510, RX1511, RX1512, RX1524, RX1536

https://www.siemens.com/ruggedcom

SIEMENS

SIMATIC NET

Rugged multi service platforms RUGGEDCOM ROX II v2.16 CLI

Configuration Manual

For RX1500, RX1501, RX1510, RX1511, RX1512, RX1524, RX1536

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

WAN and Wireless 11

Tunneling and VPNs 12

Unicast and Multicast Routing 13

Network Redundancy 14

Network Discovery and Management 15

Traffic Control and Classification 16

Continued on next page

11/2023
C79000-G8976-1538-02

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8976-1538-02
© 11/2023 Subject to change

Copyright © Siemens Canada Ltd. 2023
All rights reserved

SIEMENS

Continued

Time Services 17

Applications 18

Troubleshooting 19

Reference 20

SIMATIC NET

Rugged multi service platforms RUGGEDCOM ROX II v2.16 CLI

Configuration Manual

For RX1500, RX1501, RX1510, RX1511, RX1512, RX1524, RX1536

11/2023
C79000-G8976-1538-02

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8976-1538-02
© 11/2023 Subject to change

Copyright © Siemens Canada Ltd. 2023
All rights reserved

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.

⚠ DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

⚠ NOTICE
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:

⚠ WARNING
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.

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8976-1538-02
© 11/2023 Subject to change

Copyright © Siemens Canada Ltd. 2023
All rights reserved

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8976-1538-02
© 11/2023 Subject to change

Copyright © Siemens Canada Ltd. 2023
All rights reserved

Table of contents

Preface xxxix
Cybersecurity information xxxix
Firmware/software support model xl
CLI command syntax xl
SIMATIC NET glossary xli
System Requirements xli
Accessing documentation xli
License conditions xlii
Registered trademarks xlii
Warranty xlii
Training xlii
Customer support xliii
Contacting Siemens xliii

1 Introduction 1

1.1 Features and Benefits 1
1.2 Feature Keys 7
1.3 Security Recommendations 8
1.4 Available Services by Port 13
1.5 User Permissions 14
1.6 Removable Memory 16
1.7 Logged Events 17
1.7.1 Structure of a Syslog Event 17
1.7.2 Syslog Event Types 18
1.7.3 Logged Security Events 18

2 Using RUGGEDCOM ROX II 25

2.1 Default User Names and Passwords 25
2.2 Logging In 25
2.3 Logging Out 26
2.4 Using Network Utilities 26
2.4.1 Pinging an IPv4 Address or Host 27
2.4.2 Pinging an IPv6 Address or Host 27
2.4.3 Pinging MPLS Endpoints 27
2.4.4 Pinging VRF Endpoints 28
2.4.5 Tracing a Route to an IPv4 Host 28
2.4.6 Tracing a Route to an IPv6 Host 28
2.4.7 Tracing a Route to an MPLS Endpoint 29
2.4.8 Tracing a Route to a VRF Endpoint 29
2.4.9 Capturing Packets from a Network Interface 29
2.4.10 Capturing Packets from a VRF Network Interface 30

2.5 Using the Command Line Interface 31
2.5.1 Accessing Different CLI Modes 31
2.5.2 Using Command Line Completion 32
2.5.3 Displaying Available Commands 32
2.5.4 Editing Commands 33
2.5.5 Using Double Quotes 34
2.5.6 Using Output Redirects 35
2.5.7 Using Regular Expressions 42
2.5.8 Using CLI Utilities 42
2.5.9 Specifying a Range 44
2.5.10 Common Commands 44
2.5.10.1 Basic CLI Commands 44
2.5.10.2 File Commands 46
2.5.10.3 Interface and Services Commands 56
2.5.10.4 Administration Commands 56
2.5.10.5 Configuration Mode General Commands 59
2.6 Configuring the CLI Interface 64
2.7 Accessing Different Modes 65
2.7.1 Accessing BIST Mode 65
2.7.2 Accessing Service Mode 67
2.7.3 Accessing Maintenance Mode 69
2.7.4 Enabling/Disabling SSH Access in Maintenance Mode 70
2.7.5 Managing Maintenance Mode Authorization 71
2.7.5.1 Temporarily Enabling Maintenance Mode Authorization 71
2.7.5.2 Permanently Enabling Maintenance Mode Authorization 72
2.7.5.3 Disabling Maintenance Mode Authorization 73
3 Getting Started 75
3.1 Connecting to RUGGEDCOM ROX II 75
3.1.1 Default IP Address 75
3.1.2 Connecting Directly via Serial Console 75
3.1.3 Connecting Remotely via SSH 76
3.2 Configuring a Basic Network 77
3.2.1 Configuring a Basic IPv4 Network 77
3.2.2 Configuring a Basic IPv6 Network 78
4 Device Management 79
4.1 Displaying Device and Software Information 79
4.2 Viewing Chassis Information and Status 80
4.2.1 Viewing the Slot Hardware 80
4.2.2 Viewing Module Information 81
4.2.3 Viewing Flash Card Storage Utilization 81
4.2.4 Viewing CPU/RAM Utilization 82
4.2.5 Viewing the Slot Status 83
4.2.6 Viewing the Slot Sensor Status 84
4.2.7 Viewing the Power Controller Status 85
4.3 Viewing the Parts List 86

4.4 Shutting Down the Device ... 86
4.5 Rebooting the Device ... 87
4.6 Restoring Factory Defaults ... 87
4.7 Decommissioning the Device ... 87
4.8 Managing Feature Keys ... 88
4.8.1 Viewing the Contents of a Feature Key ... 89
4.8.2 Installing Feature Keys ... 89
4.9 Managing Files ... 90
4.9.1 Installing Files ... 91
4.9.2 Backing Up Files ... 91
4.10 Managing Logs ... 93
4.10.1 Viewing Logs ... 93
4.10.2 Deleting Logs ... 94
4.10.3 Configuring Secure Remote Syslog ... 94
4.10.3.1 Enabling/Disabling Secure Remote Syslog ... 95
4.10.3.2 Viewing a List of Permitted Peers ... 96
4.10.3.3 Adding a Permitted Peer ... 96
4.10.3.4 Deleting a Permitted Peer ... 96
4.10.3.5 Configuring a Source IP Address for Remote Syslog Messages ... 97
4.10.4 Managing Diagnostic Logs ... 97
4.10.4.1 Enabling/Disabling the Developer's Log ... 98
4.10.4.2 Enabling/Disabling the SNMP Log ... 98
4.10.4.3 Enabling/Disabling the NETCONF Summary Log ... 99
4.10.4.4 Enabling/Disabling the NETCONF Trace Log ... 99
4.10.4.5 Enabling/Disabling the XPATH Trace Log ... 100
4.10.4.6 Enabling/Disabling the WebUI Trace Log ... 101
4.10.4.7 Enabling/Disabling the JSON-PRC Log ... 101
4.10.5 Managing Remote Syslog Servers ... 102
4.10.5.1 Viewing a List of Remote Servers ... 102
4.10.5.2 Adding a Remote Server ... 102
4.10.5.3 Deleting a Remote Server ... 103
4.10.6 Managing Remote Server Selectors ... 103
4.10.6.1 Viewing a List of Remote Server Selectors ... 103
4.10.6.2 Adding a Remote Server Selector ... 104
4.10.6.3 Deleting a Remote Server Selector ... 105
4.11 Managing the Software Configuration ... 105
4.11.1 Backing Up the Software Configuration ... 106
4.11.2 Saving the Configuration ... 106
4.11.3 Loading a Configuration ... 107
4.11.4 Managing Automatic Configuration Loading ... 108
4.11.4.1 Enabling/Disabling Automatic Configuration Loading ... 108
4.11.4.2 Automatically Loading a Configuration File from a Removable Drive ... 108
4.11.4.3 Overriding Factory Settings Using a Removable Drive ... 109
4.11.4.4 Deleting an Automatic Configuration File ... 110
4.12 Managing Upgrade Servers ... 110

4.12.1 Understanding Upgrade Servers 110
4.12.2 Configuring the Upgrade Server 111

4.13 Managing Software Versions 112
4.13.1 Understanding Upgrades/Downgrades 112
4.13.2 Upgrading/Downgrading Software 113
4.13.2.1 Determining the Current Software Partition and Version 113
4.13.2.2 Obtaining a Software Release 114
4.13.2.3 Stopping/Declining a Software Upgrade 115
4.13.2.4 Upgrading the Software and Retaining the Configuration 115
4.13.2.5 Upgrading the Software and Resetting the Configuration 118
4.13.2.6 Downgrading Software 121
4.13.2.7 Rolling Back a Software Upgrade 123
4.13.2.8 Monitoring Software Upgrades/Downgrades 123

4.14 Monitoring Firmware Integrity 124
4.14.1 Enabling/Disabling the Boot Time Firmware Integrity 125
4.14.2 Checking the Firmware Integrity 125
4.14.3 Scheduling a Recurring Firmware Integrity Check 125
4.14.4 Viewing the Status of the Firmware Integrity Check 125

4.15 Managing Fixed Modules 126
4.15.1 Viewing a List of Fixed Module Configurations 126

4.16 Managing Line Modules 127
4.16.1 Removing a Line Module 127
4.16.2 Installing a New Line Module 127
4.16.3 Viewing a List of Line Module Configurations 128
4.16.4 Configuring a Line Module 128
4.16.5 Enabling/Disabling Controlled Bypass for M12 Line Modules 129

4.17 Managing SFP Transceivers 130
4.17.1 SFP Transceiver Support 130
4.17.2 Viewing SFP Information 131
4.17.3 Enabling/Disabling Smart SFP Mode 132

4.18 Managing Routable Ethernet Ports 133
4.18.1 Viewing a List of Routable Ethernet Ports 133
4.18.2 Configuring a Routable Ethernet Port 133
4.18.3 Managing VLANs for Routable Ethernet Ports 135
4.18.3.1 Viewing a List of VLANs for Routable Ethernet Ports 135
4.18.3.2 Adding a VLAN to a Routable Ethernet Port 136
4.18.3.3 Deleting a VLAN for a Routable Ethernet Port 136

5 System Administration 139

5.1 Configuring the System Name and Location 139

5.2 Configuring the Host Name 139

5.3 Customizing the Welcome Screen 140

5.4 Setting the Maximum Number of Sessions 140

5.5 Enabling and Configuring WWW Interface Sessions 141

5.6 Enabling/Disabling Remote Access Through a VRF Interface 142
5.7 Managing Alarms 144
5.7.1 Pre-Configured Alarms 144
5.7.2 Viewing a List of Active Alarms 147
5.7.3 Clearing and Acknowledging Alarms 147
5.7.3.1 Clearing Alarms 147
5.7.3.2 Acknowledging Alarms 148
5.7.4 Configuring an Alarm 148
5.7.5 List of Alarms 149
5.8 Managing Users 151
5.8.1 Viewing a List of Users 151
5.8.2 Adding a User 152
5.8.3 Deleting a User 152
5.8.4 Monitoring Users 152
5.8.4.1 Logging Out Users from a Session 153
5.8.4.2 Sending Messages to Users 153
5.9 Managing Passwords and Passphrases 153
5.9.1 Configuring Password/Passphrase Complexity Rules 154
5.9.2 Setting a User Password/Passphrase 155
5.9.3 Setting the Boot Password/Passphrase 156
5.9.4 Setting the Maintenance Password/Passphrase 157
5.9.5 Resetting the Admin Password/Passphrase 157
5.9.6 Resetting the Boot Password/Passphrase 159
5.9.7 Resetting the Maintenance Password/Passphrase 159
5.10 Scheduling Jobs 161
5.10.1 Viewing a List of Scheduled Jobs 161
5.10.2 Adding a Scheduled Job 161
5.10.3 Deleting a Scheduled Job 163
6 Security 165
6.1 Enabling and Configuring CLI Sessions 165
6.2 Enabling/Disabling Brute Force Attack Protection 166
6.3 Enabling/Disabling SYN Cookies 168
6.4 Managing Cipher Suites 168
6.4.1 Viewing Active SSH Server Algorithms 168
6.4.2 Enabling SSH Server and NETCONF Algorithms 169
6.4.3 Enabling TLS Algorithms 170
6.4.4 Configuring the Diffie-Hellman Key Exchange Length 170
6.5 Managing SFTP Sessions 171
6.5.1 Enabling and Configuring SFTP Sessions 171
6.5.2 Adding an SFTP Server's Public Key 172
6.6 Managing Port Security 173
6.6.1 Port Security Concepts 173
6.6.1.1 Static MAC Address-Based Authentication 173
6.6.1.2 Static MAC Address-Based Authentication in an MRP Ring 174

6.6.1.3 IEEE 802.1x Authentication 174
6.6.1.4 IEEE 802.1X Authentication with MAC Address-Based Authentication 175
6.6.1.5 Assigning VLANs with Tunnel Attributes 176
6.6.2 Configuring Port Security 177
6.6.3 Viewing the Security Status of Switched Ethernet Ports 179

6.7 Managing User Authentication 180
6.7.1 Setting the User Authentication Mode 180
6.7.2 Managing User Authentication Keys 181
6.7.2.1 Determining Which Keys are Associated to a User 181
6.7.2.2 Adding a User Authentication Key 182
6.7.2.3 Deleting a User Authentication Key 183
6.7.2.4 Associating/Disassociating a User Authentication Key 183
6.7.3 Managing RADIUS Authentication 184
6.7.3.1 Configuring RADIUS Authentication for LOGIN Services 186
6.7.3.2 Configuring RADIUS Authentication for PPP Services 187
6.7.3.3 Configuring RADIUS Authentication for Switched Ethernet Ports 187
6.7.4 Configuring TACACS+ Authentication 188

6.8 Managing Certificates and Keys 189
6.8.1 Viewing the Local Host SSH/RSA Public Key 190
6.8.2 Configuring Session Security 190
6.8.3 Managing the Trusted Certificate Store 191
6.8.3.1 Configuring the Trusted Certificate Store 191
6.8.3.2 Enabling/Disabling the Trusted Certificate Store 192
6.8.3.3 List of Root Certificates in the Trusted Certificate Store 192
6.8.4 Managing CA Certificates for the Trusted Certificate Store 215
6.8.4.1 Viewing a List of CA Certificates Added to the Trusted Certificate Store 215
6.8.4.2 Adding a CA Certificate to the Trusted Certificate Store 215
6.8.4.3 Deleting a CA Certificate from the Trusted Certificate Store 216
6.8.5 Managing CA Certificates and CRLs 216
6.8.5.1 Viewing a List of CA Certificates and CRLs 216
6.8.5.2 Viewing the Status of a CA Certificate and CRL 216
6.8.5.3 Adding a CA Certificate and CRL 218
6.8.5.4 Deleting a CA Certificate and CRL 219
6.8.6 Managing Private Keys 219
6.8.6.1 Viewing a List of Private Keys 220
6.8.6.2 Adding a Private Key 220
6.8.6.3 Deleting a Private Key 221
6.8.7 Managing Public Keys 221
6.8.7.1 Viewing a List of Public Keys 221
6.8.7.2 Adding a Public Key 222
6.8.7.3 Adding an IPSec-Formatted Public Key 223
6.8.7.4 Deleting a Public Key 223
6.8.8 Managing Certificates 224
6.8.8.1 Viewing a List of Certificates 224
6.8.8.2 Viewing the Status of a Certificate 224
6.8.8.3 Adding a Certificate 225
6.8.8.4 Deleting a Certificate 226
6.8.9 Managing Known Hosts 226

6.8.9.1 Viewing a List of Known Hosts 227
6.8.9.2 Adding a Known Host 227
6.8.9.3 Deleting a Known Host 228
6.8.10 Managing SCEP 228
6.8.10.1 Understanding SCEP 228
6.8.10.2 Configuring SCEP 229
6.8.10.3 Configuring the SCEP Client 230
6.8.10.4 Configuring the SCEP Certificate Signing Requests 231
6.8.10.5 Retrieving an SCEP CA Certificate 233
6.8.10.6 Retrieving an SCEP Certificate 233
6.8.10.7 Configuring Automatic Certificate Renewal 234
6.8.10.8 Renewing an Expired SCEP Certificate 234
6.8.10.9 Renewing an SCEP CA Certificate 234
6.9 Managing Firewalls 235
6.9.1 Firewall Concepts 235
6.9.1.1 Stateless vs. Stateful Firewalls 235
6.9.1.2 Linux netfilter 236
6.9.1.3 Network Address Translation 236
6.9.1.4 Port Forwarding 237
6.9.1.5 Protecting Against a SYN Flood Attack 237
6.9.1.6 Protecting Against IP Spoofing 238
6.9.1.7 Active and Working Firewall Configurations 238
6.9.2 Viewing a List of Firewalls 238
6.9.3 Adding a Firewall 239
6.9.4 Deleting a Firewall 240
6.9.5 Working with Multiple Firewall Configurations 240
6.9.6 Configuring the Firewall for a VPN 241
6.9.7 Configuring the Firewall for a VPN in a DMZ 242
6.9.8 Configuring Netfilter 243
6.9.9 Managing Zones 243
6.9.9.1 Viewing a List of Zones 243
6.9.9.2 Adding a Zone 244
6.9.9.3 Deleting a Zone 245
6.9.10 Managing Interfaces 245
6.9.10.1 Viewing a List of Interfaces 245
6.9.10.2 Adding an Interface 246
6.9.10.3 Associating an Interface with a Zone 247
6.9.10.4 Configuring a Broadcast Address 247
6.9.10.5 Deleting an Interface 248
6.9.11 Managing Hosts 248
6.9.11.1 Viewing a List of Hosts 249
6.9.11.2 Adding a Host 249
6.9.11.3 Deleting a Host 250
6.9.12 Managing Policies 250
6.9.12.1 Viewing a List of Policies 251
6.9.12.2 Adding a Policy 252
6.9.12.3 Configuring the Source Zone 252
6.9.12.4 Configuring the Destination Zone 253
6.9.12.5 Deleting a Policy 253

6.9.13 Managing Network Address Translation Settings 254
6.9.13.1 Viewing a List of NAT Settings 254
6.9.13.2 Adding a NAT Setting 254
6.9.13.3 Deleting a NAT Setting 255
6.9.14 Managing Masquerade and SNAT Settings 256
6.9.14.1 Viewing a List of Masquerade and SNAT Settings 256
6.9.14.2 Adding Masquerade or SNAT Settings 257
6.9.14.3 Deleting a Masquerade or SNAT Setting 258
6.9.15 Managing Rules 258
6.9.15.1 Viewing a List of Rules 258
6.9.15.2 Adding a Rule 259
6.9.15.3 Configuring the Source Zone 261
6.9.15.4 Configuring the Destination Zone 262
6.9.15.5 Deleting a Rule 262
6.9.16 Validating a Firewall Configuration 263
6.9.17 Enabling/Disabling a Firewall 263

6.10 Restricting Management Access to Specific Interfaces 263

7 IP Address Assignment 267

7.1 Managing IP Addresses for Routable Interfaces 267
7.1.1 Configuring Costing for Routable Interfaces 267
7.1.2 Viewing Statistics for Routable Interfaces 267
7.1.3 Managing IPv4 Addresses 269
7.1.3.1 Viewing a List of IPv4 Addresses 269
7.1.3.2 Adding an IPv4 Address 269
7.1.3.3 Deleting an IPv4 Address 270
7.1.4 Managing IPv6 Addresses 270
7.1.4.1 Viewing a List of IPv6 Addresses 270
7.1.4.2 Adding an IPv6 Address 270
7.1.4.3 Deleting an IPv6 Address 271
7.1.5 Configuring IPv6 Neighbor Discovery 271
7.1.6 Managing IPv6 Network Prefixes 273
7.1.6.1 Adding an IPv6 Network Prefix 273
7.1.6.2 Deleting an IPv6 Network Prefix 274

7.2 Managing the DHCP Relay Agent 275
7.2.1 Configuring the DHCP Relay Agent 275
7.2.2 Assigning a DHCP Server Address 276
7.2.3 Viewing a List of DHCP Client Ports 276
7.2.4 Adding a DHCP Client Port 276
7.2.5 Deleting a DHCP Client Port 277
7.2.6 Example: Configuring the Device as a Relay Agent 277

7.3 Managing the DHCP Server 279
7.3.1 Viewing a List of Active Leases 279
7.3.2 Configuring the DHCP Server 280
7.3.3 Enabling/Disabling the DHCP Server 281
7.3.4 Configuring DHCP Server Options 281
7.3.5 Managing DHCP Client Configuration Options 282
7.3.5.1 Configuring Standard DHCP Client Configuration Options (IPv4) 282

7.3.5.2 Configuring Standard DHCP Client Configuration Options (IPv6) 284
7.3.5.3 Viewing a List of Custom DHCP Client Configuration Options 285
7.3.5.4 Adding a Custom DHCP Client Configuration Option 286
7.3.5.5 Deleting a Custom DHCP Client Configuration Option 287
7.3.6 Managing DHCP Listen Interfaces 287
7.3.6.1 Viewing a List of DHCP Listen Interfaces 288
7.3.6.2 Adding a DHCP Listen Interface 288
7.3.6.3 Deleting a DHCP Listen Interface 288
7.3.7 Managing Shared Networks 289
7.3.7.1 Viewing a List of Shared Networks 289
7.3.7.2 Adding a Shared Network 290
7.3.7.3 Configuring Shared Network Options 290
7.3.7.4 Deleting a Shared Network 292
7.3.8 Managing Subnets 292
7.3.8.1 Viewing a List of Subnets 292
7.3.8.2 Adding a Subnet 293
7.3.8.3 Configuring Subnet Options 293
7.3.8.4 Deleting a Subnet 296
7.3.9 Managing Host Groups 296
7.3.9.1 Viewing a List of Host Groups 296
7.3.9.2 Adding a Host Group 297
7.3.9.3 Configuring Host Group Options 297
7.3.9.4 Deleting a Host Group 299
7.3.10 Managing DHCP Hosts 299
7.3.10.1 Viewing a List of Hosts 299
7.3.10.2 Adding a Host 300
7.3.10.3 Configuring Host Options 300
7.3.10.4 Deleting Hosts 302
7.3.11 Managing Address Pools (IPv4) 303
7.3.11.1 Viewing a List of Address Pools (IPv4) 303
7.3.11.2 Adding an Address Pool (IPv4) 304
7.3.11.3 Deleting an Address Pool (IPv4) 304
7.3.12 Managing Address Pools (IPv6) 305
7.3.12.1 Viewing a List of Address Pools (IPv6) 305
7.3.12.2 Adding an Address Pool (IPv6) 306
7.3.12.3 Deleting an Address Pool (IPv6) 307
7.3.13 Managing IP Ranges (IPv4) 307
7.3.13.1 Viewing a List of IP Ranges (IPv4) 307
7.3.13.2 Adding an IP Range (IPv4) 308
7.3.13.3 Deleting an IP Range (IPv4) 309
7.3.14 Managing IP Ranges (IPv6) 309
7.3.14.1 Viewing a List of IP Ranges (IPv6) 309
7.3.14.2 Adding an IP Range (IPv6) 310
7.3.14.3 Deleting an IP Range (IPv6) 311
7.3.15 Managing IPv6 Prefixes 311
7.3.15.1 Viewing a List of IPv6 Prefixes 311
7.3.15.2 Adding an IPv6 Prefix 312
7.3.15.3 Deleting an IPv6 Prefix 313
7.3.16 Managing Temporary Subnets 313

7.3.16.1 Viewing a List of Temporary Subnets 314
7.3.16.2 Adding a Temporary Subnet 314
7.3.16.3 Deleting a Temporary Subnet 315
7.3.17 Managing IPv6 Subnets 315
7.3.17.1 Viewing a List of IPv6 Subnets 315
7.3.17.2 Adding a IPv6 Subnet 316
7.3.17.3 Deleting an IPv6 Subnet 317
7.3.18 Managing Option 82 Classes for Address Pools 317
7.3.18.1 Viewing a List of Option 82 Classes for Address Pools 318
7.3.18.2 Adding an Option 82 Class to an Address Pool 319
7.3.18.3 Deleting an Option 82 Class From an Address Pool 319
7.3.19 Example: Configuring the Device as a DHCP Server to Support a Relay Agent 320

7.4 Managing Static DNS 324
7.4.1 Managing Domain Names 324
7.4.1.1 Viewing a List of Domain Names 324
7.4.1.2 Adding a Domain Name 325
7.4.1.3 Deleting a Domain Name 325
7.4.2 Managing Domain Name Servers 325
7.4.2.1 Viewing a List of Domain Name Servers 325
7.4.2.2 Adding a Domain Name Server 326
7.4.2.3 Deleting a Domain Name Server 326

7.5 Managing Dynamic DNS 326
7.5.1 Enabling and Configuring Dynamic DNS 327
7.5.2 Managing Dynamic DNS Servers 327
7.5.2.1 Viewing a List of Dynamic DNS Servers 328
7.5.2.2 Viewing the Status of a Dynamic DNS Server 328
7.5.2.3 Adding a Dynamic DNS Server 329
7.5.2.4 Deleting a Dynamic DNS Server 329
7.5.3 Managing Dynamic DNS Server Host Names 329
7.5.3.1 Viewing a List of Host Names 330
7.5.3.2 Adding a Host Name 330
7.5.3.3 Deleting a Host Name 330

8 Layer 2 333

8.1 Configuring Link Detection 333

8.2 Managing Switched Ethernet Ports 334
8.2.1 Viewing a List of Switched Ethernet Ports 334
8.2.2 Configuring a Switched Ethernet Port 335
8.2.3 Configuring RMON Threshold Alerts 340
8.2.4 Viewing Switched Ethernet Port Statistics 342
8.2.5 Viewing the Status of a Switched Ethernet Port 342
8.2.6 Viewing RMON Port Statistics 344
8.2.7 Clearing Switched Ethernet Port Statistics 347
8.2.8 Resetting a Switched Ethernet Port 347
8.2.9 Testing Switched Ethernet Port Cables 348
8.2.9.1 Running a Cable Diagnostic Test 348
8.2.9.2 Viewing Cable Diagnostic Statistics 349
8.2.9.3 Clearing Cable Diagnostic Statistics 350

8.3 Managing Ethernet Trunk Interfaces 350
8.3.1 Viewing a List of Ethernet Trunk Interfaces 351
8.3.2 Adding an Ethernet Trunk Interface 351
8.3.3 Deleting an Ethernet Trunk Interface 354
8.3.4 Managing Ethernet Trunk Ports 354
8.3.4.1 Viewing a List of Ethernet Trunk Ports 354
8.3.4.2 Adding an Ethernet Trunk Port 355
8.3.4.3 Deleting an Ethernet Trunk Port 355
8.4 Managing MAC Addresses 355
8.4.1 Viewing a Dynamic List of MAC Addresses 356
8.4.2 Purging the Dynamic MAC Address List 357
8.4.3 Configuring MAC Address Learning Options 357
8.4.4 Managing Static MAC Addresses 357
8.4.4.1 Viewing a List of Static MAC Addresses 358
8.4.4.2 Adding a Static MAC Address 358
8.4.4.3 Deleting a Static MAC Address 359
8.5 Managing Multicast Filtering 359
8.5.1 Multicast Filtering Concepts 359
8.5.1.1 IGMP 360
8.5.1.2 GMRP (GARP Multicast Registration Protocol) 364
8.5.2 Enabling and Configuring GMRP 367
8.5.3 Managing IGMP Snooping 367
8.5.3.1 Configuring IGMP Snooping 368
8.5.3.2 Viewing a List of Router Ports 369
8.5.3.3 Adding a Router Port 369
8.5.3.4 Deleting a Router Port 369
8.5.4 Managing the Static Multicast Group Table 370
8.5.4.1 Viewing a List of Static Multicast Group Entries 370
8.5.4.2 Adding a Static Multicast Group Entry 370
8.5.4.3 Deleting a Static Multicast Group Entry 371
8.5.5 Managing Egress Ports for Multicast Groups 371
8.5.5.1 Viewing a List of Egress Ports 371
8.5.5.2 Adding an Egress Port 372
8.5.5.3 Deleting an Egress Port 372
8.5.6 Viewing a Summary of Multicast Groups 373
8.5.7 Viewing a List of IP Multicast Groups 374
8.6 Managing VLANs 374
8.6.1 VLAN Concepts 375
8.6.1.1 Tagged vs. Untagged Frames 375
8.6.1.2 Native VLAN 375
8.6.1.3 Edge and Trunk Port Types 375
8.6.1.4 Ingress Filtering 376
8.6.1.5 Forbidden Ports List 376
8.6.1.6 VLAN-Aware Mode of Operation 377
8.6.1.7 GARP VLAN Registration Protocol (GVRP) 377
8.6.1.8 PVLAN Edge 379
8.6.1.9 Restricted VLANs 379
8.6.1.10 VLAN Advantages 380

8.6.2 Configuring the Internal VLAN Range 382
8.6.3 Enabling/Disabling Ingress Filtering 383
8.6.4 Managing VLANs for Switched Ethernet Ports 384
8.6.4.1 Viewing VLAN Assignments for Switched Ethernet Ports 384
8.6.4.2 Configuring VLANs for Switched Ethernet Ports 385
8.6.5 Managing Static VLANs 385
8.6.5.1 Viewing a List of Static VLANs 386
8.6.5.2 Adding a Static VLAN 386
8.6.5.3 Deleting a Static VLAN 387
8.6.6 Managing Forbidden Ports 387
8.6.6.1 Viewing a List of Forbidden Ports 387
8.6.6.2 Adding a Forbidden Port 387
8.6.6.3 Deleting a Forbidden Port 388
8.6.7 Managing VLANs for Interfaces and Tunnels 388

9 Layer 3 389

9.1 Layer 3 Switching Concepts 389
9.1.1 Layer 3 Switch Forwarding Table 389
9.1.2 Static Layer 3 Switching Rules 390
9.1.3 Dynamic Learning of Layer 3 Switching Rules 390
9.1.4 Layer 3 Switch ARP Table 391
9.1.5 Multicast Cross-VLAN Layer 2 Switching 391
9.1.6 Size of the Layer 3 Switch Forwarding Table 392
9.1.7 Interaction with the Firewall 392
9.1.8 Layer 3 Switching Summary 392
9.2 Configuring Layer 3 Switching 393
9.3 Enabling/Disabling IPSec Hardware Acceleration 395
9.4 Managing Static ARP Table Entries 395
9.4.1 Viewing a List of ARP Table Entries 396
9.4.2 Adding a Static ARP Table Entry 396
9.4.3 Deleting a Static ARP Table Entry 396
9.5 Viewing a Static and Dynamic ARP Table Summary 397
9.6 Viewing Routing Rules 397
9.7 Flushing Dynamic Hardware Routing Rules 400

10 Serial Server 401

10.1 Managing Serial Ports 401
10.1.1 Viewing a List of Serial Ports 401
10.1.2 Viewing Serial Port Statistics 401
10.1.3 Viewing Transport Connection Statistics 403
10.1.4 Viewing DNP Device Table Statistics 404
10.1.5 Clearing Serial Port Statistics 404
10.1.6 Configuring a Serial Port 405
10.1.7 Restarting the Serial Server 406
10.1.8 Resetting a Serial Port 406
10.2 Managing Serial Port Protocols 406

10.2.1 Serial Port Protocol Concepts 406
10.2.1.1 Raw Socket Applications 406
10.2.1.2 Modbus TCP Applications 408
10.2.1.3 DNP Applications 409
10.2.1.4 MicroLok Applications 410
10.2.1.5 Incoming/Outgoing Serial Connections 412
10.2.2 Viewing a List of Serial Port Protocols 412
10.2.3 Adding a Serial Port Protocol 412
10.2.4 Configuring the DNP Protocol 413
10.2.5 Configuring the Modbus TCP Protocol 414
10.2.6 Configuring the Raw Socket Protocol 415
10.2.7 Configuring the MicroLok Protocol 416
10.2.8 Deleting a Serial Port Protocol 417

10.3 Managing DNP Device Address Tables 417
10.3.1 Viewing a List of DNP Device Address Tables 417
10.3.2 Adding a DNP Device Address Table 418
10.3.3 Deleting a Device Address Table 419

10.4 Managing MicroLok Device Address Tables 419
10.4.1 Viewing a List of MicroLok Device Address Tables 419
10.4.2 Adding a MicroLok Device Address Table 420
10.4.3 Deleting a MicroLok Device Address Table 420

10.5 Managing Serial Multicast Streaming 421
10.5.1 Understanding Serial Multicast Streaming 421
10.5.1.1 Sink vs. Source Ports 421
10.5.1.2 Multicast Streaming Examples 422
10.5.2 Configuring Serial Multicast Streaming 422
10.5.3 Example: Serial Interfaces Configured as a Sink for Multicast Streams 423
10.5.4 Example: Serial Interfaces Configured as a Source for Multicast Streams 425
10.5.5 Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams .. 428

10.6 Managing Remote Hosts 431
10.6.1 Viewing a List of Remote Hosts 431
10.6.2 Adding a Remote Host 432
10.6.3 Deleting a Remote Host 433

10.7 Managing Local Hosts 433
10.7.1 Viewing a List of Local Hosts 433
10.7.2 Adding a Local Host 434
10.7.3 Deleting a Local Host 434

10.8 Managing Remote Host Interfaces 435
10.8.1 Viewing a List of Remote Host Interfaces 435
10.8.2 Adding a Remote Host Interface 436
10.8.3 Deleting a Remote Host Interface 436

10.9 Managing Local Host Interfaces 437
10.9.1 Viewing a List of Local Host Interfaces 437
10.9.2 Adding a Local Host Interface 437
10.9.3 Deleting a Local Host Interface 438

11 WAN and Wireless 439

11.1 Connecting as a PPP Client 439

11.2 Managing WAN Interfaces 440
11.2.1 Viewing a List of WAN Interfaces 440
11.2.2 Configuring a WAN Interface 440
11.2.3 Viewing WAN Statistics 441
11.2.4 Clearing WAN Statistics 442
11.2.5 Performing a Loopback Test 443
11.2.6 Configuring a T1 Line 444
11.2.7 Configuring an E1 Line 444
11.2.8 Configuring DDS 445
11.2.9 Managing Channels 446
11.2.9.1 Viewing a List of Channels 446
11.2.9.2 Adding a Channel 446
11.2.9.3 Deleting a Channel 447
11.2.10 Configuring an HDLC-ETH Connection 448
11.2.11 Configuring a Multi Link PPP Connection 449
11.2.12 Configuring a PPP Connection 449
11.2.13 Configuring a Frame Relay Connection 450
11.2.14 Managing Data Links for Frame Relay Connections 451
11.2.14.1 Viewing a List of Data Links 452
11.2.14.2 Adding a Data Link 452
11.2.14.3 Deleting a Data Link 453
11.2.15 Managing VLANs for HDLC-ETH Connections 453
11.2.15.1 Viewing a List of HDLC-ETH VLANs 453
11.2.15.2 Adding an HDLC-ETH VLAN 454
11.2.15.3 Deleting an HDLC-ETH VLAN 455

11.3 Managing Cellular Modem Interfaces 455
11.3.1 Enabling/Disabling Cellular Modem Interfaces 455
11.3.2 Configuring a Cellular Modem Interface 456
11.3.3 Activating Dual SIM Cards 457
11.3.4 Viewing a List of Cellular Modem Interfaces 457
11.3.5 Viewing the Status of a Cellular Modem Interface 457
11.3.6 Viewing PPP Interface Statistics 458
11.3.7 Viewing the HSPA Network Status for Cellular Modems 459
11.3.8 Viewing the CDMA Network Status for Cellular Modems 460
11.3.9 Activating a Cellular Modem Account 462
11.3.9.1 Activating a Cellular Modem Account Over-the-Air 462
11.3.9.2 Activating a Cellular Modem Account Manually 463

11.4 Running AT Commands 463

11.5 Managing Cellular Modem Profiles 464
11.5.1 Managing CDMA Profiles 464
11.5.1.1 Viewing a List of CDMA Profiles 464
11.5.1.2 Adding a CDMA Profile 464
11.5.1.3 Deleting a CDMA Profile 466
11.5.2 Managing GSM Profiles 466
11.5.2.1 Viewing a List of GSM Profiles 466

11.5.2.2 Adding a GSM Profile 466
11.5.2.3 Deleting a GSM Profile 468

11.6 Managing the LTE Modem 469
11.6.1 Viewing LTE Cellular Modem Information 469
11.6.2 Configuring an LTE Modem 470
11.6.3 Enabling/Disabling the LTE Modem 472
11.6.4 Resetting the Cellular Modem 473
11.6.4.1 Performing a Manual Soft Reset 473
11.6.4.2 Enabling/Disabling a Hard Reset 474
11.6.5 Enabling/Disabling GPS 474
11.6.6 Viewing the Configured GPS Mode 475
11.6.7 Enabling and Configuring GPS NMEA Data Streams 475
11.6.8 Managing Firmware Updates 476
11.6.8.1 Viewing the Firmware Update Status 477
11.6.8.2 Configuring the Firmware Update Mode and Source 477
11.6.8.3 Launching a Firmware Update 479

11.7 Managing PPPoE 480
11.7.1 Understanding PPPoE 480
11.7.2 Managing PPPoE Profiles 481
11.7.2.1 Viewing a List of PPPoE Profiles 482
11.7.2.2 Adding PPPoE Profile 482
11.7.2.3 Deleting a PPPoE Profile 483
11.7.3 Managing PPPoE Interfaces 483
11.7.3.1 Configuring a PPPoE Interface 484
11.7.3.2 Viewing PPPoE Statistics 484
11.7.4 Example: Configuring a PPPoE Connection with an ISP 485

12 Tunneling and VPNs 487

12.1 Managing Virtual Switches 487
12.1.1 Viewing a List of Virtual Switches 488
12.1.2 Adding a Virtual Switch 489
12.1.3 Deleting a Virtual Switch 490
12.1.4 Managing Virtual Switch Interfaces 490
12.1.4.1 Viewing a List of Virtual Switch Interfaces 490
12.1.4.2 Adding a Virtual Switch Interface 491
12.1.4.3 Deleting a Virtual Switch Interface 491
12.1.5 Filtering Virtual Switch Traffic 492
12.1.5.1 Enabling/Disabling Virtual Switch Filtering 492
12.1.5.2 Viewing a List of Virtual Switch Filters 493
12.1.5.3 Adding a Virtual Switch Filter 493
12.1.5.4 Deleting a Virtual Switch Filter 494
12.1.6 Managing Filtering Rules 494
12.1.6.1 Viewing a List of Rules 494
12.1.6.2 Viewing a List of Rules Assigned to a Virtual Switch Filter 494
12.1.6.3 Adding a Rule 495
12.1.6.4 Adding a Rule to a Virtual Switch Filter 496
12.1.6.5 Deleting a Rule 496
12.1.6.6 Deleting a Rule from a Virtual Switch Filter 496

12.1.7 Managing In/Out Interfaces 497
12.1.7.1 Viewing a List of In/Out Interfaces 497
12.1.7.2 Adding an In/Out Interface 498
12.1.7.3 Deleting an In/Out Interface 498
12.1.8 Managing VLANs for Virtual Switches 498
12.1.8.1 Viewing a List of Virtual Switch VLANs 498
12.1.8.2 Adding a Virtual Switch VLAN 499
12.1.8.3 Deleting a Virtual Switch VLAN 500

12.2 Managing the Layer2 Tunnel Daemon 500
12.2.1 Viewing Round Trip Time Statistics 500
12.2.2 Configuring the Layer 2 Tunnel Daemon 501

12.3 Managing L2TP Tunnels 502
12.3.1 Configuring L2TP Tunnels 502
12.3.2 Configuring DNS Servers 503
12.3.3 Configuring PPP Options 503
12.3.4 Configuring WINS Servers 504

12.4 Managing L2TPv3 Tunnels 505
12.4.1 L2TPv3 Tunnel Scenarios 505
12.4.2 Creating an L2TPv3 Tunnel 507
12.4.3 Managing Static L2TPv3 Tunnels 507
12.4.3.1 Enabling/Disabling Static L2TPv3 Tunnels 507
12.4.3.2 Viewing a List of Static L2TPv3 Tunnels 508
12.4.3.3 Adding a Static L2TPv3 Tunnel 508
12.4.3.4 Deleting a Static L2TPv3 Tunnel 510
12.4.4 Managing Dynamic L2TPv3 Tunnels 510
12.4.4.1 Enabling and Configuring Dynamic L2TPv3 Tunnels 510
12.4.4.2 Viewing a List of Dynamic L2TPv3 Tunnels 511
12.4.4.3 Adding a Dynamic L2TPv3 Tunnel 511
12.4.4.4 Deleting a Dynamic L2TPv3 Tunnel 513
12.4.5 Managing Sessions for L2TPv3 Tunnels 514
12.4.5.1 Viewing a List of Sessions 514
12.4.5.2 Adding a Session for a Static L2TPv3 Tunnel 514
12.4.5.3 Adding a Session for a Dynamic L2TPv3 Tunnel 515
12.4.5.4 Configuring Local and Remote Cookies 516
12.4.5.5 Deleting a Session 517
12.4.6 Managing VLANs for L2TPv3 Tunnels 518
12.4.6.1 Viewing a List of VLANs 518
12.4.6.2 Adding a VLAN 518
12.4.6.3 Deleting a VLAN 519
12.4.7 Example: Establishing an L2TPv3 Tunnel Between Routers 519

12.5 Managing GOOSE Tunnels 521
12.5.1 Viewing the GOOSE Tunnel Statistics 523
12.5.2 Viewing a List of GOOSE Tunnels 523
12.5.3 Adding a GOOSE Tunnel 524
12.5.4 Deleting a GOOSE Tunnel 524
12.5.5 Managing Remote Daemons for GOOSE Tunnels 525
12.5.5.1 Viewing a List of Remote Daemons 525

12.5.5.2 Adding a Remote Daemon 525
12.5.5.3 Deleting a Remote Daemon 526
12.5.6 Example: Establishing a GOOSE Tunnel Between Routers 526

12.6 Managing Generic Tunnels 527
12.6.1 Viewing the Generic Tunnel Statistics 528
12.6.2 Viewing a List of Generic Tunnels 529
12.6.3 Adding a Generic Tunnel 529
12.6.4 Deleting a Generic Tunnel 530
12.6.5 Managing Remote Daemon IP Addresses for Generic Tunnels 530
12.6.5.1 Viewing a List of IP Addresses 530
12.6.5.2 Adding an IP Address 531
12.6.5.3 Deleting an IP Address 531
12.6.6 Managing Remote Daemon Egress Interfaces for Generic Tunnels 531
12.6.6.1 Viewing a List of Egress Interfaces 532
12.6.6.2 Adding an Egress Interface 532
12.6.6.3 Deleting an Egress Interface 532
12.6.7 Managing Ethernet Types for Generic Tunnels 533
12.6.7.1 Viewing a List of Ethernet Types 533
12.6.7.2 Adding an Ethernet Type 533
12.6.7.3 Deleting an Ethernet Type 534

12.7 Managing Generic Routing Encapsulation Tunnels 534
12.7.1 Viewing Statistics for GRE Tunnels 535
12.7.2 Viewing a List of GRE Tunnels 536
12.7.3 Adding a GRE Tunnel 536
12.7.4 Configuring a DSCP Marking for GRE Tunnel Traffic 538
12.7.5 Enabling/Disabling Keepalive Messages 538
12.7.6 Deleting a GRE Tunnel 540
12.7.7 Example: Configuring a GRE Tunnel with IPsec 540

12.8 Managing IPsec Tunnels 546
12.8.1 IPsec Tunneling Concepts 547
12.8.1.1 IPsec Modes 547
12.8.1.2 Supported Encryption Protocols 547
12.8.1.3 Public and Secret Key Cryptography 548
12.8.1.4 X509 Certificates 548
12.8.1.5 NAT Traversal 548
12.8.1.6 Remote IPsec Client Support 549
12.8.1.7 IPsec and Router Interfaces 549
12.8.2 Configuring IPsec Tunnels 549
12.8.3 Configuring Certificates and Keys 550
12.8.4 Viewing the IPsec Tunnel Status 551
12.8.5 Managing Pre-Shared Keys 552
12.8.5.1 Viewing a List of Pre-Shared Keys 553
12.8.5.2 Adding a Pre-Shared Key 553
12.8.5.3 Deleting a Pre-Shared Key 553
12.8.6 Managing Connections 554
12.8.6.1 Viewing a List of Connections 554
12.8.6.2 Adding a Connection 555
12.8.6.3 Configuring Dead Peer Detection 557

12.8.6.4 Deleting a Connection 558
12.8.6.5 Viewing the Status of a Connection 558
12.8.7 Managing the Internet Key Exchange (IKE) Protocol 559
12.8.7.1 Viewing a List of IKE Algorithms 559
12.8.7.2 Adding an IKE Algorithm 560
12.8.7.3 Deleting an IKE Algorithm 560
12.8.8 Managing the Encapsulated Security Payload (ESP) Protocol 561
12.8.8.1 Configuring ESP Encryption 561
12.8.8.2 Viewing a List of ESP Algorithms 562
12.8.8.3 Adding an ESP Algorithm 562
12.8.8.4 Deleting an ESP Algorithm 563
12.8.9 Managing Connection Ends 563
12.8.9.1 Configuring the Public IP Address for a Connection End 563
12.8.9.2 Configuring the System Public Key for a Connection End 564
12.8.9.3 Configuring the System Identifier for a Connection End 565
12.8.9.4 Configuring the Next Hop for a Connection End 565
12.8.9.5 Configuring the NAT Traversal Negotiation Method for a Connection End 566
12.8.10 Managing Private Subnets 567
12.8.10.1 Viewing a List of Addresses for Private Subnets 567
12.8.10.2 Adding an Address for a Private Subnet 567
12.8.10.3 Deleting an Address for a Private Subnet 568
12.8.11 Example: Configuring an Encrypted VPN Tunnel 568

12.9 Managing 6in4 and 4in6 Tunnels 572
12.9.1 Enabling/Disabling 6in4 or 4in6 Tunnels 572
12.9.2 Viewing a List of 6in4 or 4in6 Tunnels 573
12.9.3 Viewing the Status of 6in4/4in6 Tunnels 573
12.9.4 Adding a 6in4 or 4in6 Tunnel 573
12.9.5 Deleting a 6in4 or 4in6 Tunnel 574

12.10 Managing DMVPN 575
12.10.1 Understanding DMVPN 575
12.10.2 Configuring DMVPN 576
12.10.3 Managing DMVPN Interfaces 577
12.10.3.1 Viewing a List of DMVPN Interfaces 577
12.10.3.2 Adding a DMVPN Interface 577
12.10.3.3 Deleting a DMVPN Interface 578
12.10.4 Viewing the Status of DMVPN 579

13 Unicast and Multicast Routing 581

13.1 Viewing the Status of IPv4 Routes 581

13.2 Viewing the Status of IPv6 Routes 582

13.3 Viewing the Memory Statistics 583

13.4 Configuring ICMP 584

13.5 Managing Event Trackers 584
13.5.1 Viewing a List of Event Trackers 585
13.5.2 Viewing Event Tracker Statistics 585
13.5.3 Adding an Event Tracker 586

13.5.4 Deleting an Event Tracker 587
13.6 Managing IS-IS 587
13.6.1 IS-IS Concepts 587
13.6.1.1 IS-IS Routers 588
13.6.1.2 Network Entity Title (NET) Addresses 588
13.6.1.3 Advantages and Disadvantages of Using IS-IS 589
13.6.2 Configuring IS-IS 589
13.6.3 Viewing the Status of Neighbors 590
13.6.4 Viewing the Status of the Link-State Database 591
13.6.5 Managing Area Tags 592
13.6.5.1 Viewing a List of Area Tags 592
13.6.5.2 Adding an Area Tag 593
13.6.5.3 Deleting an Area Tag 595
13.6.6 Managing Interfaces 595
13.6.6.1 Viewing a List of Interfaces 595
13.6.6.2 Configuring an Interface 596
13.6.7 Managing LSP Generation 597
13.6.7.1 Viewing a List of LSP Generation Intervals 597
13.6.7.2 Adding an LSP Generation Interval 598
13.6.7.3 Deleting an LSP Generation Interval 598
13.6.8 Managing SPF Calculations 599
13.6.8.1 Viewing a List of SPF Calculation Intervals 599
13.6.8.2 Adding an SPF Calculation Interval 599
13.6.8.3 Deleting an SPF Calculation Interval 600
13.6.9 Managing the Lifetime of LSPs 600
13.6.9.1 Viewing a List of LSP Lifetime Intervals 601
13.6.9.2 Adding an LSP Lifetime Interval 601
13.6.9.3 Deleting an LSP Lifetime Interval 602
13.6.10 Managing LSP Refresh Intervals 602
13.6.10.1 Viewing a List of LSP Refresh Intervals 603
13.6.10.2 Adding an LSP Refresh Interval 603
13.6.10.3 Deleting an LSP Refresh Interval 604
13.6.11 Managing Network Entity Titles (NETs) 604
13.6.11.1 Viewing a List of NETs 605
13.6.11.2 Adding a NET 605
13.6.11.3 Deleting a NET 605
13.6.12 Managing Redistribution Metrics 606
13.6.12.1 Viewing a List of Redistribution Metrics 606
13.6.12.2 Adding a Redistribution Metric 607
13.6.12.3 Deleting a Redistribution Metric 607
13.7 Managing RIP 608
13.7.1 Configuring RIP 608
13.7.2 Viewing the Status of Dynamic RIP Routes 610
13.7.3 Managing Prefix Lists and Entries 611
13.7.3.1 Viewing a List of Prefix Lists 612
13.7.3.2 Viewing a List of Prefix Entries 612
13.7.3.3 Adding a Prefix List 612
13.7.3.4 Adding a Prefix Entry 613

13.7.3.5 Deleting a Prefix List 614
13.7.3.6 Deleting a Prefix Entry 614
13.7.4 Managing Networks 614
13.7.4.1 Configuring a Network 615
13.7.4.2 Tracking Commands 615
13.7.5 Managing Network IP Addresses 616
13.7.5.1 Viewing a List of Network IP Addresses 616
13.7.5.2 Adding a Network IP Address 616
13.7.5.3 Deleting a Network IP Address 617
13.7.6 Managing Network Interfaces 617
13.7.6.1 Viewing a List of Network Interfaces 617
13.7.6.2 Adding a Network Interface 617
13.7.6.3 Deleting a Network Interface 618
13.7.7 Managing Neighbors 618
13.7.7.1 Viewing a List of Neighbors 618
13.7.7.2 Adding a Neighbor 618
13.7.7.3 Deleting a Neighbor 619
13.7.8 Managing the Prefix List Distribution 619
13.7.8.1 Viewing a List of Prefix List Distribution Paths 619
13.7.8.2 Adding a Prefix List Distribution Path 619
13.7.8.3 Deleting a Prefix List Distribution Path 620
13.7.9 Managing Key Chains and Keys 620
13.7.9.1 Viewing a List of Key Chains 620
13.7.9.2 Viewing a List of Keys 621
13.7.9.3 Adding a Key Chain 621
13.7.9.4 Adding a Key 622
13.7.9.5 Deleting a Key Chain 623
13.7.9.6 Deleting a Key 623
13.7.10 Managing Redistribution Metrics 623
13.7.10.1 Viewing a List of Redistribution Metrics 624
13.7.10.2 Adding a Redistribution Metric 624
13.7.10.3 Deleting a Redistribution Metric 624
13.7.11 Managing Routing Interfaces 624
13.7.11.1 Viewing a List of Routing Interfaces 625
13.7.11.2 Configuring a Routing Interface 625

13.8 Managing BGP 626
13.8.1 Configuring BGP 626
13.8.2 Managing Route Maps 628
13.8.2.1 Viewing a List of Route Map Filters 628
13.8.2.2 Viewing a List of Route Map Filter Entries 628
13.8.2.3 Adding a Route Map Filter 629
13.8.2.4 Adding a Route Map Filter Entry 629
13.8.2.5 Deleting a Route Map Filter 630
13.8.2.6 Deleting a Route Map Filter Entry 630
13.8.2.7 Configuring Match Rules 631
13.8.2.8 Configuring a Set 632
13.8.3 Managing Prepended and Excluded Autonomous System Path Filters 633
13.8.3.1 Viewing a List of Prepended Autonomous System Path Filters 633
13.8.3.2 Viewing a List of Excluded Autonomous System Paths 634

13.8.3.3 Adding a Prepended Autonomous System Path Filter 634
13.8.3.4 Adding an Excluded Autonomous System Path filter 635
13.8.3.5 Deleting a Prepended Autonomous System Path Filter 635
13.8.3.6 Deleting an Excluded Autonomous System Path Filter 635
13.8.4 Managing Prefix Lists and Entries 636
13.8.4.1 Viewing a List of Prefix Lists 636
13.8.4.2 Viewing a List of Prefix Entries 636
13.8.4.3 Adding a Prefix List 637
13.8.4.4 Adding a Prefix Entry 637
13.8.4.5 Deleting a Prefix List 638
13.8.4.6 Deleting a Prefix Entry 638
13.8.5 Managing Autonomous System Paths and Entries 639
13.8.5.1 Viewing a List of Autonomous System Paths 639
13.8.5.2 Viewing a List of Autonomous System Path Entries 639
13.8.5.3 Adding an Autonomous System Path Filter 640
13.8.5.4 Adding an Autonomous System Path Filter Entry 640
13.8.5.5 Deleting an Autonomous System Path 641
13.8.5.6 Deleting an Autonomous System Path Filter Entry 641
13.8.6 Managing Neighbors 641
13.8.6.1 Viewing a List of Neighbors 642
13.8.6.2 Adding a Neighbor 642
13.8.6.3 Configuring the Distribution of Prefix Lists 643
13.8.6.4 Tracking Commands for BGP Neighbors 644
13.8.6.5 Deleting a Neighbor 645
13.8.7 Managing Networks 645
13.8.7.1 Viewing a List of Networks 645
13.8.7.2 Adding a Network 646
13.8.7.3 Tracking Commands for a BGP Network 646
13.8.7.4 Deleting a Network 647
13.8.8 Managing Aggregate Addresses 647
13.8.8.1 Viewing a List of Aggregate Addresses 647
13.8.8.2 Adding an Aggregate Address 648
13.8.8.3 Deleting an Aggregate Address 648
13.8.9 Managing Aggregate Address Options 648
13.8.9.1 Viewing a List of Aggregate Address Options 648
13.8.9.2 Adding an Aggregate Address Option 649
13.8.9.3 Deleting an Aggregate Address Option 649
13.8.10 Managing Redistribution Metrics 649
13.8.10.1 Viewing a List of Redistribution Metrics 649
13.8.10.2 Adding a Redistribution Metric 650
13.8.10.3 Deleting a Redistribution Metric 650
13.8.11 Managing Route Reflector Options 650
13.8.11.1 Understanding Route Reflectors 651
13.8.11.2 Configuring the Device as a Route Reflector 654
13.8.11.3 Configuring BGP Neighbors as Clients 654
13.8.11.4 Example: Basic Route Reflection 655
13.8.11.5 Example: Linking Clusters 657
13.8.11.6 Example: Clusters in Clusters 659
13.8.11.7 Example: Route Reflection in a VRF Instance 661

13.8.11.8 Example: Route Reflection with VPNv4 Clients 664
13.8.12 Viewing the Status of Dynamic BGP Routes 665
13.8.13 Resetting a BGP Session 667
13.9 Managing OSPF 668
13.9.1 OSPF Concepts 669
13.9.2 Configuring OSPF 669
13.9.3 Viewing the Status of Dynamic OSPF Routes 672
13.9.4 Managing Prefix Lists and Entries 675
13.9.4.1 Viewing a List of Prefix Lists 675
13.9.4.2 Viewing a List of Prefix Entries 676
13.9.4.3 Adding a Prefix List 676
13.9.4.4 Adding a Prefix Entry 677
13.9.4.5 Deleting a Prefix List 678
13.9.4.6 Deleting a Prefix Entry 678
13.9.5 Managing Areas 679
13.9.5.1 Viewing a List of Areas 679
13.9.5.2 Adding an Area 679
13.9.5.3 Deleting an Area 680
13.9.6 Managing Route Maps 681
13.9.6.1 Viewing a List of Route Map Filters 681
13.9.6.2 Viewing a List of Route Map Filter Entries 681
13.9.6.3 Adding a Route Map Filter 682
13.9.6.4 Adding a Route Map Filter Entry 683
13.9.6.5 Deleting a Route Map Filter 683
13.9.6.6 Deleting a Route Map Filter Entry 684
13.9.6.7 Configuring Match Rules 684
13.9.7 Managing Incoming Route Filters 685
13.9.7.1 Viewing List of Incoming Route Filters 685
13.9.7.2 Adding an Incoming Route Filter 686
13.9.7.3 Deleting an Incoming Route Filter 686
13.9.8 Managing Redistribution Metrics 687
13.9.8.1 Viewing a List of Redistribution Metrics 687
13.9.8.2 Adding a Redistribution Metric 687
13.9.8.3 Deleting a Redistribution Metric 688
13.9.9 Managing Routing Interfaces 688
13.9.9.1 Viewing a List of Routing Interfaces 688
13.9.9.2 Configuring a Routing Interface 689
13.9.10 Managing Message Digest Keys 691
13.9.10.1 Viewing a List of Message Digest Keys 692
13.9.10.2 Adding a Message Digest Key 692
13.9.10.3 Deleting a Message Digest Key 693
13.9.11 Managing ABR Route Summarization 693
13.9.11.1 Understanding ABR Route Summarization 693
13.9.11.2 Viewing a List of Summary Routes 694
13.9.11.3 Adding a Summary Route 694
13.9.11.4 Deleting a Summary Route 695
13.9.11.5 Example: Basic Route Summarization 695
13.10 Managing MPLS 697

13.10.1 Viewing the Status of IP Binding 697
13.10.2 Viewing the Status of the Forwarding Table 698
13.10.3 Enabling/Disabling MPLS 699
13.10.4 Managing the MPLS Interfaces 699
13.10.4.1 Viewing the Status of MPLS Interfaces 699
13.10.4.2 Viewing a List of MPLS Interfaces 700
13.10.4.3 Enabling/Disabling an MPLS Interface 700
13.10.5 Managing Static Label Binding 700
13.10.5.1 Viewing the Status of Static Label Binding 701
13.10.5.2 Viewing a List of Static Labels 701
13.10.5.3 Adding a Static Label 702
13.10.5.4 Deleting a Static Label 702
13.10.6 Managing Static Cross-Connects 703
13.10.6.1 Viewing the Status of Static Cross-Connects 703
13.10.6.2 Viewing a List of Static Cross-Connects 704
13.10.6.3 Adding a Static Cross-Connect 704
13.10.6.4 Deleting a Static Cross-Connect 705
13.10.7 Managing LDP 705
13.10.7.1 Viewing the Status of LDP Binding 705
13.10.7.2 Viewing the Status of the LDP Discovery Interfaces 706
13.10.7.3 Viewing the Status of the LDP Neighbor Local Node Information 707
13.10.7.4 Viewing the Status of the LDP Neighbor Connection Information 707
13.10.7.5 Viewing the Status of the LDP Neighbor Discovery Information 708
13.10.7.6 Configuring LDP 709
13.10.7.7 Configuring Neighbor Discovery 710
13.10.7.8 Viewing a List of LDP Interfaces 710
13.10.7.9 Enabling/Disabling an LDP Interface 710

13.11 Managing Virtual Routing and Forwarding (VRF) 711
13.11.1 VRF Concepts 711
13.11.1.1 VRF and VRF-Lite 711
13.11.1.2 Advantages and Disadvantages of Using VRF 712
13.11.2 Viewing VRF Interface Statistics 712
13.11.3 Configuring VRF 713
13.11.4 Configuring a VRF Interface 714
13.11.5 Managing VRF Definitions 715
13.11.5.1 Viewing a List of VRF Definitions 715
13.11.5.2 Adding a VRF Definition 715
13.11.5.3 Deleting a VRF Definition 716
13.11.6 Managing Route Targets 717
13.11.6.1 Viewing a List of Route Targets 717
13.11.6.2 Adding a Route Target 717
13.11.6.3 Deleting a Route Target 718
13.11.7 Managing VRF Instances and OSPF 718
13.11.7.1 Viewing a List of VRF Instances 718
13.11.7.2 Adding a VRF Instance and Configuring OSPF 719
13.11.7.3 Deleting a VRF Instance 723
13.11.8 Managing IP/VPN Tunnels 724
13.11.8.1 Viewing a List of IP/VPN Tunnels 724
13.11.8.2 Adding an IP/VPN Tunnel 724

13.11.8.3 Deleting an IP/VPN Tunnels 725
13.11.9 Managing VPNv4 Neighbors 725
13.11.9.1 Viewing a List of Neighbors 725
13.11.9.2 Adding a Neighbor 725
13.11.9.3 Deleting a Neighbor 726
13.11.10 Managing IPv4 Address Families 726
13.11.10.1 Viewing a List of IPv4 Address Families 726
13.11.10.2 Adding an IPv4 Address Family 727
13.11.10.3 Deleting an IPv4 Address Family 727
13.11.11 Managing Redistribution for IPv4 Address Families 727
13.11.11.1 Viewing a List of Redistributions 728
13.11.11.2 Adding a Redistribution 728
13.11.11.3 Deleting a Redistribution 729
13.11.12 Managing Neighbors for IPv4 Address Families 729
13.11.12.1 Viewing a List of Neighbors 729
13.11.12.2 Adding a Neighbor 730
13.11.12.3 Configuring the Distribution of Prefix Lists 731
13.11.12.4 Tracking Commands 732
13.11.12.5 Deleting a Neighbor 732
13.11.13 Managing Static VRF Routes 733
13.11.13.1 Viewing a List of Static VRF Routes 733
13.11.13.2 Adding a Static VRF Route 733
13.11.13.3 Configuring a Black Hole Connection for a Static VRF Route 734
13.11.13.4 Deleting a Static VRF Route 734
13.11.14 Managing Gateways for Static VRF Routes 735
13.11.14.1 Viewing a List of Gateways for Static VRF Routes 735
13.11.14.2 Adding a Gateway for a Static VRF Route 735
13.11.14.3 Deleting a Gateway for a Static VRF Route 736
13.11.15 Managing Interfaces for Static VRF Routes 736
13.11.15.1 Viewing a List of Interfaces for Static VRF Routes 736
13.11.15.2 Adding a Gateway for a Static VRF Route 737
13.11.15.3 Deleting a Gateway for a Static VRF Route 737
13.11.16 Example: Configuring OSPF on a VRF-Lite Instance 738
13.11.17 Example: Configuring BGP on a VRF-Lite Instance 740

13.12 Managing Static Routing 744
13.12.1 Viewing a List of Static Routes 744
13.12.2 Adding an IPv4 Static Route 744
13.12.3 Adding an IPv6 Static Route 745
13.12.4 Deleting a Static Route 746
13.12.5 Configuring a Black Hole Connection for an IPv4 Static Route 746
13.12.6 Managing Gateways for Static Routes 747
13.12.6.1 Configuring Gateways for IPv6 Static Routes 747
13.12.6.2 Viewing a List of Gateways for IPv4 Static Routes 747
13.12.6.3 Adding a Gateway for an IPv4 Static Route 748
13.12.6.4 Deleting a Gateway for an IPv4 Static Route 748
13.12.7 Managing Interfaces for Static Routes 749
13.12.7.1 Configuring Interfaces for IPv6 Static Routes 749
13.12.7.2 Viewing a List of Interfaces for IPv4 Static Routes 749
13.12.7.3 Adding an Interface for an IPv4 Static Route 750

13.12.7.4 Deleting an Interface for an IPv4 Static Route 750
13.13 Managing Static Multicast Routing 750
13.13.1 Enabling/Disabling Static Multicast Routing 750
13.13.2 Managing Static Multicast Groups 751
13.13.2.1 Viewing a List of Static Multicast Groups 751
13.13.2.2 Adding a Static Multicast Group 751
13.13.2.3 Deleting a Static Multicast Group 752
13.13.3 Managing Out-Interfaces 753
13.13.3.1 Viewing a List of Out-Interfaces 753
13.13.3.2 Adding an Out-Interface 753
13.13.3.3 Deleting an Out-Interface 753
13.14 Managing Dynamic Multicast Routing 754
13.14.1 Understanding Protocol Independent Multicast 754
13.14.1.1 PIM-SM Concepts 754
13.14.1.2 Internet Group Management Protocol 756
13.14.1.3 PIM-SSM 757
13.14.2 Viewing the Status of PIM-SM 757
13.14.3 Viewing the Status of Dynamic Multicast Routing 762
13.14.4 Configuring PIM-SM 762
13.14.5 Setting the Device as a BSR Candidate 763
13.14.6 Setting the Device as an RP Candidate 764
13.14.7 Managing PIM-SM Interfaces 764
13.14.7.1 Viewing a List of PIM-SM Interfaces 764
13.14.7.2 Enabling/Disabling a PIM-SM Interface 765
13.14.8 Managing Static RP Addresses 766
13.14.8.1 Viewing a List of Static RP Addresses 766
13.14.8.2 Adding a Static RP Address 766
13.14.8.3 Deleting a Static RP Address 767
13.14.9 Managing Multicast Group Prefixes 767
13.14.9.1 Viewing a List of Multicast Group Prefixes 767
13.14.9.2 Adding a Multicast Group Prefix 768
13.14.9.3 Deleting a Multicast Group Prefix 768
13.14.10 Example: Configuring Protocol Independent Multicast 768
14 Network Redundancy 775
14.1 Managing VRRP 775
14.1.1 VRRP Concepts 775
14.1.1.1 Static Routing vs. VRRP 775
14.1.1.2 VRRP Terminology 776
14.1.1.3 Connection Synchronization 779
14.1.2 Viewing the Status of VRRP 779
14.1.3 Enabling/Disabling VRRP 780
14.1.4 Managing VRRP Trackers 780
14.1.4.1 Viewing a List of VRRP Trackers 781
14.1.4.2 Adding a VRRP Tracker 781
14.1.4.3 Deleting a VRRP Tracker 782
14.1.5 Managing VRRP Groups 782
14.1.5.1 Viewing a List of VRRP Groups 783

14.1.5.2 Adding a VRRP Group 783
14.1.5.3 Deleting a VRRP Group 783
14.1.6 Managing VRRP Instances 784
14.1.6.1 Viewing a List of VRRP Instances 784
14.1.6.2 Adding a VRRP Instance 784
14.1.6.3 Deleting a VRRP Instance 786
14.1.7 Managing VRRP Monitors 787
14.1.7.1 Viewing a List of VRRP Monitors 787
14.1.7.2 Adding a VRRP Monitor 787
14.1.7.3 Deleting a VRRP Monitor 788
14.1.8 Managing Track Scripts 788
14.1.8.1 Viewing a List of Track Scripts 788
14.1.8.2 Adding a Track Script 789
14.1.8.3 Deleting a Track Script 789
14.1.9 Managing Virtual IP Addresses 789
14.1.9.1 Viewing a List of Virtual IP Addresses 790
14.1.9.2 Adding a Virtual IP Address 790
14.1.9.3 Deleting a Virtual IP Address 790
14.1.10 Managing Connection Synchronization 791
14.1.10.1 Configuring Connection Synchronization 791
14.1.10.2 Enabling/Disabling Connection Synchronization 792
14.1.10.3 Viewing a List of Dedicated Links 792
14.1.10.4 Adding a Dedicated Link 792
14.1.10.5 Deleting a Dedicated Link 793
14.1.10.6 Selecting a Default Dedicated Link 793
14.1.10.7 Viewing the Status of Each Dedicated Link 794

14.2 Managing VRRP within VRF 795
14.2.1 Configuring VRRP within VRF 795
14.2.2 Viewing the VRRP Status for a VRF 796
14.2.3 Configuring VRRP Service for a VRF 796
14.2.3.1 Viewing a List of VRFs Configured with VRRP Service 796
14.2.3.2 Adding VRRP Service to a VRF 797
14.2.3.3 Deleting VRRP Service from a VRF 798
14.2.4 Managing VRRP Trackers for a VRF 798
14.2.4.1 Viewing a List of VRRP Trackers for a VRF 798
14.2.4.2 Adding a VRRP Tracker for a VRF 799
14.2.4.3 Deleting a VRRP Tracker for a VRF 800
14.2.5 Managing VRRP Groups for a VRF 800
14.2.5.1 Viewing a List of VRRP Groups for a VRF 800
14.2.5.2 Adding a VRRP Group for a VRF 800
14.2.5.3 Deleting a VRRP Group 801
14.2.6 Managing VRRP Instances for a VRF 801
14.2.6.1 Viewing a List of VRRP Instances for a VRF 801
14.2.6.2 Adding a VRRP Instance for a VRF 802
14.2.6.3 Deleting a VRRP Instance for a VRF 803
14.2.7 Managing VRRP Monitors for a VRF 804
14.2.7.1 Viewing a List of VRRP Monitors for a VRF 804
14.2.7.2 Adding a VRRP Monitor to a VRF 804
14.2.7.3 Deleting a VRRP Monitor from a VRF 805

14.2.8 Managing VRRP Track Scripts for a VRF 805
14.2.8.1 Viewing a List of VRRP Track Scripts for a VRF 805
14.2.8.2 Adding a VRRP Track Script to a VRF 806
14.2.8.3 Deleting a VRRP Track Script from a VRF 806
14.2.9 Managing Virtual IP Addresses for a VRF 807
14.2.9.1 Viewing a List of Virtual IP Addresses 807
14.2.9.2 Adding a Virtual IP Address to a VRF 808
14.2.9.3 Deleting a Virtual IP Address from a VRF 808
14.2.10 Example: Configuring VRRP within a VRF 808

14.3 Managing Link Failover Protection 811
14.3.1 Viewing the Link Failover Log 812
14.3.2 Viewing the Link Failover Status 812
14.3.3 Managing Link Failover Parameters 813
14.3.3.1 Viewing a List of Link Failover Parameters 813
14.3.3.2 Adding a Link Failover Parameter 814
14.3.3.3 Deleting a Link Failover Parameter 815
14.3.4 Managing Link Failover Backup Interfaces 815
14.3.4.1 Viewing a List of Link Failover Backup Interfaces 815
14.3.4.2 Adding a Link Failover Backup Interface 816
14.3.4.3 Deleting a Link Failover Backup Interface 817
14.3.5 Managing Link Failover Ping Targets 817
14.3.5.1 Viewing a List of Link Failover Ping Targets 818
14.3.5.2 Adding a Link Failover Ping Target 818
14.3.5.3 Deleting a Link Failover Ping target 819
14.3.6 Testing Link Failover 819
14.3.7 Canceling a Link Failover Test 820

14.4 Managing Spanning Tree Protocol 820
14.4.1 RSTP Operation 820
14.4.1.1 RSTP States and Roles 820
14.4.1.2 Edge Ports 822
14.4.1.3 Point-to-Point and Multipoint Links 822
14.4.1.4 Path and Port Costs 823
14.4.1.5 Bridge Diameter 823
14.4.1.6 eRSTP 824
14.4.1.7 Fast Root Failover 824
14.4.2 RSTP Applications 825
14.4.2.1 RSTP in Structured Wiring Configurations 826
14.4.2.2 RSTP in Ring Backbone Configurations 827
14.4.2.3 RSTP Port Redundancy 828
14.4.3 MSTP Operation 829
14.4.3.1 MSTP Regions and Interoperability 829
14.4.3.2 MSTP Bridge and Port Roles 830
14.4.3.3 Benefits of MSTP 832
14.4.3.4 Implementing MSTP on a Bridged Network 833
14.4.4 Configuring STP Globally 833
14.4.5 Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces 836
14.4.6 Managing Multiple Spanning Tree Instances Globally 838
14.4.6.1 Viewing Statistics for Multiple Spanning Tree Instances 839

14.4.6.2 Viewing a List of Multiple Spanning Tree Instances 840
14.4.6.3 Adding a Multiple Spanning Tree Instance 841
14.4.6.4 Deleting a Multiple Spanning Tree Instance 841
14.4.7 Managing Multiple Spanning Tree Instances Per-Port 842
14.4.7.1 Viewing Per-Port Multiple Spanning Tree Instance Statistics 842
14.4.7.2 Viewing a List of Per-Port Multiple Spanning Tree Instances 844
14.4.7.3 Adding a Port-Specific Multiple Spanning Tree Instance 845
14.4.7.4 Deleting a Port-Specific Multiple Spanning Tree Instances 846
14.4.8 Viewing the Status of RSTP 847
14.4.9 Viewing RSTP Per-Port Statistics 849
14.4.10 Clearing Spanning Tree Protocol Statistics 851

14.5 Managing the Media Redundancy Protocol (MRP) 851
14.5.1 Understanding MRP 852
14.5.1.1 MRP Operation 852
14.5.1.2 MRA 853
14.5.1.3 MRP Instances 853
14.5.1.4 Requirements and Restrictions 854
14.5.2 Configuring MRP Globally 854
14.5.3 Enabling/Disabling SNMP Traps for MRP 854
14.5.4 Viewing the List of MRP Instances 855
14.5.5 Adding an MRP Instance 856
14.5.6 Deleting an MRP Instance 858
14.5.7 Viewing the Status of MRP Instances 858
14.5.8 Example: Configuring an MRP Ring 860

15 Network Discovery and Management 863

15.1 Managing LLDP 863
15.1.1 Configuring LLDP 864
15.1.2 Viewing Global Statistics 865
15.1.3 Viewing Global Statistics and Advertised System Information 866
15.1.4 Viewing Statistics for LLDP Neighbors 868
15.1.5 Viewing Statistics for LLDP Ports 873

15.2 Managing SNMP 874
15.2.1 Enabling and Configuring SNMP Sessions 875
15.2.2 Viewing Statistics for SNMP 877
15.2.3 Discovering SNMP Engine IDs 878
15.2.4 Managing SNMP Communities 879
15.2.4.1 Viewing a List of SNMP Communities 879
15.2.4.2 Adding an SNMP Community 879
15.2.4.3 Deleting an SNMP Community 880
15.2.5 Managing SNMP Target Addresses 880
15.2.5.1 Viewing a List of SNMP Target Addresses 880
15.2.5.2 Adding an SNMP Target Address 880
15.2.5.3 Deleting an SNMP Target Address 883
15.2.6 Managing SNMP Users 883
15.2.6.1 Viewing a List of SNMP Users 883
15.2.6.2 Adding an SNMP User 883
15.2.6.3 Deleting an SNMP User 885

15.2.7 Managing SNMP Security Model Mapping 885
15.2.7.1 Viewing a List of SNMP Security Models 885
15.2.7.2 Adding an SNMP Security Model 886
15.2.7.3 Deleting an SNMP Security Model 886
15.2.8 Managing SNMP Group Access 886
15.2.8.1 Viewing a List of SNMP Groups 887
15.2.8.2 Adding an SNMP Group 887
15.2.8.3 Deleting an SNMP Group 888

15.3 Managing NETCONF 889
15.3.1 Enabling and Configuring NETCONF Sessions 889
15.3.2 Viewing NETCONF Statistics 891

15.4 Managing IPv4 Neighbors 892
15.4.1 IPv4 Neighbor Concepts 892
15.4.2 Viewing IPv4 Neighbors 892
15.4.3 Clearing IPv4 Neighbors 894

16 Traffic Control and Classification 895

16.1 Managing Port Mirroring 895
16.1.1 Configuring Port Mirroring 895
16.1.2 Managing Egress Source Ports 896
16.1.2.1 Viewing a List of Egress Source Ports 896
16.1.2.2 Adding an Egress Source Port 897
16.1.2.3 Deleting an Egress Source Port 897
16.1.3 Managing Ingress Source Ports 897
16.1.3.1 Viewing a List of Ingress Source Ports 898
16.1.3.2 Adding an Ingress Source Port 898
16.1.3.3 Deleting an Ingress Source Port 898

16.2 Managing Traffic Control 899
16.2.1 Enabling and Configuring Traffic Control 899
16.2.2 Managing Traffic Control Interfaces 901
16.2.2.1 Viewing a List of Traffic Control Interfaces 901
16.2.2.2 Adding a Traffic Control Interface 901
16.2.2.3 Deleting a Traffic Control Interface 902
16.2.3 Managing Traffic Control Priorities 903
16.2.3.1 Viewing a List of Traffic Control Priorities 903
16.2.3.2 Adding a Traffic Control Priority 904
16.2.3.3 Deleting a Traffic Control Priority 905
16.2.4 Managing Traffic Control Classes 905
16.2.4.1 Viewing a List of Traffic Control Classes 906
16.2.4.2 Adding a Traffic Control Class 906
16.2.4.3 Deleting a Traffic Control Class 908
16.2.5 Managing Traffic Control Devices 908
16.2.5.1 Viewing a List of Traffic Control Devices 909
16.2.5.2 Adding a Traffic Control Device 909
16.2.5.3 Deleting a Traffic Control Device 910
16.2.6 Managing Traffic Control Rules 910
16.2.6.1 Viewing a List of Traffic Control Rules 911
16.2.6.2 Adding a Traffic Control Rule 911

16.2.6.3 Configuring QoS Marking 913
16.2.6.4 Deleting aTraffic Control Rule 917
16.2.7 Managing QoS Mapping for VLANs 917
16.2.7.1 Viewing a List of QoS Maps for VLANs 917
16.2.7.2 Adding a QoS Map 919
16.2.7.3 Deleting a QoS Map 920
16.2.8 Managing Egress Markers for QoS Maps 921
16.2.8.1 Viewing a List of Egress Marks 921
16.2.8.2 Adding an Egress Mark 922
16.2.8.3 Deleting an Egress Mark 924
16.2.9 Viewing QoS Statistics 925

16.3 Managing Classes of Service 926
16.3.1 Configuring Classes of Service 927
16.3.2 Managing Priority-to-CoS Mapping 927
16.3.2.1 Viewing a List of Priority-to-CoS Mapping Entries 928
16.3.2.2 Adding a Priority-to-CoS Mapping Entry 928
16.3.2.3 Deleting a Priority-to-CoS Mapping Entry 929
16.3.3 Managing DSCP-to-CoS Mapping 929
16.3.3.1 Viewing a List of DSCP-to-CoS Mapping Entries 929
16.3.3.2 Adding a DSCP-to-CoS Mapping Entry 929
16.3.3.3 Deleting a DSCP-to-CoS Mapping Entry 930

16.4 Managing NetFlow Data Export 930
16.4.1 Understanding NetFlow Data Export 931
16.4.1.1 Flow Records 932
16.4.2 Configuring NetFlow Data Export 932
16.4.3 Enabling/Disabling NetFlow 933
16.4.4 Setting the NetFlow Engine ID 933
16.4.5 Controlling the NetFlow Cache 934
16.4.6 Controlling Active/Inactive Flows 934
16.4.7 Managing NetFlow Interfaces 935
16.4.7.1 Viewing a List of NetFlow Interfaces 935
16.4.7.2 Adding a NetFlow Interface 935
16.4.7.3 Deleting a NetFlow Interface 936
16.4.8 Managing NetFlow Collectors 936
16.4.8.1 Viewing a List of NetFlow Collectors 936
16.4.8.2 Adding a NetFlow Collector 936
16.4.8.3 Enabling/Disabling a NetFlow Collector 937
16.4.8.4 Deleting a NetFlow Collector 937
16.4.9 Viewing the Status of NetFlow 938
16.4.10 Example: Exporting Flows to Multiple Collectors 938

16.5 Managing Port Rate Limiting 940
16.5.1 Understanding Port Rate Limiting 940
16.5.2 Configuring Port Rate Limiting 940

17 Time Services 943

17.1 Configuring the Time Synchronization Settings 943

17.2 Configuring the System Time and Date 944

17.3 Configuring the System Time Zone 944
17.4 Configuring the Local Time Settings 944
17.5 Enabling and Configuring the NTP Service 945
17.6 Viewing the NTP Service Status 945
17.7 Viewing the Status of Reference Clocks 947
17.8 Managing NTP Servers 948
17.8.1 Viewing a List of NTP Servers 948
17.8.2 Monitoring Subscribers 949
17.8.3 Adding an NTP Server 950
17.8.4 Deleting an NTP Server 951
17.8.5 Managing Server Keys 951
17.8.5.1 Viewing a List of Server Keys 952
17.8.5.2 Adding a Server Key 952
17.8.5.3 Deleting a Server Key 952
17.8.6 Managing Server Restrictions 953
17.8.6.1 Viewing a List of Server Restrictions 953
17.8.6.2 Adding a Server Restriction 953
17.8.6.3 Deleting a Server Restriction 954
17.9 Managing NTP Broadcast/Multicast Clients 955
17.9.1 Enabling and Configuring NTP Multicast Clients 955
17.9.2 Enabling and Configuring NTP Broadcast Clients 955
17.9.3 Managing NTP Broadcast/Multicast Addresses 956
17.9.3.1 Viewing a List of Broadcast/Multicast Addresses 956
17.9.3.2 Adding a Broadcast/Multicast Address 957
17.9.3.3 Deleting a Broadcast/Multicast Address 957
18 Applications 959
18.1 Viewing a List of Installed Applications 959
18.2 Installing an Application 959
18.3 Upgrading an Application 960
18.4 Uninstalling an Application 960
18.5 Managing the RUGGEDCOM CROSSBOW Application 960
18.5.1 Enabling/Disabling CROSSBOW 961
18.5.2 Configuring the Client Connection 961
18.5.3 Configuring CROSSBOW Certificates and Private Keys 962
18.5.4 Managing SAC Connections 962
18.5.4.1 Viewing a List of SAC Connections 963
18.5.4.2 Adding a SAC Connection 963
18.5.4.3 Deleting a SAC Connection 963
18.5.5 Managing CROSSBOW CA Certificate Lists 964
18.5.5.1 Viewing a List of RUGGEDCOM CROSSBOW Certificate Lists 964
18.5.5.2 Adding a CA Certificate List 964
18.5.5.3 Deleting a CA Certificate List 965
18.5.6 Viewing the Status of RUGGEDCOM CROSSBOW 965
18.5.7 Viewing the RUGGEDCOM CROSSBOW Log 965

19 Troubleshooting 967
19.1 Management Access 967
19.2 Feature Keys 968
19.3 Ethernet Ports 968
19.4 Multicast Filtering 968
19.5 Spanning Tree 969
19.6 VLANs 971
19.7 Firmware Updates 972
20 Reference 973
20.1 Supported MIBs 973
20.2 Standard SNMP Traps 1041
20.3 Proprietary SNMP Traps 1043
20.4 Supported Cipher Suites 1054

Preface

This document describes the CLI user interface for RUGGEDCOM ROX II v2.16 running on the RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536. 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] 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.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit https://www.siemens.com/cybersecurity-industry.

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 Cybersecurity 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.

CLI command syntax

This document details CLI commands. A CLI command consists of a key command, parameters, options and/or user variables.

Elements of a CLI command

In the following CLI command, `interface` is the key command, { name } is a user-defined value, `vlan` and `type` are parameters, and `access` and `trunk` are fixed options.

```
interface { name } vlan type [ access | trunk ]
```

Command formatting

CLI commands are displayed in this document according to the following syntax rules:

Convention	Description	Example
Font	All commands, parameters, and options are displayed in a monospace font.	`command parameter`
User-Defined Values	Some parameters require a user-defined value. Values that need to be defined by you are wrapped in braces (curly brackets). The value can be a string, such as a name or description.	`command parameter { value }`

Convention	Description	Example
	The value may be a system component, such as an ID or interface. In all cases, the key word between the braces indicates the type of value to enter.	
Number Ranges	When the value of a parameter is a number within a specific range, the range is enclosed in braces (curly brackets).	`command parameter { 0 - 10 }`
Options	When multiple choices are available for the value of a parameter, all choices are wrapped in square brackets. Choices are often comprised of fixed values, but may also include user-defined values and/or number ranges.	`command parameter [ option1 | option2 | { value } | { 0 - 10 } ]`

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 Rugged CLI interface must meet the following system requirements:

- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536.
- The ability to configure an IP address and netmask on the computer's Ethernet interface
- A suitable Ethernet cable
- An SSH client application installed on a computer

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.

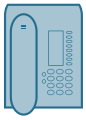
For more information about training services and course availability, visit https://www.siemens.com or contact a Siemens Sales representative.

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:

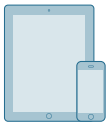
Online

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.



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

Address	Siemens Canada Ltd. Digital Industries Process Automation 300 Applewood Crescent Concord, Ontario Canada, L4K 5C7
Telephone	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288 Fax: +1 905 856 1995
E-Mail	info.ruggedcom@siemens.com
Web	https://www.siemens.com

1 Introduction

Welcome to the **RUGGEDCOM ROX II (Rugged Operating System on Linux®) v2.16 Configuration Manual**. This document details how to configure the RX1500 via the RUGGEDCOM ROX II Command Line Interface (CLI). RUGGEDCOM ROX II also features a Web interface, 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 Web interface. This is indicated throughout the Configuration Manual where applicable.

This document is specific to the following device platforms:

- RUGGEDCOM RX1500
- RUGGEDCOM RX1501
- RUGGEDCOM RX1510
- RUGGEDCOM RX1511
- RUGGEDCOM RX1512
- RUGGEDCOM RX1524
- RUGGEDCOM RX1536

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 7).

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:

Passwords	Multi-level user passwords secures against unauthorized configuration
SSH/SSL	Extends capability of password protection to add encryption of passwords and data as they cross the network
Enable/Disable Ports	Capability to disable ports so that traffic cannot pass

IEEE 802.1Q VLAN	Provides the ability to logically segregate traffic between predefined ports on switches
SNMPv3	Encrypted authentication and access security
HTTPS	For secure access to the Web interface
Firewall	Integrated stateful firewall provides protected network zones
VPN/IPSEC	Allows creation of secure encrypted and authenticated tunnels
IEEE 802.1X	Offers network access control through port-based authentication and authorization
RADIUS/TACACS+	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 1054).

- **RUGGEDCOM CROSSBOW ADM Agent**
  The RUGGEDCOM CROSSBOW Asset Discovery and Management (ADM) Agent is a security feature used to discover and monitor the activity of network connected devices. This information is collected and reported to the Secure Access Manager (SAM). Operators using CROSSBOW are then made aware of any devices added to the operational environment within minutes of activation through the CROSSBOW user interface and event logging system. Purposefully deployed devices can be identified and vetted for inclusion, while rogue devices can be quickly identified and isolated.

  RUGGEDCOM CROSSBOW ADM is available through a dedicated ADM module with ADM software installed.

  Note

  The ADM must be reachable from the RUGGEDCOM CROSSBOW SAM server.

  For more information about RUGGEDCOM CROSSBOW ADM, including configuration steps and specific security recommendations, contact Siemens Customer Support.

- **Enhanced Rapid Spanning Tree Protocol (eRSTP)™**
  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]".
- **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]).

- **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 RX1500 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.

- **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 RX1500/RX1501/RX1510/RX1511/RX1512 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.

The following feature keys are currently available for select devices:

Feature Key	RX1500	RX1501	RX1510	RX1511	RX1512	RX1524	RX1536
Layer 2 Standard Edition (L2SE)	•	•	•	•	•		
Layer 3 Standard Edition with Layer 3 Hardware (L3SEL3HW)	•	•	•	•	•	•	•
Layer 3 Standard Edition with Layer 2 Hardware (L3SEL2HW)	•	•	•	•	•		
Layer 3 Security Edition with Layer 3 Hardware (L3SECL3HW)	•	•	•	•	•	•	•
Layer 3 Security Edition with Layer 2 Hardware (L3SECL2HW)	•	•	•	•	•		

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	•	•	•	•	•

Feature	Feature Key				
	Layer 2 Standard Edition (L2SE)	L3SEL3HW	L3SEL2HW	L3SECL3HW	L3SECL2HW
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		•		•	
Jumbo Frame Support		•		•	

For information about installing and viewing the contents of feature keys, refer to "Managing Feature Keys" (Page 88).

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 153).

  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 166).

- 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 895). For more information about enabling ingress filtering, refer to "Enabling/Disabling Ingress Filtering" (Page 383).
- 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 383).
- 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 874).

- 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 235).
- 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 93).
- 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 235) and "Managing IPsec Tunnels" (Page 546).
- 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.
- Make sure the device is fully decommissioned before taking the device out of service. For more information, refer to "Decommissioning the Device" (Page 87).

- 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 177).

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 and security advisories, visit the CERT services website [https://new.siemens.com/global/en/products/services/cert.html]. To stay informed about new product security advisories, consider registering for the Siemens ProductCERT mailing list or subscribing to the RSS feed.
- 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 13).
- 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 124).

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
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

Services	Port Number	Port Default	Authenticated Access
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[a]
/admin/alarms-config/	R/U	R/U	No[b]
/admin/users	C/R/U	No	No
/admin/users/userid	R/U	R/U[c]	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

Commands/Paths Permitted	Access		
	Administrator	Operator	Guest
/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/sytem-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
/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

Commands/Paths Permitted	Access		
	Administrator	Operator	Guest
/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

[a] Only administrator and operator profiles can clear and acknowledge alarms or see the status of active alarms.

[b] Only administrator and operator profiles can create and delete alarm lists.

[c] Operator profiles can only change their own password and cannot create users.

1.6 Removable Memory

The RUGGEDCOM RX1500 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 RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 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 RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536.

For CLI commands used to manage the USB Mass Storage device, refer to "File Commands" (Page 46) and "Administration Commands" (Page 56).

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 94).

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[a]	The source of the event. Options include: • AUTH • AUTHPRIV • DAEMON • USER
Severity[a]	The severity level associated with the event. Options include: • INFO • NOTICE • AUTH • AUTHPRIV

Element	Description
	• ERR • CRITICAL • EMERGENCY
Message Text	Information about the event.

[a] 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 *authorized* activities that can be expected to occur during routine use.
Alarm	Alarms are activities that may indicate *unauthorized* 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[{pid}]: audit user: {user}/{user id} assigned to groups: {role}	LOG_AUTHPRIV	Info	Event	Auth.log
ruggedcom rmfmgr[{pid}]: username:{user name} usid: {user id} started {context} session from ip:127.0.0.1 source-port:{src port} through {local interface} protocol	LOG_AUTH	Notice	Event	Auth.log

- **SE_LOCAL_UNSUCCESSFUL_LOGON (Invalid Username)**

Event Message	Facility	Severity	Event Type	Log
audit user: {user name}1/0 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

Event Message	Facility	Severity	Event Type	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} usid:{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} usid: {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}	LOG_AUTH	Notice	Event	Auth.log

Event Message	Facility	Severity	Event Type	Log
source-port:{Port} through {Protocol} protocol				

- **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 operating system files have been modified or tampered with. For assistance, contact Siemens Customer Support.	LOG_DAEMON	Critical	Alarm	Syslog

- **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

2 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:

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

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 153).

Mode	Username	Password
Service	root	admin
Maintenance	root	admin
Administrator	admin	admin

2.2 Logging In

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

1. Connect to the device. For more information about the various methods of connecting to the device, refer "Connecting to RUGGEDCOM ROX II " (Page 75).
2. Once a connection is established with the device, press **Enter**. The login prompt appears.

   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 152).

3. Type the user name and press **Enter**. The password prompt appears.

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 25).

⚠ NOTICE

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 166).

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

4. Type the password associated with the username and press **Enter**.

```
login as: admin
admin@127.0.0.1's password:
Welcome to Rugged CLI
admin connected from 127.0.0.1 using console on ruggedcom
ruggedcom#
```

2.3 Logging Out

To log out of the device, type **`exit`** at the root level.

```
ruggedcom#  exit
```

2.4 Using Network Utilities

RUGGEDCOM ROX II features built-in troubleshooting tools for pinging hosts, tracing routes, and analyzing packets.

2.4.1 Pinging an IPv4 Address or Host

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

1. At the command prompt, type:

   ```
   ping { address }
   ```

   Where { address } is the target IPv4 address or host name.

   The results of the ping are displayed. For example:

   ```
   ruggedcom# ping 192.168.0.7
   PING 192.168.0.7 (192.168.0.7) 56(84) bytes of data.
   64 bytes from 192.168.0.7: icmp_seq=1 ttl=60 time=0.639 ms
   64 bytes from 192.168.0.7: icmp_seq=2 ttl=60 time=0.730 ms
   64 bytes from 192.168.0.7: icmp_seq=3 ttl=60 time=0.591 ms
   64 bytes from 192.168.0.7: icmp_seq=4 ttl=60 time=0.596 ms
   ```

2. Press **Ctrl-C** to stop the ping request.

2.4.2 Pinging an IPv6 Address or Host

To ping an IPv6 address or host, type:

- **For Hosts with IPv4 Addresses**

  ```
  ping { address } iface { interface } count { attempts }
  wait { seconds }
  ```

- **For Hosts with IPv6 Addresses**

  ```
  ping6 { address } iface { interface } count { attempts }
  wait { seconds }
  ```

Where:

- { address } is the IP address of the host
- { attempts } is the number of ping attempts
- { interface } is the interface to use
- { seconds } is the maximum number of seconds to for a response from the host

2.4.3 Pinging MPLS Endpoints

To ping an MPLS endpoint, type:

```
mpls-ping { address } { number }
```

Where:

- { address } is the IPv4 address and prefix of the MPLS endpoint
- { number } is the number of ping attempts

2.4.4 Pinging VRF Endpoints

To ping an VRF endpoint, type:

```
vrf-ping address { address } count { attempts } vrfname
{ name }
```

Where:

- { address } is the IPv4 address and prefix of the VRF endpoint
- { attempts } is the number of ping attempts
- { name } is the target VRF

2.4.5 Tracing a Route to an IPv4 Host

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

```
traceroute { host }
```

Where:

- `{ host }` is the name or IP address of the remote host

The results of the trace are displayed. For example:

```
ruggedcom# traceroute 192.168.0.7
traceroute to 192.168.0.7 (192.168.0.7), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 .
 .
 .
```

2.4.6 Tracing a Route to an IPv6 Host

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

```
traceroute6 { address }
```

Where { address } is the name or IP address of the remote host

The results of the trace are displayed. For example:

```
ruggedcom# traceroute6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
traceroute to 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 (2001:0db8:85a3:0000:0000:8a2e:0370:7334), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 .
```

```
.
.
```

2.4.7 Tracing a Route to an MPLS Endpoint

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

```
mpls-traceroute { address }
```

Where { address } is the IPv4 address of the MPLS trace route.

2.4.8 Tracing a Route to a VRF Endpoint

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

```
vrf-traceroute vrfname { name }
```

Where { name } is the VRF endpoint

2.4.9 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, type `tcpdump` and configure the following parameters:

Parameter	Description
`count`	The number of packets to capture
`host`	The host name to be ignored or allowed.
`interface`	The interface from the IP list to dump.
`port`	The ports to trace.
`verbosity`	The verbosity level. Type v, vv or vvv to set the level.
`address`	Displays the source IP for each packet.
`hex`	Converts the data to hexadecimal or ASCII characters.
`linkheader`	Displays the link level header.
`proto`	**Synopsis:** [t | u | i | a | v | g | o | e | h | p | s | n] The protocol or protocols to filter out. Options include: • **t** – Transmission Control Protocol (TCP) • **u** – User Datagram Protocol (UDP) • **i** – Internet Control Message Protocol (ICMP) • **a** – Address Resolution Protocol (ARP) • **v** – Virtual Redunancy Router Protocol (VRRP)

Parameter	Description
	• **g** – Internet Group Management Protocol (IGMP) • **o** – Open Shortest Path First (OSPF) • **e** – Encapsulating Security Payload (ESP) • **h** – Authentication Header (AH) • **p** – Protocol-Independent Multicast (PIM) • **s** – Spanning Tree Protocol (STP) • **n** – Ignores the protocols specified after To select more than one protocol, string the letters together. For example, **tui** will filter out TCP, UDP, and ICMP packets. To ignore a protocol, place **n** before the protocol or protocols that should be ingored. For example, **tui** filters TCP, UDP, and ICMP protocols, but **ntui** filters all protocols except TCP, UDP, and ICMP.

Sample Output

```
ruggedcom# tcpdump address y
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on switch, link-type EN10MB (Ethernet), capture size 262144 bytes
14:41:39.681559 IP 192.168.12.2 > 224.0.0.2: igmp v2 report 224.0.0.2
14:41:40.872170 IP 192.168.23.3 > 224.0.0.13: PIMv2, Hello, length 26
14:41:41.542195 IP 192.168.12.1 > 224.0.0.13: PIMv2, Hello, length 26
14:41:42.342000 IP 192.168.12.1 > 224.0.0.6: igmp v2 report 224.0.0.6
14:41:43.089546 IP 192.168.12.2 > 224.0.0.5: igmp v2 report 224.0.0.5
14:41:45.092975 IP 192.168.12.2 > 224.0.0.13: PIMv2, Hello, length 26
14:41:45.093216 IP 192.168.23.2 > 224.0.0.1: igmp query v2
14:41:45.693560 IP 192.168.23.2 > 224.0.0.13: igmp v2 report 224.0.0.13
14:41:45.808012 IP 192.168.23.3 > 224.0.0.6: igmp v2 report 224.0.0.6
14:41:47.065571 IP 192.168.23.2 > 224.0.0.5: igmp v2 report 224.0.0.5
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

2.4.10 Capturing Packets from a VRF Network Interface

VRF Tcpdump 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, type `vrf-tcpdump` and configure the following parameters:

Parameter	Description
`vrfname`	Displays the source IP for each packet.
`address`	Displays the source IP for each packet.
`count`	The number of packets to capture
`hex`	Converts the data to hexadecimal or ASCII characters.
`host`	The host name to be ignored or allowed.
`interface`	The interface from the IP list to dump.

Parameter	Description
`linkheader`	Displays the link level header.
`port`	The ports to trace.
`proto`	**Synopsis:** [t | u | i | a | v | q | o | e | h] The protocol or protocols to filter out. Options include: • **t** – Transmission Control Protocol (TCP) • **u** – User Datagram Protocol (UDP) • **i** – Internet Control Message Protocol (ICMP) • **a** – Address Resolution Protocol (ARP) • **v** – Virtual Redunancy Router Protocol (VRRP) • **g** – Internet Group Management Protocol (IGMP) • **o** – Open Shortest Path First (OSPF) • **e** – Encapsulating Security Payload (ESP) • **h** – Authentication Header (AH) • **p** – Protocol-Independent Multicast (PIM) • **s** – Spanning Tree Protocol (STP) • **n** – Ignores the protocols specified after To select more than one protocol, string the letters together. For example, **tui** will filter out TCP, UDP, and ICMP packets. To ignore a protocol, place **n** before the protocol or protocols that should be ingored. For example, **tui** filters TCP, UDP, and ICMP protocols, but **ntui** filters all protocols except TCP, UDP, and ICMP.
`verbosity`	The verbosity level. Type v, vv or vvv to set the level.

2.5 Using the Command Line Interface

This section describes how to use Command Line Interface (CLI) for RUGGEDCOM ROX II. It covers common commands, conventions, and useful techniques.

2.5.1 Accessing Different CLI Modes

RUGGEDCOM ROX II provides commands for monitoring and configuring software, hardware and network connectivity. The Command Line Interface (CLI) supports the following modes:

Mode	Description
Operational Mode	Operational mode is the default mode after a user logs in to the device. It allows users to perform general device management actions and provides troubleshooting and maintenance utilities. It is used for viewing the system status, controlling the CLI environment, monitoring and troubleshooting network connectivity, and launching the Configuration mode.
Configuration Mode	Configuration mode is launched from the Operational Mode. It allows users to change the actual configuration of the device.

Mode	Description
	All changes to the configuration are made on a copy of the active configuration, called the candidate configuration. Changes do not take effect until they are committed.

In both modes, the CLI prompt indicates the current mode. In Operational mode, the prompt is:

```
ruggedcom#
```

In Configuration mode, the prompt is:

```
ruggedcom(config)#
```

As a user navigates through the configuration data hierarchy, the prompt indicates the user's location in the configuration. For example, after navigating to ***interface » eth » lm3 » 1***, the CLI prompt will be:

```
ruggedcom(config-eth-lm3/1)#
```

2.5.2 Using Command Line Completion

Commands and parameters do not need to be entered completely for the CLI to recognize them. By typing the first few letters of a command and pressing **Tab**, the CLI will display the possible completions. If the first few letters are unique to a specific command, the full command is automatically displayed. If the first few letters match more than one possible command, a lit of possible completions appears.

Note

Automatic completion is disabled inside quotation marks. If the name of a command or parameter contains a space, such as a filename, escape the space with a \ or enclose the string in quotation marks. For example:

```
who file foo\ bar
```

or

```
who file "foo bar"
```

Note

Auto-completion also applies to filenames and directories, but cannot be initiated using a space. Auto-completion using a space is disabled when typing a filename or directory name.

2.5.3 Displaying Available Commands

To display a list of available commands at any point in the CLI, type `?`.

For example, in Operational mode, typing ? at the command prompt displays a list of all Operational mode commands:

```
ruggedcom# ?
Possible completions:
  admin               Configures the general device characteristics
  autowizard       Automatically query for mandatory elements
  clear                 Clear parameter
  commit             Confirm a pending commit
  .
  .
  .
  traceserial        Trace serial ports activities
  who                  Display currently logged on users
  write                 Write configuration
ruggedcom#
```

2.5.4 Editing Commands

The following commands can be used to edit command lines and move around the command history.

Moving the Cursor

Command	Description
Ctrl-B or **Left Arrow**	Moves the cursor back one character
Ctrl-F or **Right Arrow**	Moves the cursor forward one character
Esc-B or **Alt-B**	Moves the cursor back one word
Esc-F or **Alt-F**	Moves the cursor forward one word
Ctrl-A or **Home**	Moves the cursor to the beginning of the command line
Ctrl-E or **End**	Moves the cursor to the end of the command line

Deleting Characters

Command	Description
Ctrl-H, **Delete** or **Backspace**	Delete the character before the cursor
Ctrl-D	Delete the character after the cursor
Ctrl-K	Delete all characters from the cursor to the end of the line
Ctrl-U or **Ctrl-X**	Delete the whole line
Ctrl-W, **Esc-Backspace** or **Alt-Backspace**	Delete the whole before the cursor
Esc-D or **Alt-D**	Delete the whole after the cursor

Inserting Recently Deleted Text

Command	Description
Ctrl-Y	Inserts the most recently deleted text at the cursor's location

Displaying Previously Entered Commands

Command	Description
Ctrl-P or **Up Arrow**	Shows the previous command in the command history
Ctrl-N or **Down Arrow**	Shows the next command in the command history
Ctrl-R	Reverses the order of commands in the command history
`show history`	shows a list of previous commands

Capitalization

Command	Description
Esc-C	Capitalizes the first letter of the word at the cursor's location and sets all other characters to lowercase
Esc-L	Changes the entire word at the cursor's location to lowercase
Esc-U	Changes the entire word at the cursor's location to uppercase

Special Actions

Command	Description
Ctrl-C	Aborts a command or clears the command line
Ctrl-V or **Esc-Q**	Treats the next character(s) as character data, not a command
Ctrl-L	Redraws the screen
Ctrl-T	Transposes characters
Esc-M	Enters multi-line mode
Ctrl-D	Exits multi-line mode
Ctrl-Z	Exits configuration mode

Inserting Hard Returns

Command	Description
Esc-M	Inserts a hard return

2.5.5 Using Double Quotes

When the value for a parameter contains spaces, unless otherwise stated, wrap the value in double-quotes ("").

For example:

```
admin scheduler scheduled-jobs save-myconfig job-command
"show running-config | save myconfig"
```

2.5.6 Using Output Redirects

Information returned from a CLI term can be processed in various ways using an output redirect term. To specify an output redirect, type | after the CLI term and then type the redirect term. To display the available redirects, type | ? after a CLI term. For example:

```
 show admin | ?
Possible completions
  append        Append output text to a file
  begin         Begin with the line that matches
  best-effort   Display data even if data provider is unavailable or continue
                loading from file in presence of failures
  count         Count the number of lines in the output
  csv           Show table output in CSV format
  de-select     De-select columns
  display       Display options
  exclude       Exclude lines that match
  include       Include lines that match
  linnum        Enumerate lines in the output
  match-all     All selected filters must match
  match-any     At least one filter must match
  more          Paginate output
  nomore        Suppress pagination
  notab         Suppress table output
  repeat        Repeat show command with a given interval
  save          Save output text to a file
  select        Select additional columns
  sort-by       Select sorting indices
  tab           Enforce table output
  until         End with the line that matches
```

Command	Description

append	Appends the output text to a specified ASCII text file.
	For example, running these two terms appends the admin and chassis information to the specified file:
	`ruggedcom# show admin | append foo.txt`
	`ruggedcom# show interface | append foo.txt`
	The resulting file contains the results of `show interface` appended to the results of `show admin` (lines truncated with ... are shortened for illustrative purposes only):
	`ruggedcom# file show-config foo.txt`
	`admin`
	` time`
	`  gmtime  "Wed Oct 22 20:05:50 2014"`

Command	Description
	localtime "Wed Oct 22 16:05:50 2014" rox-imaging roxflash-progress phase Inactive status message "" image flashing 0 netconf statistics in bad hellos 0 in sessions 0 dropped sessions 0 in rpcs 0 in bad rpcs 0 out rpc errors 0 out notifications 0 alarms active-alarms chassis 11 1 severity notice description "Line Module with serial number L15R-1710-PR002 in slot lm4 is inserted or up"

`begin`	Begins the output with the line containing the specified text. Regular expressions can be used with this redirect. For more information about regular expressions, refer to "Using Regular Expressions" (Page 42).
	For example, `show admin | begin netconf` returns all of the **admin** information following the `netconf` line:
	`ruggedcom# show admin | begin netconf`
	`netconf`
	`statistics`
	`in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in bad rpcs 0 in not...`

`best-effort`	Displays data even if the data provider is unavailable, or continues loading from file in presence of failures.
	For example, `show chassis line-modules line-module | best-effort` shows the line module status in the chassis, including slots with no line module detected.
	`show chassis line-modules line-module | best-effort`
	`BYPASS OVERCURRENT`
	`SLOT DETECTED MODULE STATUS STATUS`
	`lm1 none - -`
	`lm2 none - -`
	`lm3 none - -`
	`lm4 1x Cell LTE NAM V/S - -`
	`lm5 none - -`
	`lm6 1x Cell LTE APAC - -`

Command	Description

`csv`	Shows table output in CSV (Comma-Separated-Values) format.
	For example, `show admin alarms | csv` shows the **alarms** information in CSV format.
	`show admin alarms | csv`
	`,ALARM,EVENT,,,,,`
	`SUBSYSTEM,ID,ID,SEVERITY,DESCRIP`
	`TION,DATE TIME,USER ACTIONS,ACTUA`
	`TORS`
	`switch,1,1,notice,Link-up on port`
	` swport/1,Sat Mar  2 15:34:34`
	` 2019,clear-or-ack,none`

`de-select`	De-selects columns from table entries.
	For example, `show chassis line-modules line-module | de-select bypass` removes the BYPASS column from the display.
	`show chassis line-modules line-mod`
	`ule`
	
	`              BYPASS  OVERCURRENT`
	`SLOT  DETECTED MODULE`
	`               STATUS  STATUS`
	`---------------------------------------`
	`lm1   1000TX w/ 2x RJ45`
	`              -       -`
	`lm2   T1/E1 w/ 2x RJ48`
	`              -       -`
	`lm3   6x RS232/RS422/RS485 via RJ45`
	`              -       -`
	`lm4   E1 w/ 2x BNC`
	`              -       -`
	`lm5   6x 100FX SFP Blank (no optical`
	` transceiver)  -       -`
	`lm6   none`
	`              -       -`
	`show chassis line-modules line-mod`
	`ule | de-select bypass`
	`SLOT  DETECTED MODULE`
	`---------------------------------------`
	`lm1   1000TX w/ 2x RJ45`
	`lm2   T1/E1 w/ 2x RJ48`
	`lm3   6x RS232/RS422/RS485 via RJ45`
	`lm4   E1 w/ 2x BNC`
	`lm5   6x 100FX SFP Blank (no optical`
	` transceiver)`
	`lm6   none`

`display`	Provides displays options.
	For example, `show admin alarms | display xml` shows the **alarms** information in extensible markup language format.
	`& show admin alarms | display xml`
	`<config xmlns="http://tail-f.com/ns/`
	`config/1.0">`
	`  <admin xmlns="http://rugged`
	`com.com/ns/rmf_admin">`
	`  <alarms>`
	`    <active-alarms>`
	`      <subsystem>switch</subsystem>`

Command	Description
	<alarm-id>1</alarm-id> <event-id>1</event-id> <severity>notice</severity> <description>Link-up on port swport/1</description> <date-time>Sat Mar 2 15:34:34 2019</date-time> <user-actions>clear-or-ack</user-actions> <actuators>none</actuators> </active-alarms> </alarms> </admin> </config>

`exclude`	Excludes lines containing the specified text. Information that is a *child* of the excluded line is also excluded. Regular expressions can be used with this redirect. For more information about regular expressions, refer to "Using Regular Expressions" (Page 42).
	For example, `show admin | exclude netconf` shows the **admin** information, excluding the `netconf` lines.
	`ruggedcom# show admin | exclude net conf`
	`admin`
	` time`
	`  gmtime "Tue Feb 15 08:25:27 2011\n" localtime "Tue Feb 15 03:25:27 2011\n"`
	` software-upgrade`
	`  upgrade-progress`
	`   software partition "Partition #1" current version "ROX 2.1.0 (2010-12-03 17:38) ...`
	`  statistics`
	`   in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in bad rpcs 0 in not...`
	`    supported rpcs 0 out rpc replies 0 out rpc errors 0 out notifica tions 0`

`include`	Includes lines containing the specified text. Information that is a *child* of the included line is usually included, but may not be in some cases. Regular expressions can be used with this redirect. For more information about regular expressions, refer to "Using Regular Expressions" (Page 42).
	For example, `show admin | include time` shows the `time` lines from the **admin** information.
	`ruggedcom# show admin | include time`
	` time`
	`  gmtime "Tue Feb 15 08:34:55 2011\n" localtime "Tue Feb 15 03:34:55 2011\n"`

Command	Description
	`ruggedcom#`

`linnum`	Numbers the lines in the output. For example:
	`ruggedcom# show admin | linnum`
	`1: admin`
	`2:  time`
	`3:   gmtime "Tue Feb 15 08:37:42 2011\n" localtime "Tue Feb 15 03:37:42 2011\n"`
	`4:  software-upgrade`
	`.`
	`.`
	`.`

`match-all`	All selected filters must match.
	For example, `show running-config | include interface | match-all` adds a filter to show all available interfaces.
	`show running-config | include interface | match-all`
	`  partname "(MX)Rack Rear Mount, No interfaces/LEDs on Front Panel"`
	`  partname "Rack Rear Mount, No interfaces/LEDs on Front Panel"`
	`interface`
	`interface-mpls cel-6-1`
	`interface-mpls fe-cm-1`
	`  interface-ldp cel-6-1`
	`  interface-ldp fe-cm-1`
	`interface cel-6-1`
	`interface fe-cm-1`
	`interface cel-6-1`
	`interface fe-cm-1`
	`interface cel-6-1`
	`interface fe-cm-1`
	`interface cel-6-1`
	`interface dummy0`
	`interface fe-cm-1`

`match-any`	At least one filter must match.
`more`	Paginates the output. When the output reaches the screen-length setting, the CLI prompts you to press a key for more. Press **Enter** to advance line-by-line; press **space** to advance page-by-page.
`nomore`	Suppresses pagination.

`notab`	Suppresses table output.
	For example, `show chassis | begin line-modules` shows the following table:
	`ruggedcom# show chassis | begin line-modules`
	`line-modules`
	`line-module`
	`BYPASS  OVERCURRENT`
	`SLOT  DETECTED MODULE`
	`STATUS  STATUS`
	`----------`
	`lm1  1000TX w/ 2x RJ45`
	`-  -`

Command	Description

	`lm2 none`
	`- -`
	`lm3 6x RS232/RS422/RS485 via RJ45`
	`- -`
	`lm4 E1 w/ 2x BNC`
	`- -`
	`lm5 none`
	`- -`
	`lm6 none`
	`- -`
	
	`power-controller`
	`PM MOV PM PM`
	`PM`
	`SLOT PROTECTION TEMPERATURE CUR`
	`RENT VOLTAGE`
	`----------`
	`pm1 na 43 2907`
	`3381`
	
	For example, `show chassis | begin line-modules | notab` suppresses the table formatting:
	
	`ruggedcom# show chassis | begin`
	`line-modules | notab`
	`line-modules`
	`line-module lm1`
	`detected module "1000TX w/ 2x`
	`RJ45"`
	`line-module lm2`
	`detected module none`
	`line-module lm3`
	`detected module "6x RS232/RS422/`
	`RS485 via RJ45"`
	`line-module lm4`
	`detected module "E1 w/ 2x BNC"`
	`line-module lm5`
	`detected module none`
	`line-module lm6`
	`detected module none`
	`power-controller`
	`PM MOV PM PM`
	`PM`
	`SLOT PROTECTION TEMPERATURE CUR`
	`RENT VOLTAGE`
	`----------`
	`pm1 na 43 2892`
	`3381`

`repeat`	Repeats the term at the specified interval. Specify an interval in seconds. The term repeats until you cancel it with **Ctrl-C**. For example, `show admin | repeat 10s` repeats the `show admin` term every 10 seconds.
`save`	Saves the output to the specified ASCII text file. For example, `show chassis | save foo.txt` saves the **chassis** information to the file `foo.txt`
`select`	Only the specified parameter is shown in in table entries.

Command	Description

	For example, `show chassis line-modules line-module | select detected-module` displays the DETECTED MODULE column.
	`show chassis line-modules line-module | select detected-module`
	`SLOT  DETECTED MODULE`
	`--------------------------`
	`lm1   none`
	`lm2   none`
	`lm3   none`
	`lm4   1x Cell LTE NAM V/S`
	`lm5   none`
	`lm6   1x Cell LTE APAC`

`sort-by`	Sorts the output according to the specified parameter.
	For example, `show chassis line-modules line-module | sort-by detected-module` sorts the output per the DETECTED MODULE column.
	`show chassis line-modules line-module | sort-by detected-module`
	`BYPASS  OVERCURRENT`
	`SLOT  DETECTED MODULE  STATUS  STATUS`
	`----------`
	`celport  1x Cell LTE NAM A/R/B/T  -  -`
	`wlanport  1x WLAN 802.11  -  -`
	`serport  2xRS232/422/485  -  -`
	`swport  SM M88E6097F, 4FT 2GP  -  -`

`tab`	Enforces table layout for columnar data.

`until`	Includes output until a line containing the specified text appears. Regular expressions can be used with this redirect. For more information about regular expressions, refer to "Using Regular Expressions" (Page 42).
	For example, `show chassis | begin cpu | until status` returns the **chassis** information beginning with `cpu` and ending with `status`:
	`ruggedcom# show chassis | begin cpu | until status`
	`cpu`
	`slot-cpu main`
	`detected module "RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots"`
	`cpu load  22`
	`ram avail  53`
	`ram avail low  20`
	`status`

2.5.7 Using Regular Expressions

RUGGEDCOM ROX II command line regular expressions are a subset of the regular expressions found in egrep and in the AWK programming language. Regular expressions can be used along with several of the output redirects. For more information about using output redirects, refer to "Using Output Redirects" (Page 35).

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: • Each space ( ) and comma (,) • Each AS set delimiter (e.g. *{* and *}*) • Each AS confederation delimiter (e.g. *(* and *)*) • The beginning and end of the line Therefore, the underscore can be used to match AS values.	_100,100_, _100_

For example, to show all the IP interfaces that are in the *up* state:

```
ruggedcom# show interfaces ip | include up
 admin state up
 state       up
 admin state up
 state       up
 admin state up
 state       up
 admin state up
 admin state up
 admin state up
 admin state up
 admin state up
```

2.5.8 Using CLI Utilities

The Operational mode provides a set of standard utility applications, similar to those on a typical Linux-based operating system.

Command	Description
`ssh host { address/name } { bind-address { address } | cipher-spec { cipher } | kex-spec { kex } | mac-`	Opens a secure shell on another host. Parameters include:

Command	Description
`spec { mac } | key-spec { hostkey } | login { name } | port { number } | sub-system { name } }`	• `host` is the name or IP address of the host. It is mandatory. • `bind-address` is the source address of the connection. Only useful on systems with more than one address. • `cipher-spec` is a comma-separated list of the encryption algorithms to support for encrypting the session. To see which algorithms are available, use the `list-ciphers` parameter. Supported algorithms are also listed in "Supported Cipher Suites" (Page 1054). If no algorithms are specified, default algorithms (grade 4 or higher) will be used automatically. • `kex-spec` is a comma-separated list of the key exchange algorithms to support for encrypting the session. To see which algorithms are available, use the `list-kexes` parameter. Supported algorithms are also listed in "Supported Cipher Suites" (Page 1054). If no algorithms are specified, default algorithms (grade 4 or higher) will be used automatically. • `mac-spec` is a comma-separated list of the MAC algorithms to support for encrypting the session. To see which algorithms are available, use the `list-macs` parameter. Supported algorithms are also listed in "Supported Cipher Suites" (Page 1054). If no algorithms are specified, default algorithms (grade 4 or higher) will be used automatically. • `key-spec` is a comma-separated list of the server host key algorithms to support for encrypting the session. To see which algorithms are available, use the `list-keys` parameter. Supported algorithms are also listed in "Supported Cipher Suites" (Page 1054). If no algorithms are specified, default algorithms (grade 4 or higher) will be used automatically. • `login` is the users login name on the host. • `port` is the TCP port number to open an SSH session to. • `sub-system` invokes a subsystem on the remote system, such as NETCONF.
`ssh { list-ciphers | list-kexes | list-keys | list-macs }`	Lists information about available algorithms. Parameters include: • `list-ciphers` is the list of supported encryption algorithms.

Command	Description
	• `list-kexes` is the list of supported key exchange algorithms. • `list-keys` is the list of supported server host key algorithms. • `list-macs` is the list of supported MAC algorithms.
`telnet host { address/name }`	Opens a telnet session to another host. Parameters include: • `{ host }` is the name or IP address of the host

Further information about these well-known applications is publicly available on the Internet.

2.5.9 Specifying a Range

Some CLI commands accept a range of values, such as LM1-3 or 3-6, to specify multiple targets. In the following example, a command is applied to port 1 on LM1, LM2 and LM3:

```
ruggedcom(config)# interface switch lm1-3 1
```

In this example, a command is issued to ports 1, 2 and 4 on LM1, LM2 and LM4:

```
ruggedcom(config)# interface switch lm1-2,4 1-2,4
```

When available, the `range` parameter can be included before the value range:

```
ruggedcom(config)# interface switch range lm1-3 1-6
```

2.5.10 Common Commands

This section details common commands available in operational and configuration mode.

2.5.10.1 Basic CLI Commands

Use the following commands to perform basic CLI functions.

Command	Description
`exit [ level | configuration-mode | no-confirm ]`	**Default:** level Exits from the current mode. • `level` exits from the current mode. If performed at the top level, this command exits from the configuration mode. • `configuration-mode` exits from configuration mode regardless of mode.

Command	Description
	• `no-confirm` exits from configuration mode without prompting the user to commit any pending changes.
`help { command }`	Displays help text for the specified command.

`id`	Displays the current user's information. For example:
	`ruggedcom# id`
	` user = admin(0), gid=0, groups=admin, gids=`

`logout [ logout | sessionid ]`	Terminates the specified session. A session can be specified based on its user ID or session ID.
`quit`	Logs out of and ends the CLI session.

`send [ all | admin ] { message }`	Sends a message to all users of the specified type. For example:
	`ruggedcom# send all "Rebooting at midnight!"Message from admin@ruggedcom at 2011-02-15 08:42:49...`
	`Rebooting at midnight!`
	`EOF`

`show [ admin | chassis | interface | interfaces | netconf | routing | services ]`	Shows selected configuration information. Use auto completion to display the list of options available at each configuration level. For example:
	`ruggedcom# show chassis hardware slot-hardware ORDER`
	`SLOT FIELD DETECTED MODULE SERIAL NUMBER`
	`---`
	`pm1 48 48VDC (36-59VDC) Power Supply`
	`lm1 XX none none`
	`lm2 M1_ Old V90 Modem`
	`lm3 TX01 2x 10/100Tx RJ45`
	`lm4 TX01 2x 10/100Tx RJ45`
	`lm5 DS3 1x T3/E3`
	`lm6 TC2 2x Chan T1/E1`
	`pm2 XX none none`
	`main CM01 RX1000 Main Board RX1K-12-11-0015`

`show [ cli | history | jobs | log | { logfile } ]`	Shows selected system information.
	• `cli` shows the CLI environment settings. For example:
	`ruggedcom# show cli`
	`autowizard true`
	`complete-on-space true`

Command	Description
| | ```
display-level         99999999
history               100
ignore-leading-space  true
output-file           terminal
paginate              true
screen-length         65
screen-width          237
service prompt config true
show-defaults         false
terminal              xterm
```<br>• `history` displays the CLI command history.<br>• `jobs` displays currently running background jobs. For example:<br>```<br>ruggedcom# show jobs<br>JOB COMMAND<br>2   monitor start /tmp/saved<br>```<br>• `log` and `logfile` display the selected log file. Use auto completion to view a list of available log files. |
| `show parser dump { command }` | Displays all possible commands starting with the specified command. |
| `show running-config { option }` | Displays the current configuration. If an `{ option }` parameter is not specified, the entire configuration will be displayed by default . Use auto completion to see a list of configuration options. Use \| and one or more output redirects to restrict the information to be shown. |

2.5.10.2 File Commands

Operational mode provides commands for managing log, configuration and feature key files on the device.

Note

Secure Copy Protocol (SCP) commands, such as `file scp-log-to-url`, require a user name, host name, or file path in the form of:

`{ user }@{ host }:{ path }`

Specific rules apply.

User Names

- May only contain alphabetic characters, numeric characters, underscores (_), and dashes (-)
- Must start and end with an alphabetic or numeric character

Host Names

- May be a valid host name or IP address
- Host names may only contain alphabetic characters, numeric characters, dashes (-), and periods (.)
```

- IP address must be valid IPv4 addresses of the format AAA.BBB.CCC.DDD

File Paths

- May only contain alphabetic characters, numeric characters, forward slashes (/), dashes (-), periods (.), underscores (_), astericks (*), plus signs (+), and tildes (~)

Command	Description

`file compare-config { filename1 } { filename2 }`	Compares the contents of two files. A **<** character indicates text that is present in the first selected file but not in the second file. A **>** character indicates text that is present in the second selected file but not in the first file. In the following example, the user information is present in the second file, but not in the first:
	`ruggedcom# file compare deleted_users all_users`
	`125,127d124`
	`<  userid jsmith`
	`<   password $1$N1YT8Azl$KcG1E6/r91EXc4mgEEsAW. role administrator`
	`<  !`

`file copy-config { current-filename } { new-filename }`	Copies a configuration file. After typing the command, press **Tab** to view a list of available files. For example, the following command copies the **deleted_users** file to the **archive001** file: `ruggedcom# file copy-config deleted_users archive001`

`file copy-config-from-removable { path } [ { config-filename } | force | no-force ]`	Copies a config file from the removable drive to the **var/lib/config** directory. After typing the command, press **Tab** to view a list of available files.
	Options include:
	• `{ path }` is the path to the removable drive/configuration file.
	For example, the following command copies the **lnx2** file:
	`ruggedcom# file copy-config-from-removable usb://usb-cm-4/lnx2`
	Additional options include:
	• `{ config-filename }` is the desired new filename of the configuration file to be copied. To use the current filename, specify the current filename or exclude this parameter from the command.
	For example, the following command copies and renames the **lnx2** file to **lnx3**:
	`ruggedcom# file copy-config-from-removable usb://usb-cm-4/lnx2/lnx3`

Command	Description
	• `force`/ `no force` allows the overwriting of a configuration with the same name that may exist in the **var/lib/config** directory. Excluding this parameter defaults to `no force`, meaning the existing file will not be overwritten. For example, the following command copies and overwrites the existing **lnx2** file in the **var/lib/config** directory: `ruggedcom# file copy-config-from-removable usb://usb-cm-4/lnx2 force`

`file copy-config-to-removable { config-filename } { path } [ force | no-force ]`	Copies a config file from the **var/lib/config** directory to the removable drive. After typing the command, press **Tab** to view a list of available files.
	Options include:
	• `{ config-filename }` is name of the configuration file to be copied.
	• `{ path }` is the path to the removable drive.
	For example, the following command copies the **nextgen** file:
	`file copy-config-to-removable nextgen usb://usb-cm-6/nextgen`
	Redefining the path allows renaming the configuration file on the removable drive. For example, the following command copies the **nextgen** file from the **var/lib/config** directory and renames it **nextgen2** on the removable drive:
	`file copy-config-to-removable nextgen usb://usb-cm-6/nextgen2`
	Additional options include:
	• `force`/ `no force` allows the overwriting of a configuration with the same name that may exist on the removable drive. Excluding this parameter defaults to `no force`, meaning the existing file will not be overwritten.
	For example, the following command copies and overwrites the existing **nextgen** file in the removeable drive:
	`ruggedcom# file copy-config-to-removable nextgen usb://usb-cm-6/nextgen force`

`file copy-from-remote-to-removable { source-path } { removable-drive-path } [ force | no-force ]`	Copies a file from a remote host to the removable drive. After typing the command, press **Tab** to view a list of available files. Options include:

Command	Description

	• `{ source-path }` is the path to the source file, either a remote PC or other host.
	• `{ removable-drive-path }` is the path to the removable drive.
	For example, the following command copies the **nextgen** file:
	`ruggedcom# file copy-from-remote-to-removable ftp://username:password@172.30.142.230/nextgen usb://usb-cm-6/nextgen`
	Redefining the path allows renaming the configuration file on the removable drive. For example, the following command copies the **nextgen** file from the remote host and renames it **nextgen2** on the removable drive:
	`ruggedcom# file copy-from-remote-to-removable ftp://username:password@172.30.142.230/nextgen usb://usb-cm-6/nextgen2`
	Additional options include:
	• `force`/ `no force` allows the overwriting of a configuration with the same name that may exist on the removable drive. Excluding this parameter defaults to `no force`, meaning the existing file will not be overwritten.
	For example, the following command copies and overwrites the existing **nextgen** file in the removable drive:
	`ruggedcom# file copy-from-remote-to-removable ftp://username:password@172.30.142.230/nextgen usb://usb-cm-6/nextgen force`

`file copy-from-removable-to-remote { removable-drive-path } { target-path }`	**Note** Remote web servers must support **HTTP PUT** requests to accept files from the removable drive. Copies a file from the removable drive to a remote host. After typing the command, press **Tab** to view a list of available files. Options include: • `{ removable-drive-path }` is the path to the removable drive. • `{ target-path }` is the path to the target, either a remote PC or other host. For example, the following command copies the **nextgen** file: `ruggedcom# file copy-from-removable-to-remote usb://usb-cm-6/`

Command	Description

	`nextgen ftp://username:pass word@172.30.142.230/nextgen`
	
	Redefining the path allows renaming the configuration file on the removable drive. For example, the following command copies the **nextgen** file from the remote host and renames it **nextgen2** on the removable drive:
	
	`ruggedcom# file copy-from-remov able-to-remote usb://usb-cm-6/ nextgen ftp://username:pass word@172.30.142.230/nextgen2`

`file create-directory-on-removable { removable-drive-path }`	Creates a directory on the removable drive. Options include: • `{ removable-drive-path }` is the path/name of the new directory on the removable drive. For example, the following command creates the **lnx10** directory: `ruggedcom# file create-directory-on-removable usb://usb-cm-4/lnx10`
`file delete-config { filename }`	Deletes a configuration file. After typing the command, press **Tab** to view a list of available files. For example, the following command deletes the **deleted_users** file: `ruggedcom# file delete-config delet ed_users`
`file delete-featurekey { filename }`	Deletes a feature key file. After typing the command, press **Tab** to view a list of available files. For example, the following command deletes the feature key **1_cmRX1K-12-11-0217.key** file: `ruggedcom# file delete-featurekey 1_cmRX1K-12-11-0217.key`
`file delete-from-removable { removable-drive-path } [ force | no-force ]`	Deletes a directory from the removable drive. Options include: • `{ removable-drive-path }` is the path/name of the directory to be deleted from the removable drive. For example, the following command deletes the **lnx6** directory: `ruggedcom# file delete-from-removable usb://usb-cm-6/lnx6` Additional options include: • `force`/ `no force` allows the deletion of a directory containing files. Excluding this parameter defaults to `no force`, meaning a directory containing files cannot be deleted.

Command	Description
	For example, the following command deletes the **lnx6** directory, containing files, from the removable drive: `ruggedcom# file delete-from-removable usb://usb-cm-6/lnx6 force`
`file list-config`	Lists the configuration files. For example: `ruggedcom# file list-config --help 10.200.20.39 _tmp_confd_cmd.0 archive001 archive002 default_rx1000_config`
`file list-featurekey`	Lists the feature key files. For example: `ruggedcom# file list-featurekey 1_cmRX1K-12-11-0015.key`

`file list-removable-directory { removable-drive-path } [ size | no-size ]`	Lists directory contents on the removable drive.
	Options include:
	• `{ removable-drive-path }` is the path/name of the directory to be listed.
	For example, the following command lists the contents of the **usb-cm-6** directory:
	`ruggedcom# file list-removable-directory usb://usb-cm-6/`
	Note
	The forward slash (/) is used to display the contents of the parent directory. To display the contents of a subdirectory, specify the full path.
	Additional options include:
	• `size`/`no size` allows the display of each file size in the listing. Excluding this parameter defaults to `size`, meaning file sizes will be displayed.
	For example, the following command lists files in the **usb-cm-6** directory, including the size of each file:
	`ruggedcom# file list-removable-directory usb://usb-cm-6/ size`

`file rename-config { current-filename } { new-filename }`	Renames a configuration file. For example, the following command renames the **test002** file to **production_config**: `ruggedcom# file rename-config test002 production_config`
`file rename-on-removable { current-name-path } { new-name-path }`	Renames a file or directory on the removable drive. For example, the following command renames the **test001.txt** file in the **usb-cm-6** directory to **test002.txt**:

Command	Description
	`ruggedcom# file list-removable-di rectory usb://usb-cm-6/test001.txt test002.txt`
`file rename-config { current-file name } { new-filename }`	Renames a feature key file. For example, the following command renames the feature key **1_cmRX1K-12-11-0217.key** file to **old_featurekey**: `ruggedcom# file rename-featurekey 1_cmRX1K-12-11-0217.key old_fea turekey`

`file scp-config-from-url { user }@{ host }:/{ path }/{ cur rent-filename } { new-filename }`	Securely copies a configuration file from a remote computer to the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.
	To use this command, the user credentials for the remote computer, the IP address or host name of the remote computer, the directory path to the configuration file on the remote computer, and the configuration file filename must all be known.
	Type the command in the following format:
	`file scp-config-from-url { user }@{ host }:/{ path }/{ cur rent-filename } { new-filename }`
	Where:
	• `{ user }` is a user name with access rights to the remote computer.
	• `{ host }` is the host name or IP address of the remote computer.
	• `{ path }` path is the path to the configuration file on the remote computer.
	• `{ current-filename }` is the current filename of the configuration file.
	• `{ new-filename }` is the new filename for the configuration file. To use the current filename, specify the current filename or exclude this parameter from the command.
	When prompted, type the password to connect to the remote computer. For example:
	`ruggedcom# file scp-config-from-url jsmith@10.200.20.39:/c:/rugged com/standard_config standard_config jsmith@10.200.20.39's password: standard_config.txt 100% 7673 7.5KB/s 00:00`

`file scp-config-to-url { cur rent-filename } { user }@{ host }:/ { path }/{ new-filename }`	Securely copies a configuration file from the device to a remote computer. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.

Command	Description

	To use this command, the user credentials for the remote computer, the IP address or host name of the remote computer, the directory path to the configuration file on the remote computer, and the configuration file filename must all be known.
	Type the command in the following format:
	`file scp-config-to-url { current-filename } { user }@{ host }:/{ path }/{ new-filename }`
	Where:
	• `{ current-filename }` is the current filename of the configuration file.
	• `{ user }` is a user name with access rights to the remote computer.
	• `{ host }` is the host name or IP address of the remote computer.
	• `{ path }` path specifies where to save the configuration file on the remote computer.
	• `{ new-filename }` is the new filename for the configuration file. To use the current filename, specify the current filename or exclude this parameter from the command.
	When prompted, type the password to connect to the remote computer. For example:
	`ruggedcom# file scp-config-to-url default_config jsmith@10.200.20.39:/c:/ruggedcom/default_config`
	`jsmith@10.200.20.39's password:`
	`standard_config.txt 100% 7673 7.5KB/s 00:00`

`file scp-featurekey-from-url { user }@{ host }:/{ path }/{ current-filename } { new-filename }`	Securely copies a feature key file from a remote computer to the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running. To use this command, the user credentials for the remote computer, the IP address or host name of the remote computer, the directory path to the feature key file on the remote computer, and the feature key file filename must all be known. Type the command in the following format: `file scp-featurekey-from-url { current-filename } { user }@{ host }:/{ path }/{ new-filename }` Where: • `{ user }` is a user name with access rights to the remote computer. • `{ host }` is the host name or IP address of the remote computer.

Command	Description

	• `{ path }` path is the path to the feature key file on the remote computer.
	• `{ current-filename }` is the current filename of the feature key file.
	• `{ new-filename }` is the new filename for the feature key file. To use the current filename, specify the current filename or exclude this parameter from the command.
	When prompted, type the password to connect to the remote computer. For example:
	`ruggedcom# file scp-featurekey-from-url jsmith@10.200.20.39:/c:/ruggedcom/1_cmRX1K-12-11-0015.key 1_cmRX1K-12-11-0015.key`
	`jsmith@10.200.20.39's password:`
	`1_cmRX1K-12-11-0015.key 100% 192 0.2KB/s 00:00`

`file scp-featurekey-to-url { current-filename } { user }@{ host }:/{ path }/{ new-filename }`	Securely copies a feature key file to a remote computer from the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.
	To use this command, the user credentials for the remote computer, the IP address or host name of the remote computer, the directory path to the feature key file on the remote computer, and the feature key file filename must all be known.
	Type the command in the following format:
	`file scp-featurekey-to-url { current-filename } { user }@{ host }:/{ path }/{ new-filename }`
	Where:
	• `{ current-filename }` is the current filename of the feature key file.
	• `{ user }` is a user name with access rights to the remote computer.
	• `{ host }` is the host name or IP address of the remote computer.
	• `{ path }` path specifies where to save the feature key file on the remote computer.
	• `{ new-filename }` is the new filename for the feature key file. To use the current filename, specify the current filename or exclude this parameter from the command.
	When prompted, type the password to connect to the remote computer. For example:
	`ruggedcom# file scp-featurekey-to-url 1_cmRX1K-12-11-0015.key jsmith@10.200.20.39:/c:/ruggedcom/1_cmRX1K-12-11-0015.key`
	`jsmith@10.200.20.39's password:`

Command	Description
	`1_cmRX1K-12-11-0015.key 100% 192 0.2KB/s 00:00`
`file scp-log-to-url { current-file name } { user }@{ host }:/{ path }/ { new-filename }`	Securely copies a log file to a remote computer from the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running. To use this command, the user credentials for the remote computer, the IP address or host name of the remote computer, the directory path to the log file on the remote computer, and the log file filename must all be known. Where: • `{ current-filename }` is the current filename of the log file. • `{ user }` is a user name with access rights to the remote computer. • `{ host }` is the host name or IP address of the remote computer. • `{ path }` path specifies where to save the log file on the remote computer. • `{ new-filename }` is the new filename for the log file. To use the current filename, specify the current filename or exclude this parameter from the command. When prompted, type the password to connect to the remote computer. For example: `ruggedcom# file scp-log-to-url sys log.1 jsmith@10.200.20.39:/c:/ ruggedcom/syslog.1 jsmith@10.200.20.39's password: syslog.1 100% 12KB 12.4KB/s 00:00`
`file show-config { filename }`	Displays the content of a specified file. Use auto completion to display a list of available files. For example: `ruggedcom# file show-config added_users.txt admin system-name "System Name" lo cation Location contact Contact admin hostname name ruggedcom domain localdomain admin session-limits max-sessions 50 . . .`
`file show-featurekey { filename }`	Displays the content of a specified feature key file. Use auto completion to display a list of available feature key files. For example: `ruggedcom# file show-featurekey 1_cmRX1K-12-11-0015.key GPG_FEATUREKEY_LEVEL=1`

Command	Description
	GPG_FEATUREKEY_CM_SERIALNUM BER=RX1K-12-11-0015 GPG_FEATUREKEY_SIGNATURE=iEYE ABECAAYFAk091pAACgkQP 2pya+G5kdZeKACeKd HUB2G1T73Dymq8IjSdYDKAiskAn3abBp CEhfLXxY2ZlVbvGNwDZow2

2.5.10.3 Interface and Services Commands

Operational mode provides commands for restarting and displaying information for various interfaces and services.

Command	Description
`interfaces modem { modem } [ at | reset ]`	Sends an AT or reset command to the specified modem. Use auto completion to display a list of available modems. • **at** – Sends an AT command to the selected modem. To send multiple AT commands, separate each command with a : colon. • **reset** – Resets the modem.
`interfaces serial restart-serserver`	Restarts the serial communication service.
`interfaces clearstatistics [ ddsName | t1e1Name | t3e3Name ] { name }`	Clears statistics for the specified WAN interface. Use tab completion to display a list of available WAN interfaces.
`services dhcpserver show-active-leases`	Displays active DHCP leases.

2.5.10.4 Administration Commands

Operational mode provides commands for performing device administration tasks.

Command	Description
`admin acknowledge-all-alarms`	Acknowledges all system alarms.
`admin clear-all-alarms`	Clears all system alarms.
`admin delete-autoload-configuration-from-removable`	Deletes the automatic-loading file **autoload-config.cli** (if present) from the removable drive.
`admin restore-factory-defaults`	Restores the factory default configuration and settings, but does not erase any files you have saved on the device.
`admin reboot`	Reboots the device.
`admin save-configuration-to-removable allow-overwrite [ false | true ]`	Saves the current configuration to the removable drive as automatic-loading file **autoload-config.cli**. The allow-overwrite default option is `false`, meaning the action will fail if a file with the same name exists on the removable drive. The `true` options allows the existing **autoload-**

Command	Description
	config.cli file on the removable drive to be overwritten.
`admin save-configuration-to-removable { filename } allow-overwrite [ false | true ]`	Saves the specified file to the removable drive. The allow-overwrite default option is `false`, meaning the action will fail if a file with the same name exists on the removable drive. The `true` options allows the existing file with the same name on the removable drive to be overwritten.
`admin set-system-clock time { YYYY-MM-DD } { HH:MM:SS }`	Sets the date and time on the device. To specify just the date, type the date in the format `{ YYYY-MM-DD }`. To specify just the time, type the time in the format `{ HH:MM:SS }`. To specify both date and time, enclose the string in quotation marks and type the date and time in the format `{ "YYYY-MM-DD HH:MM:SS" }`. **Note** When setting the time, specifying seconds seconds (SS) is optional.
`admin shutdown`	Shuts down the device. For more information on shutting down the device, refer to "Shutting Down the Device" (Page 86)
`admin rox-imaging decline-upgrade`	Cancels (or declines) a recent software upgrade that is waiting for a reboot to the upgraded partition.
`admin rox-imaging software-upgrade`	Launches an upgrade in the alternate partition.
`admin rox-imaging rollback-reboot`	Boots to a previous software release on the alternate partition.
`key-tool-maint-mode`	A key tool to enter the maintenance mode key in hexadecimal format. The hexadecimal format key is available from Siemens Customer Support via telephone when email support is unavailable. The user must be an administrator.
`maint-login`	**⚠ NOTICE** **Configuration hazard – risk of data loss/ corruption** Maintenance mode is provided for troubleshooting purposes and should only be used by Siemens Canada Ltd. technicians. Maintenance mode is provided for troubleshooting purposes and all possible commands are not documented. Misuse of maintenance mode commands can corrupt the operational state of the device and render the device inaccessible. Logs in to the underlying operating system as the root user. The user must be an administrator and be able to provide the maint-login password.

Command	Description
`monitor start { filename }`	Starts displaying the specified system log or tracing the specified file. If necessary, the output can be redirected to a file. For information on how to redirect output, refer to "Using Output Redirects" (Page 35). Use auto completion to view a list of available logs and files.
`monitor stop { filename }`	Stops displaying the specified system log or tracing the specified file. Use auto completion to view a list of available logs and files.
`reportstats`	Displays an extensive collection of device-specific statistics. If necessary, the output can be redirected to a file. For information on how to redirect output, refer to "Using Output Redirects" (Page 35).
`config private`	Enters a configuration mode where users can make changes to the system. This is the primary mode for most users who want to make changes to the device/network configuration. It can be accessed by multiple Operator and Admin users. All changes made during a private configuration session are hidden from other users until they are committed. Each change must be committed before it is applied to the active system. If a user opens an exclusive configuration session during another user's private configuration session, the user in the private configuration session cannot commit their changes until the other user ends their session.
`config exclusive`	Enters a configuration mode where users can make changes to the system. This mode is similar to the private configuration mode, except all other users are blocked from committing their changes until the user using the exclusive configuration mode exits. Only one Operator or Admin user can use the exclusive configuration mode at a time per device. When committing changes in exclusive configuration mode, use the confirmed option to set a timeout period. Changes will be applied for the set period of time, after which the configuration will be reset to its previous settings. This allows users to test their configuration changes before fully applying them to the active system. For more information about the confirmed option, refer to "Configuration Mode General Commands" (Page 59). **⚠ NOTICE** Always log out of the exclusive configuration mode or exit the transaction. If the session is terminated before a user exits properly, other users logged in to the device will continue to be

Command	Description
	blocked from making changes until the session timeout period expires.

2.5.10.5 Configuration Mode General Commands

Configuration mode provides a set of general commands that allow users to work with configuration data.

Command	Description
`abort`	Exits the configuration session without saving changes. **Note** In an edit exclusive session, any pending unconfirmed commits will not be canceled until their timeout periods expire. A new edit exclusive session cannot be opened until the timeout period ends.
`clear`	Deletes all configuration changes.
`commit no-confirm`	Immediately commits the current set of configuration changes. This command will prompt the user to confirm the action. Use the `no-confirm` parameter to revert the configuration without requiring confirmation.
`commit abort`	In an edit exclusive session, this command aborts/ cancels all confirmed commits.
`commit and-quit`	Commits all confirmed and unconfirmed changes and exits the configuration mode.
`commit check`	Validates the current configuration.

`commit confirmed { timeout }`	Temporarily commits changes for a period of time, allowing users to test the configuration before fully committing the changes. The changes must be committed using a standard `commit` command before the timeout period ends. If changes are not committed before the timeout period ends, they are automatically discarded and the previous settings are restored.
	A timeout period can be specified at the end of the command. The default timeout period is 10 minutes. The minimum timeout period is 1 minute. For example:
	`ruggedcom(config-admin)# commit con firmed 2`
	To cancel a commit before the time elapses and discard the changes, type:
	`commit abort`

Command	Description
	To permanently commit the changes before the time elapses, type: `commit`
`commit comment { text }`	Immediately commits the current set of configuration changes along with a custom comment. The comment will appear next to the commit in a list of pending of commits.
`commit label { text }`	Immediately commits the current set of configuration changes along with a custom label. In a list of pending commits, the label will appear instead of the auto-generated commit ID.
`commit persist-id { text }`	Immediately commits the current set of configuration changes and assigns a user-specified ID or flag.
`commit save-running { file }`	Immediately commits the current set of configuration changes and saves them to the specified file. It does not save the complete running configuration.
`copy`	Copies a configured element to a new element. For example, the following command copies the userid *admin* to the new userid *wsmith*: `ruggedcom(config)# copy admin users userid admin smith` The new item has all of the attributes of the item from which it is copied. In this example, userid *wsmith* will have the same password and role attributes as the userid *admin*.

`details`	When used in combination with the `save` command, the `details` command includes default values in the saved configuration file. For example:
	`ruggedcom(config)# save {filename} | details`
	The details command can also be used to show default configuration values. For example:
	`ruggedcom(config)# show running-config admin session-limits | details`

`do`	Performs an Operational mode command. For example, the following command performs the Operational mode `ping` command in the Configuration mode session: `ruggedcom(config)# do ping 172.30.134.12`
`end`	Terminates the configuration session. The system prompts the user to commit uncommitted changes.
`exit`	Exits from the current mode. Unlike the `end` command, the system does not prompt the user to commit uncommitted changes.

Command	Description
`help command`	Displays help information for the specified command.

`load [ merge | override ] { file name }`	Loads a configuration from an ASCII CLI configuration file.
	Two parameters are available for the CLI load command: `override` and `merge`.
	• **Override:** this parameter is for users who have a full configuration file saved and want to load it back on to the device. The full configuration file can be previously created with the CLI **save** command executed from the top level in the configuration tree or with the `admin full-configuration-save` command. With the `override` parameter, the entire running configuration is overwritten by the contents of the configuration file.
	The override option has the following restrictions:
	  • The configuration file must be a *complete* configuration for the device. A *complete* configuration is the entire configuration tree.
	  • The `load` command must be invoked at the base of the configuration tree.
	• **Merge** – this parameter is for users who want to build a template configuration and load it to many devices. The template configuration file can be obtained by using the CLI save command. With the merge parameter, the contents of the configuration file will be merged with the running configuration. The remaining configurations, which are not included in the configuration file, will remain unchanged.
	After loading the configuration, use the `commit` command to commit the changes.

`move ip { interface } ipv4 address { address } [ after | before | first | last ] { address }`	Moves an existing IPv4 address to a new position in the list of addresses. The address can be moved to the first or last (default) position in the list, or before or after another address. For example, the following command moves 172.30.137.37/9 before 172.30.137.31/19: `ruggedcom(config)# move ip fe-3-1 ipv4 address 172.30.137.37/19 before 172.30.137.31/19`
`no`	Negates a command or sets it to its default setting. For example, the following command deletes the IP address 172.30.137.37/19: `ruggedcom(config)# no ip fe-3-1 ipv4 address 172.30.137.37/19`

Command	Description

	Note
	The `no` command affects only the parameter or setting of the node explicitly specified in the command. When using `no` to negate a parameter or setting that has dependencies, clearing the specific parameter does not clear the related dependencies.
	For example, the following command adds an IPv4 route with a gateway:
	`ruggedcom(config)# routing stat ic ipv4 route 192.168.33.0/24 via 192.168.11.2`
	The following command deletes the gateway, but it does not delete the route:
	`ruggedcom(config)# no routing sta tic ipv4 route 192.168.33.0/24 via 192.168.11.2`
	The `no` deletes only the explicitly specified parameter or object.

`pwd`	Displays the path to the current node. For example, after navigating to an IPv4 address, the following command displays the path through the command hierarchy to the current node: `ruggedcom(config-ad dress-172.30.137.31/19)# pwd Current submode path: ip fe-3-1 \ ipv4 \ address 172.30.137.31/19`
`rename`	Changes the value of a parameter. For example, the following command changes the IPv4 address 172.30.137.36/19 to 172.30.137.40/19: `ruggedcom(config)# rename ip fe-3-1 ipv4 address 172.30.137.36/19 172.30.137.40/19`
`resolved`	Issue this command when conflicts have been resolved. Conflicts are normally discovered when the commit operation is performed. Conflicts typically arise when multiple users edit the same parts of a configuration.
`revert no-confirm`	Copies the running configuration into the current configuration. This discards all changes to the current configuration. This command will prompt the user to confirm the action. Use the `no-confirm` parameter to revert the configuration without requiring confirmation.
`rollback configuration { number }`	Returns the configuration to a previously committed configuration. The system stores

Command	Description

	a limited number of old configurations.
	After reaching the maximum number of old configurations, storing a new configuration deletes the oldest configuration in the list. The most recently committed configuration (the running configuration) appears as item 0 in the list. Select a number from the list and press **Enter**.
	`ruggedcom(config)# rollback configu ration`
	` Possible completions:`
	` 0 2012-01-08 13:51:46 by admin`
	` via cli`
	` 1 2012-01-08 13:50:58 by admin`
	` via cli`
	` 2 2012-01-08 12:05:46 by admin`
	` via cli`
	` 3 2012-01-08 10:47:42 by admin`
	` via cli`
	` 4 2012-01-08 07:49:38 by admin`
	` via cli`
	` 5 2012-01-08 07:46:14 by admin`
	` via cli`
	` ruggedcom(config)# rollback config uration`
	After rolling back the configuration, use the `commit` command to commit the changes.

`save { filename }`	Saves the current configuration, without default values, to an ASCII file. Specify a filename for the file.
	Current configuration means the configuration of the user's current level in the configuration data hierarchy. For example, if the user is at the top level, the `save` command will save the complete/full configuration of the device.
	`ruggedcom(config)# save {full-con figuration-filename}`
	If the user is at a level other than the top level, such as the *firewall* level, the `save` command will save a partial configuration of the current level.
	`ruggedcom(config)#security firewall`
	`ruggedcom(config-firewall)# save`
	` {firewall-configuration-filename}`
	Use this command along with the `details` command to include default values in the saved configuration file. For example:
	`ruggedcom(config)# save {filename} |`
	` details`

`show`	Shows configuration, history or command line interface parser information. Type `show` and press **Tab** to navigate through the items available to display.

Command	Description
	This command can also be combined with the `details` command to display the default configuration values. For example: `ruggedcom# show running-config admin session-limits | details`
`top command`	Exits to the top level of the command hierarchy and, optionally, runs a command.
`validate`	Validates the current configuration.
`wizard [ rox_flash ]`	Runs the rox_flash wizard. For more information, refer to "Downgrading Software" (Page 121).
`wizard [ rox_upgrade ]`	Runs the rox_upgrade wizard. For more information, refer to either "Upgrading the Software and Retaining the Configuration" (Page 115) or "Upgrading the Software and Resetting the Configuration" (Page 118).

2.6 Configuring the CLI Interface

The following commands can be used to configure certain characteristics and customize the CLI interface.

Command	Description
`autowizard { true | false }`	When enabled, the CLI prompts for required settings when a new identifier is created.
`clear history`	Clears the CLI history.
`display-level`	Determines the depth of hierarchical information to display in command results.
`history { integer }`	Determines the number of items to record in the CLI history.
`output-file { { filename } | terminal }`	Directs CLI output to the specified ASCII text file, or to the terminal. Output is directed to the specified destination until another destination is set with a subsequent `output-file` command.
`paginate { true | false }`	Lengthy output is paginated by default. When the output reaches the screen-length setting, the CLI prompts the user to press a key for more output. Press **Enter** to advance line-by-line or press **Space** to advance page-by-page. When disabled, output is not paginated.
`screen-length { integer }`	Determines the number of lines in a terminal page.
`screen-width { integer }`	Determines the length of terminal lines.
`show-defaults { true | false }`	Determines if default values are shown when displaying the configuration. When enabled, default values appear as comments after the configured value. In the following example, the default value for the contact value is shown as

Command	Description

	a comment following the configured contact string of *wsmith@example.com*:
	`ruggedcom# show running-config admin`
	` contact`
	` admin`
	` contact "wsmith@example.com"  !`
	` Contact`
	` !`
	Default values only appear for parameters that have default values. If a parameter does not have a default value, no default appears when `show-defaults` is set to true.

`terminal { dumb | vt100 | xterm | linux | ansi }`	Determines the terminal type and controls how line editing is performed. Supported terminals are: dumb, vt100, xterm, linux, and ansi. Other terminals may also work but have no explicit support.

2.7 Accessing Different Modes

Aside from normal mode, there are three additional modes within RUGGEDCOM ROX II that offer various controls over the operating system.

2.7.1 Accessing BIST Mode

BIST (Built-In-Self-Test) mode is used by RUGGEDCOM ROX II to test and configure internal functions of the device. The method for accessing BIST is different if a new software image has been flashed onto the flash card.

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

BIST mode is available to users with console access. As such, console access should be restricted to authorized personnel only.

⚠ NOTICE

Configuration hazard – risk of data corruption

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

Note

BIST mode opens port TCP/222 and cannot be disabled. An IP address must be configured before users attempt to access the device via SSH.

To access BIST mode normally, do the following:

⚠ NOTICE

Do not connect the device to the network when it is in BIST mode. The device will generate excess multicast traffic in this mode.

1. Disconnect the device from the network.
2. Connect to the RUGGEDCOM RX1500 through the RS-232 console connection and a terminal application. For more information, refer to "Connecting Directly via Serial Console" (Page 75).
3. Reboot the device. For more information, refer to "Rebooting the Device" (Page 87).
4. If prompted, provide the boot password/passphrase for the device.
5. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
 'h' Show this help menu
 'l' List the available boot targets
 'c' Exit to the boot loader command line

 Will reboot after 60 seconds of inactivity
 :
```

Note

In the example above, the text `Auto booting [4-0]` indicates the active partition is Boot Partition 4.

6. Enter boot mode on the active partition by typing the associated target number. For example, if the active partition is Boot Partition 6, type `6-1` and press **Enter**. The self-test cycle begins.
7. Press **Ctrl+c** to stop the self-test cycle and halt the excess multicast traffic. A BIST prompt appears.

```
BIST:~#
```

To access BIST mode after flashing a new software image on to the flash card, do the following:

1. Connect to the RUGGEDCOM RX1500 through the RS-232 console connection and a terminal application. For more information, refer to "Connecting Directly via Serial Console" (Page 75).
2. Cycle power to the device.
3. If prompted, provide the boot password/passphrase for the device.
4. Press **Ctrl+c** to stop the self-test cycle and halt the excess multicast traffic. A BIST prompt appears.

```
BIST:~#
```

Once all configuration changes or tests are complete, it is important to change the boot mode by doing the following:

1. Set the next boot to normal by typing:

```
nextboot normal
```

2. Reboot the device by typing:

```
reboot
```

3. Connect the device to the network.

2.7.2 Accessing Service Mode

Service mode grants access to the Linux shell.

To access service mode, do the following:

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

Service mode opens port TCP/222 and cannot be disabled. If the device is connected to the network, a user with remote access to the device and the root password could access the Linux shell. If required, protect the device by either:

- Disconnecting the device from the network
- Making sure a strong password is configured and the device is connected to a trusted network

⚠ NOTICE

Configuration hazard – risk of data corruption

Service mode is provided for troubleshooting and advanced configuration purposes and should only be used by Siemens technicians. As such, this mode is not fully documented. Misuse of the commands available in this mode can corrupt the operational state of the device and render it inaccessible.

⚠ NOTICE

Changes made to the configuration in this mode will override the current configuration settings (e.g. IP addresses, VLAN settings, etc.), but are discarded following a system reboot.

1. Connect to RUGGEDCOM ROX II through the RS-232 console connection and a terminal application. For more information, refer to "Connecting Directly via Serial Console" (Page 75).
2. Reboot the device. For more information, refer to "Rebooting the Device" (Page 87).
3. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
 'h' Show this help menu
 'l' List the available boot targets
 'c' Exit to the boot loader command line

 Will reboot after 60 seconds of inactivity
 :
```

Note

In the example above, the text `Auto booting [4-0]` indicates the active partition is Boot Partition 4.

4. Enter service mode on the active partition by typing the associated target number. For example, if the active partition is Boot Partition 6, type `6-3`. A login prompt for service mode appears.
5. Type `root` and press **Enter**. A password prompt appears.

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 25).

Note

The current service mode password/passphrase is the same as the password/passphrase for accessing maintenance mode.

6. Type the current service mode password/passphrase and press **Enter**.

```
ruggedcom login: root
 Password:
 Last login: Tue Oct 13 13:37:38 EDT 2020 on ttyS0
 Linux ruggedcom 3.0.0-2-8360e #1 Thu Jan 24 21:20:30 UTC 2013 ppc

 The programs included with the Debian GNU/Linux system are free software;
 the exact distribution terms for each program are described in the
 individual files in /usr/share/doc/*/copyright.

 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
 permitted by applicable law.

  8t-eterminal size now 80x20

 Welcome to ruggedcom Partition1 (Rev ROX 2.4.0 (2013-01-24 18:20)) RX1510 SN
 12110102-0012-0030060017   13:42:07 up 7 min
 Temperature +38.5 C (+101.3 F)  Disk 24%  Memory 41%

 root@ruggedcom:~#
```

2.7.3 Accessing Maintenance Mode

Maintenance mode grants access to the Linux shell.

To access maintenance mode, do the following:

⚠ 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 the commands available in this mode can corrupt the operational state of the device and render it inaccessible.

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

To avoid unauthorized users from accessing maintenance mode, make sure the default maintenance mode password has been replaced with a strong password. For information about creating strong passwords, refer to "Managing Passwords and Passphrases" (Page 153).

Note

A key is required to authorize maintenance mode access. To obtain an access key, contact Siemens Customer Support.

For information about installing the access key and enabling maintenance mode, refer to "Temporarily Enabling Maintenance Mode Authorization" (Page 71).

Note

Changes made to the configuration in this mode will override the current configuration settings (e.g. IP addresses, VLAN settings, etc.), but are discarded following a system reboot.

1. If the default password has been changed previously, proceed to step 2 (Page 70). Otherwise, change the default maintenance mode password to a strong password. For information about setting the maintenance mode password, refer to "Setting the Maintenance Password/Passphrase" (Page 157).
2. Enable maintenance mode authorization. For more information, refer to "Temporarily Enabling Maintenance Mode Authorization" (Page 71).
3. In normal mode, type `maint-login` and press **Enter**. A password prompt appears.

   Note

   The current maintenance mode password/passphrase is the same as the password/passphrase for accessing service mode.

4. Type the current maintenance mode password/passphrase and press **Enter**.

   Example:

```
ruggedcom# maint-login
Password:

Welcome to ruggedcom Partition2 (Rev ROX 2.16.0 (2023-01-24 18:20)) RX1500 SN
 R15R-3410-PR061 22:29:20 up 1 day, 8:42
Temperature +41.0 C (+105.8 F) Disk 25% Memory 43%

root@ruggedcom:~#
```

5. [Optional] Enable SSH access. SSH is disabled by default. For more information, refer to "Enabling/Disabling SSH Access in Maintenance Mode" (Page 70).

2.7.4 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
```

2.7.5 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.

Maintenence 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.

2.7.5.1 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.

To support this method the following CLI command is used:

```
key-tool-maint-mode
```

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, type `maint-login` and press **Enter** .

2. Type the following:

   ```
   admin authentication enable-maint-mode key { key }
   ```

   Where:

   - `{ key }` is the access key provided by Siemens Customer Support.

   Maintenance mode authorization will be enabled until the next device reboot.

3. [Optional] To verify maintenence mode authorization status has been successfully enabled, refer to "Displaying Device and Software Information" (Page 79).
4. [Optional] Access maintenance mode with the maintenence mode password. For more information, refer to refer to "Accessing Maintenance Mode" (Page 69).

2.7.5.2 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 113).

For more information about restoring the factory default settings for the device, refer to "Restoring Factory Defaults" (Page 87).

⚠ 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 71).
2. Type the following:

   ```
   admin authentication permanent-maint-mode
   ```

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

2.7.5.3 Disabling Maintenance Mode Authorization

To disable maintenance mode authorization, do the following:

- Type the following:

  ```
  admin authentication disable-maint-mode
  ```

  Maintenance mode is disabled.

3 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 CLI, 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 Serial Console

The Command Line Interface (CLI) can be accessed directly using an appropriate cable connection between the device and a workstation.

To access the Command Line Interface (CLI) using a direct connection to the device, do the following:

1. Connect a workstation running terminal emulation software to the RS-232 console port on the device.

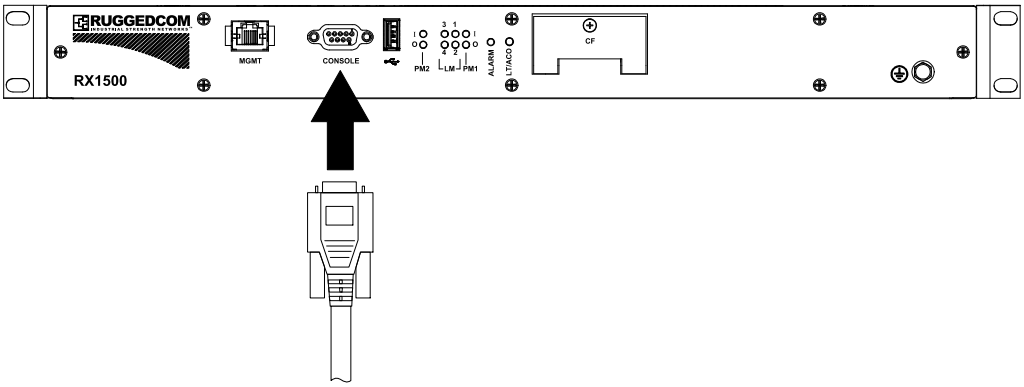


Figure 3.1 RS-232 Console Port (RUGGEDCOM RX1500 Model Shown)

2. Configure the terminal as follows:
   - 57600 bps
   - No parity
   - 8 bits
   - Set the terminal type to VT100
   - Disable hardware and software flow control
3. Establish a connection to the device and press any key. The login prompt appears.

   ```
   {host name} login:
   ```

4. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 25).

3.1.3 Connecting Remotely via SSH

The Command Line Interface (CLI) can be accessed securely and remotely using an SSH client.

To access the CLI, do the following:

1. Launch an SSH client and specify the following connection settings:
   - **Host Name:** The IP address of the device or the IP address prefixed with the desired user profile (e.g. admin@192.168.0.2)
   - **Port** – 22
2. Connect to the device.

⚠ NOTICE
Key Exchange Errors Some SSH/Telnet clients, such as PuTTy, may present an error message stating an agreement on a key exchange algorithm could not be reached. For more information about how to resolve algorithm issues, refer to "Management Access" (Page 967).

3. 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.

```
login as:
```

4. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 25).

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

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 166).
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 166).
7. Enable IPv6 Neighbor Discovery. For more information, refer to "Configuring IPv6 Neighbor Discovery" (Page 271).
8. Make sure all computers connected to the device can ping one another.

4 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, type:

```
show chassis chassis-status
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis chassis-status
chassis-status
 model                       RX1501
 software license            "Layer 3 Security Edition"
 rox release                 "ROX 2.13.0 (2023-01-01 08:00)"
 system serial number        RX1501R-0812-00664
 last integrity check        "2023-01-01 09:00"
 last integrity check result Success
 maint mode status           Disabled
```

This list provides the following information:

Parameter	Description
`model`	**Synopsis:** A string The RuggedCom device model name.
`software-license`	**Synopsis:** A string The current software capability.
`mlfb`	**Synopsis:** A string up to 256 characters long MLFB(Machine-Readable Product Designation) or order code
`rox-release`	**Synopsis:** A string The release of ROX running on the chassis.
`system-serial-number`	**Synopsis:** A string up to 32 characters long The system serial number on the chassis label.

Parameter	Description
`last-integrity-check`	**Synopsis:** A string up to 32 characters long The last time the firmware integrity was checked.
`last-integrity-check-result`	**Synopsis:** A string The result of the last integrity check.
`maint-mode-status`	**Synopsis:** 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, type:

```
show chassis hardware slot-hardware
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis hardware slot-hardware | tab
      ORDER
SLOT  FIELD      DETECTED MODULE                                          SERIAL N
-------------------------------------------------------------------------------
pm1   HI         88-300 VDC or 85-264VAC, screw terminal block            P15R-071
lm1   CG01       1000TX w/ 2x RJ45                                        L15R-081
lm2   XX         none                                                     none
lm3   S01        6x RS232/RS422/RS485 via RJ45                            L15R-081
lm4   XX         none                                                     none
lm5   XX         none                                                     none
lm6   XX         none                                                     none
main  RX1501-L3  RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots    49110102
```

The table or list provides the following information:

Parameter	Description
`{ slot }`	**Synopsis:** [--- | 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.
`order-field`	**Synopsis:** A string up to 25 characters long The order code of the chassis as derived from the current hardware configuration.

Parameter	Description
detected-module	**Synopsis:** A string up to 60 characters long The installed module's type specifier.
serial-number	**Synopsis:** A string up to 64 characters long The installed module's unique serial number.

4.2.2 Viewing Module Information

To view information about the modules installed in the device, type:

```
show chassis info slot-info
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis info slot-info | tab
SLOT  DETECTED MODULE                                          BootLoader   FPGA
-------------------------------------------------------------------------------
main  RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots  2010.09RR12  14-23
```

The table or list provides the following information:

Parameter	Description
detected-module	**Synopsis:** A string up to 60 characters long The installed module's type specifier.
boot-loader-version	**Synopsis:** A string The version of the ROX bootloader software on the installed module.
fpga-version	**Synopsis:** A string The version of the ROX FPGA firmware (if any) running on the installed module.

4.2.3 Viewing Flash Card Storage Utilization

To view the Flash card storage utilization statistics for the Flash card installed in the device, type:

```
show chassis storage
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis storage | tab
storage
 flash
  storage name                "Compact Flash"
  total capacity              994896
  current partition           "Partition #1"
```

```
  current partition capacity   490496
  secondary partition capacity 490496
  current partition usage      67
```

The table or list provides the following information:

Parameter	Description
`storage-name`	**Synopsis:** A string between 0 and 32 characters long The type of storage.
`total-capacity`	**Synopsis:** An integer between 0 and 4294967295 The total capacity of the flash storage in KB.
`current-partition`	**Synopsis:** A string between 0 and 32 characters long The partition ROX is currently running on and booted from.
`current-partition-capacity`	**Synopsis:** An integer between 0 and 4294967295 The capacity of the current partition in KB.
`secondary-partition-capacity`	**Synopsis:** An integer between 0 and 4294967295 The capacity of the secondary partition in KB.
`current-partition-usage`	**Synopsis:** An integer between 0 and 100 The %usage of the current partition.
`model-number`	**Synopsis:** A string between 0 and 255 characters long The model number of the storage device.
`serial-number`	**Synopsis:** 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, type:

```
show chassis cpu slot-cpu
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis cpu slot-cpu | tab
                                                                          RAM
                                                                CPU   RAM    AVAIL
SLOT  DETECTED MODULE                                           LOAD  AVAIL  LOW
-------------------------------------------------------------------------------------
main  RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots  26    56     56
```

The table or list provides the following information:

Parameter	Description
`detected-module`	**Synopsis:** A string up to 60 characters long The installed module's type specifier.
`cpu-load`	**Synopsis:** An integer between 0 and 100 The CPU load, in percent, on the installed module.
`ram-avail`	**Synopsis:** An integer between 0 and 100 The proportion of memory (RAM) currently unused, in percent, on the installed module.
`ram-avail-low`	**Synopsis:** 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, type:

```
show chassis status slot-status
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis status slot-status | tab
                                                                                STATUS
            START
SLOT  DETECTED MODULE                                          STATE      STRING  UPTIME
 START DATE   TIME
-------------------------------------------------------------------------------------------
pm1   88-300 VDC or 85-264VAC, screw terminal block           operating  Normal  1D 4hr 47min 12sec
 2012-10-24Z  06:44:32Z
lm1   1000TX w/ 2x RJ45                                       operating  Normal  0D 0hr 0min 0sec
 2012-10-24Z  06:42:28Z
lm2   none                                                    empty      ----    0D 0hr 0min 0sec
 2012-10-24Z  06:42:28Z
lm3   6x RS232/RS422/RS485 via RJ45                           operating  Normal  0D 0hr 0min 0sec
 2012-10-24Z  06:42:28Z
lm4   none                                                    empty      ----    0D 0hr 0min 0sec
 2012-10-24Z  06:42:28Z
lm5   none                                                    empty      ----    0D 0hr 0min 0sec
 2012-10-24Z  06:42:28Z
lm6   none                                                    empty      ----    0D 0hr 0min 0sec
 2012-10-24Z  06:42:28Z
main  RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots  operating  Normal  1D 4hr 47min 12sec
 2012-10-24Z  06:44:32Z
```

The table or list provides the following information:

Parameter	Description
`{ slot }`	**Synopsis:** [--- | 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.

Parameter	Description
`detected-module`	**Synopsis:** A string up to 60 characters long The installed module's type specifier.
`state`	**Synopsis:** [unknown | empty | disabled | resetting | operating | failed | disconnected] The current state of the installed module.
`status-string`	**Synopsis:** A string The runtime status of the installed module.
`uptime`	**Synopsis:** A string The total time elapsed since the start-up of the installed module.
`start-date`	**Synopsis:** A string The date on which the installed module was started up.
`start-time`	**Synopsis:** 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, type:.

```
show chassis sensors
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis sensors
                                                                          CURRENT  VOLTAGE
SLOT  DETECTED MODULE                                          TEMPERATURE SUPPLY   SUPPLY
-------------------------------------------------------------------------------------------
pm1   88-300 VDC or 85-264VAC, screw terminal block           48          2669     3385
lm1   1000TX w/ 2x RJ45                                       -           -        -
lm3   6x RS232/RS422/RS485 via RJ45                           -           -        -
main  RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots   42          1661     3327
```

The table or list provides the following information:

Parameter	Description
`{ slot }`	**Synopsis:** [--- | 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`	**Synopsis:** A string up to 60 characters long The installed module's type specifier.

Parameter	Description
temperature	**Synopsis:** 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.
current-supply	**Synopsis:** An integer between 0 and 15000 The power supply current, in mA, being drawn by the installed module.
voltage-supply	**Synopsis:** 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 information about the power controller, type:

```
show chassis power-controller pm-status
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis power-controller pm-status | tab
PM    MOV          PM           PM       PM
SLOT  PROTECTION   TEMPERATURE  CURRENT  VOLTAGE
-------------------------------------------------
pm1   na           48           2666     3387
```

The table or list provides the following information:

Parameter	Description
{ pm-slot }	**Synopsis:** [pm1 | pm2] The name of the power module slot as labeled on the chassis.
mov-protection	**Synopsis:** [na | working | damaged] The state of the MOV protection circuit. Possible values include: • **na** – MOV protection is not applicable to the device. • **working** – MOV protection is working. • **damaged** – The MOV protection fuse is damaged. Contact Siemens Customer Support.
pm-temperature	**Synopsis:** An integer between -55 and 125 The temperature (Celsius) inside the power module.
pm-current	**Synopsis:** An integer between 0 and 15000 The current (mA) sourced by the power module.
pm-voltage	**Synopsis:** An integer between 0 and 15000 The voltage (mV) sourced by the power module.

4.3 Viewing the Parts List

To view a list of parts installed in the device, type:

```
show running-config chassis part-list
```

If jobs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config chassis part-list | tab
MODEL   ORDERFIELD  PARTNUMBER                    PARTNAME
-------------------------------------------------------------------------------
RX1500  12          12-02-9999-001  12VDC (9-15VDC), screw terminal block
RX1500  12P         12-02-9999-002  12VDC (9-15VDC), pluggable terminal block
RX1500  24          12-02-0027-003  24VDC (10-36VDC), screw terminal block
RX1500  24          12-02-0035-003  24VDC (10-36VDC), screw terminal block
RX1500  24P         12-02-0027-004  24VDC (10-36VDC), pluggable terminal block
RX1500  24P         12-02-0035-004  24VDC (10-36VDC), pluggable terminal block
RX1500  48          12-02-0027-001  48VDC (36-72VDC), screw terminal block
RX1500  48          12-02-0035-001  48VDC (36-72VDC), screw terminal block
RX1500  48P         12-02-0027-002  48VDC (36-72VDC), pluggable terminal block
RX1500  48P         12-02-0035-002  48VDC (36-72VDC), pluggable terminal block
RX1500  4FX03       12-02-0018-005  4 x 100FX - Multimode, 1300nm, MTRJ connec
tors, 2km
RX1500  4FX06       12-02-0018-002  4 x 100FX - Singlemode, 1300nm, LC connectors,
 20km
RX1500  4FX08       12-02-0018-003  4 x 100FX - Singlemode, 1300nm, LC connectors,
 50km
.
.
.
```

4.4 Shutting Down the Device

To shut down the device, type:

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

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 devices 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.

```
admin shutdown
```

4.5 Rebooting the Device

To reboot the device, type:

```
admin reboot
```

4.6 Restoring Factory Defaults

To restore the factory defaults for the device, use the following command:

```
admin restore-factory-defaults
```

If necessary, include the following options:

Parameter	Description
`delete-logs { delete-logs }`	**Synopsis:** [true | false] **Default:** false Delete system logs as well as restoring default settings.
`default-both-partitions { default-both-partitions }`	**Synopsis:** [true | false] **Default:** false Perform the operation on both partitions.
`delete-saved-configurations { delete-saved-configurations }`	**Synopsis:** [true | false] **Default:** false Delete saved configuration files (works with default-both-partitions option).
`shutdown { shutdown }`	**Synopsis:** [true | false] **Default:** false Shutdown rather than reboot after restoring factory defaults.

4.7 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 "Accessing Maintenance Mode" (Page 69).
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 25).
6. Flash the RUGGEDCOM ROX II firmware obtained in step 1 (Page 87) to the inactive partition and reboot the device. For more information, refer to "Downgrading Software" (Page 121).
7. Repeat step 5 (Page 88) and step 6 (Page 88) to flash the RUGGEDCOM ROX II firmware obtained in step 1 (Page 87) to the other partition and reboot the device.
8. Shut down the device. For more information, refer to "Shutting Down the Device" (Page 86).

⚠ 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.

4.8 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 7). 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 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, refer to "Displaying Device and Software Information" (Page 79).

4.8.1 Viewing the Contents of a Feature Key

To view the contents of a feature key saved on the device, do the following:

1. Make sure the CLI is in Operational mode.
2. At the command prompt, type:

   ```
   file show-featurekey { filename }
   ```

   Where:

   - `{ filename }` is the name of feature key file stored on the device

   For example:

   ```
   ruggedcom# file show-featurekey 1_cmRX1K-12-11-0015.key
   ```

3. Press **Enter**. The system displays the contents of the feature key file. For example:

   ```
   ruggedcom# file show-featurekey L3SE_cmRUMHD06096338.key
   GPG_FEATUREKEY_LEVEL=L3SE
   GPG_FEATUREKEY_CM_SERIALNUMBER=RUMHD06096338
   GPG_FEATUREKEY_SIGNATURE=iEYEABECAAYFAliGF4EACgkQP2pya+G5kdYj1ACfecKysp3DK3QB
   sP87I/gXgi92cwAAnjqrsgdqwaCczY4ghWrR0ELkr2TK
   ```

4.8.2 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. Make sure the CLI is in Operational mode.
3. 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
```

4. 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 91).

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

4.9.1 Installing Files

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

⚠ NOTICE
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 RX1500/ RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 Installation Manual".
2. Navigate to ***admin » install-files*** and configure the following parameter(s) as required:

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 226).

Parameter	Description
`file-type { file-type }`	**Synopsis:** [config | featurekey | vmfile] The file types to be copied.
`url { url }`	**Synopsis:** A string between 1 and 1024 characters long The URL of the ROX II file to copy. Supported URIs are HTTP, SCP, SFTP, FTPS and FTP. 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. 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.

4.9.2 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 RX1500/ RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 Installation Manual".

2. Make sure the CLI is in Configuration mode.
3. Navigate to ***admin » backup-files*** and configure the following parameter(s) as required:

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 226).

Parameter	Description
`file-type { file-type }`	**Synopsis:** [config | featurekey | logfiles | rollbacks | licenses | logarchive] The file types to copy.
`file { file }`	**Synopsis:** 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.
`timestamp { time stamp }`	**Synopsis:** [true | false] **Default:** false If enabled, a time stamp will be appended to the file name. This option is not applicable to file names that contain '*'.
`url { url }`	**Synopsis:** A string between 1 and 1024 characters long The URL of the ROX II file to copy. Supported URIs are HTTP, SCP, SFTP, FTPS and FTP. 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. 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.

4.10 Managing Logs

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

Security Event Logs	Information related to the following security events are logged by RUGGEDCOM ROX II: **Note** Passwords can be retried up to 3 times before the login attempt is considered a security event. • Successful and unsuccessful login attempts • Local and remote (RADIUS) authentication • Security-sensitive commands (whether successful or unsuccessful) • An optionally configurable SNMP Authentication Failure Trap (disabled by default) in accordance with SNMPv2-MIB All security event logs are recorded in **var/log/auth.log** and can be viewed in the Authlog Viewer. For more information about viewing logs, refer to "Viewing Logs" (Page 93).
Syslogs	Syslog allows users to configure local and remote syslog connections to record important, non-security event information. The remote Syslog protocol, defined in RFC 3164 [http://tools.ietf.org/html/rfc3164], 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 servers. The protocol is designed to simply transport these event messages from the generating device to the collector. All log files are organized in the log directory (**/var/log**) 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. The following log files are setup with the following default selectors: • **syslog** catches all logs except daemon.debug, auth or authpriv logs • **daemon.log** catches all *err* level (and above) logs written to the daemon facility • **messages** catches all *info*, *notice* and *warn* level logs for all facilities except auth, authpriv, cron, daemon, mail and news A selector setup using the following facilities at level *info* and up is recommended: • daemon • user • kern • syslog
Diagnostic Logs	Diagnostic logs record system information for the purposes of troubleshooting.

4.10.1 Viewing Logs

Select logs can be viewed directly within the CLI. 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 91).

To view a log in the CLI, do the following:

```
show log { file }
```

Where:

- `{ file }` is the log file to view

For example, to view the auth.log, type:

```
show log auth.log
```

A result similar to the following is displayed:

```
ruggedcom# show log auth.log
Jan 29 09:25:00 ruggedcom confd[2068]: audit user: admin/0 failed to login using
 externalauth:  Local authentication
Jan 29 09:25:00 ruggedcom confd[2068]: audit user: admin/0 logged in through Web
 UI from 192.168.0.200
Jan 29 09:25:00 ruggedcom confd[2068]: audit user: admin/32 assigned to groups:
 admin
Jan 29 09:25:01 ruggedcom CRON[4599]: pam_unix(cron:session): session opened for
 user root by (uid=0)
.
.
.
```

4.10.2 Deleting Logs

To delete all logs stored on the device, type:

```
admin delete-logs
```

4.10.3 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).

⚠ NOTICE

The client (RUGGEDCOM ROX II) and server certificates must by signed by the same CA.

4.10.3.1 Enabling/Disabling Secure Remote Syslog

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

1. Make sure the CLI is in Configuration mode.

   Note

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

2. Enable or disable secure remote syslog by typing either:

   Enabling

   ```
   admin logging secure-remote-syslog enable
   ```

   Disabling

   ```
   no admin logging secure-remote-syslog enable
   ```

   ⚠ NOTICE

   All certificates must meet the following requirements:

   - X.509 v3 digital certificate format
   - PEM format
   - RSA key pair, 512 to 2048 bits in length

3. If secure remote syslog is enabled, specify a certificate to use for authentication with remote syslog server by typing:

   ```
   certificate { certificate }
   ```

   Where:

   - { certificate } is the name of the certificate

   If the desired certificate is not listed, add it. For more information, refer to "Adding a Certificate" (Page 225).

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 96).

5. Type `commit` and press **Enter** to save the changes.

4.10.3.2 Viewing a List of Permitted Peers

To view a list of permitted peers, type:

```
show running-config admin logging secure-remote-syslog per
mitted-peer
```

If peers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin logging secure-remote-syslog permitted-peer

admin
 logging
  secure-remote-syslog permitted-peer *.example.com
  !
 !
!
```

If no permitted peers have been configured, add peers as needed. For more information, refer to "Adding a Permitted Peer" (Page 96).

4.10.3.3 Adding a Permitted Peer

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

1. Make sure the CLI is in Configuration mode.
2. Add the permitted peer by typing:

   ```
   admin logging secure-remote-syslog permitted-peer { pat
   tern }
   ```

   Where:

   - { pattern } is the pattern used to match the common name defined in the SSL certificate received from the server
3. Type `commit` and press **Enter** to save the changes.

4.10.3.4 Deleting a Permitted Peer

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

1. Make sure the CLI is in Configuration mode.
2. Delete the firewall by typing:

   ```
   no admin logging secure-remote-syslog permitted-peer
   { pattern }
   ```

   Where:

   - { pattern } is the pattern used to match the server's host name to the common name defined in the SSL certificate

3. Type `commit` and press **Enter** to save the changes.

4.10.3.5 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 the CLI is in Configuration mode.
2. Make sure an IP address is first defined for the desired interface. For more information, refer to either "Adding an IPv4 Address" (Page 269) or "Adding an IPv6 Address" (Page 270).
3. Configure the source IP address by typing:

   ```
   admin logging source-ip { address }
   ```

   Where:

   - `{ address }` is the alternative source IP address
4. Type `commit` and press **Enter** to save the changes.

4.10.4 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	**/var/log/confd-dev.log**
SNMP Log	**/var/log/snmp-trace.log**
NETCONF Summary Log	**/var/log/netconf.log**
NETCONF Trace Log	**/var/log/netconf-trace.log**
XPATH Trace Log	**/var/log/xpath-trace.log**
WebUI Trace Log	**/var/log/webui-trace.log**

⚠ 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.

4.10.4.1 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the Developer's log by typing the following commands:

   Enable

   ```
   admin logging diagnostics developer-log enabled
   ```

   Disable

   ```
   no admin logging diagnostics developer-log enabled
   ```

3. Configure the level of information provided by the Developer's log by typing:

Parameter	Description
`log-level { log-level }`	**Synopsis:** [error | info | trace] **Default:** info Sets the verbosity level for developer logging.

4. Type `commit` and press **Enter** to save the changes.

4.10.4.2 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the SNMP log by typing the following commands:

   Enable

   ```
   admin logging diagnostics snmp-log enabled
   ```

   Disable

```
no admin logging diagnostics snmp-log enabled
```

3. Type `commit` and press **Enter** to save the changes.

4.10.4.3 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the NETCONF Summary log by typing the following commands:

   Enable

   ```
   admin logging diagnostics netconf-summary-log enabled
   ```

   Disable

   ```
   no admin logging diagnostics netconf-summary-log enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

4.10.4.4 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the NETCONF Trace log by typing the following commands:

   Enable

   ```
   admin logging diagnostics netconf-trace-log enabled
   ```

   Disable

   ```
   no admin logging diagnostics netconf-trace-log enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

4.10.4.5 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the XPATH Trace log by typing the following commands:

   Enable

   ```
   admin logging diagnostics xpath-trace-log enabled
   ```

   Disable

   ```
   no admin logging diagnostics xpath-trace-log enabled
   ```
3. Type `commit` and press **Enter** to save the changes.

4.10.4.6 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.

⚠ 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 WebUI Trace log, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the WebUI Trace log by typing the following commands:

   Enable

   ```
   admin logging diagnostics webui-trace-log enabled
   ```

   Disable

   ```
   no admin logging diagnostics webui-trace-log enabled
   ```
3. Type `commit` and press **Enter** to save the changes.

4.10.4.7 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the JSON-PRC log by typing the following commands:

   Enable

   ```
   admin logging diagnostics JSON-PRC-log enabled
   ```

Disable

```
no admin logging diagnostics JSON-PRC-log enabled
```

3. Type `commit` and press **Enter** to save the changes.

4.10.5 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

4.10.5.1 Viewing a List of Remote Servers

To view a list of remote servers, type:

```
show running-config admin logging server
```

If remote servers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin logging server
admin
 logging
  server 172.30.144.254
   enabled
   selector 1
    no negate
    facility-list [ all ]
   !
  !
 !
!
```

If no remote servers have been configured, add servers as needed. For more information, refer to "Adding a Remote Server" (Page 102).

4.10.5.2 Adding a Remote Server

To add a remote server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the remote server by typing:

   ```
   admin logging server { address }
   ```

   Where { address } is the IP address of the remote server.
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables/disables the feed to the remote logging server.
`transport { transport }`	**Synopsis:** [udp | tcp] **Default:** udp TCP or UDP.
`monitor-interface { monitor-interface }`	**Synopsis:** A string The interface to monitor. If the IP address is changed on the interface, the logging daemon will restart.
`port { port }`	**Synopsis:** An integer between 1 and 65535 **Default:** 514 Port number.

4. Configure one or more selectors for the server. For more information, refer to "Adding a Remote Server Selector" (Page 104).
5. Type `commit` and press **Enter** to save the changes.

4.10.5.3 Deleting a Remote Server

To delete a remote server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the remote server by typing:

   ```
   no admin logging server { address }
   ```

   Where:

   - `{ address }` is the IP address of the remote server.
3. Type `commit` and press **Enter** to save the changes.

4.10.6 Managing Remote Server Selectors

Remote server selectors filter the information sent to specific servers.

4.10.6.1 Viewing a List of Remote Server Selectors

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

To view a list of remote server selectors, type:

```
show running-config admin logging server { address } selector
```

Where:

- `{ address }` is the IP address of the remote server.

If remote server selectors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin logging server 172.30.144.254 selector
admin
 logging
  server 172.30.144.254
   selector 1
    no negate
    facility-list [ all ]
   !
  !
 !
!
```

If no remote server selectors have been configured, add selectors as needed. For more information, refer to "Adding a Remote Server Selector" (Page 104).

4.10.6.2 Adding a Remote Server Selector

To add a remote server selector, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the remote server selector by typing:

   `admin logging server { address } selector { name }`

   Where:

   - `{ address }` is the IP address of the remote server
   - `{ name }` is the name of the log selector identifier
3. Configure the following parameter(s) as required:

Parameter	Description
`negate`	Excludes messages defined in the **Remote Server Selector** fields from the log. Selecting this option acts as a logical NOT for the selector definition. For example: Selecting **same**, **debug**, and **mail** in the **Comparison**, **Level**, and **Facility-list** fields includes debug messages from the mail subsystem in the log. Selecting **Negate excludes** debug messages from the mail subsystem from the log.
`comparison { comparison }`	**Synopsis:** [same_or_higher | same] **Default:** same_or_higher The message severity levels to include in the log: • **same:** includes only messages of the severity level selected in the **Level** field. • **same_or_higher:** includes messages of the severity level selected in the **Level** field, and all messages of higher severity.

Parameter	Description
	For example: • Selecting **debug** in the **Level** field and **same** in the **Comparison** field includes only debug messages in the log. • Selecting **debug** in the **Level** field and **same_or_higher** in the **Comparison** field includes debug and all higher severity messages in the log.
`level { level }`	**Synopsis:** [emerg | alert | crit | err | warning | notice | info | debug | none | all] **Default:** all The base message severity level to include in the log. **all** includes all messages. **none** excludes all messages. Other levels are listed in order of increasing severity.
`facility-list { facility-list }`	**Synopsis:** [auth | authpriv | cron | daemon | ftp | kern | lpr | mail | news | security | syslog | user | uucp | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | all] The subsystems generating log messages. Messages from the selected subusystems are included in the log. At least one subsystem must be selected; up to 8 subsystems can be selected.

4. Type `commit` and press **Enter** to save the changes.

4.10.6.3 Deleting a Remote Server Selector

To delete a remote server selector, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the remote server selector by typing:

   ```
   no admin logging server { address } selector { name }
   ```

   Where:

   - `{ address }` is the IP address of the remote server
   - `{ name }` is the name of the log selector identifier
3. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

4.11 Managing the Software Configuration

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

4.11.1 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 161).

For information about backing up the software configuration manually, refer to "Saving the Configuration" (Page 106).

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

4.11.2 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

```
admin full-configuration-save format cli file-name { file
name }
```

Where:

- `{ filename }` is the name of the configuration file

Alternatively, to include only the default configuration parameter values in the saved configuration file, do the following:

1. Make sure the CLI is in Configuration mode.

2. Save the default values by typing:

   ```
   save { filename } | details
   ```

   Where:

   - `{ filename }` is the name of the configuration file

If required, once the configuration file has been saved, back it up to a USB mass storage drive. For more information, refer to "Backing Up Files" (Page 91).

Saving the Configuration to a USB Mass Storage Device

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

```
admin save-configuration-to-removable file-name { file name }
allow-overwrite [ true | false ]
```

Where:

- `{ file name }` is the name of the file
- `allow-overwrite { true }` will overwrite any file on the storage device that has the same file name as the new file

Note

If a file name is not defined, the configuration will be saved as **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 108).

4.11.3 Loading a Configuration

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

⚠ NOTICE

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 91).

   Note

   The `full-configuration-load` command is not supported in exclusive configuration mode.

2. Load the configuration file by typing:

   ```
   admin full-configuration-load format cli file-name { file
   name }
   ```

   Where:

   - `{ filename }` is the name of the configuration file
3. A confirmation message appears. Type **`yes`** to load the file or **`no`** to abort.

4.11.4 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.

4.11.4.1 Enabling/Disabling Automatic Configuration Loading

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

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the automatic configuration loading feature by typing:

   Enable

   ```
   admin automatic-config-load enabled
   ```

   Disable

   ```
   no admin automatic-config-load enabled
   ```
3. Type `commit` and press **Enter** to save the changes.

4.11.4.2 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 108).
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 106).
3. Copy the configuration file to the removable drive. For more information, refer to "Backing Up Files" (Page 91).

   ⚠ 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 RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 Installation Manual".
5. Reboot the target device. For more information about rebooting, refer to "Rebooting the Device" (Page 87).

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

4.11.4.3 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 108).

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 106).
2. Copy the configuration file to the removable drive. For more information, refer to "Backing Up Files" (Page 91).

3. Insert the USB Mass Storage drive into the USB port on the device. For more information, refer to the "RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 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 75).

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

4.11.4.4 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 RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 Installation Manual".
2. Enter the following command:

   ```
   admin delete-autoload-configuration-removable
   ```

   The file **autoload-config.cli** is removed from the storage device.

4.12 Managing Upgrade Servers

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

4.12.1 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/**

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.

4.12.2 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.

4.13 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 upgade 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.

4.13.1 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.

4.13.2 Upgrading/Downgrading Software

⚠ NOTICE

Restriction

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.

⚠ NOTICE

Upgrade/downgrade paths

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 "How to determine the software upgrade/downgrade path for a RUGGEDCOM ROX II device? [https://support.industry.siemens.com/cs/us/en/view/109806037]".

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.

4.13.2.1 Determining the Current Software Partition and Version

To determine which software partition is active and which version of RUGGEDCOM ROX II is running, enter the following command:

```
show admin rox-imaging partition-information
```

For example:

```
localhost# show admin rox-imaging partition-information
rox-imaging partition-information
 software partition "Partition #2"
 current version    "ROX 2.16.0 (2023-01-21 14:17)
```

The following information is displayed:

Parameter	Description
`software-partition`	**Synopsis:** A string up to 31 characters long The active partition. ROXflash is always peformed on the other partition.

Parameter	Description
`current-version`	**Synopsis:** A string up to 31 characters long The operating software version on the current software partition.

4.13.2.2 Obtaining a Software Release

Valid software releases are available online via Siemens Industry Online Support (SIOS) [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].

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/16008/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.

4.13.2.3 Stopping/Declining a Software Upgrade

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

⚠ NOTICE

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 123).

1. Make sure the CLI is in Configuration mode.
2. Rollback the software version by typing:

```
admin rox-imaging decline-upgrade
```

4.13.2.4 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 944).

---

1. Obtain the software package for the target release. For more information, refer to "Obtaining a Software Release" (Page 114).
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. Make sure the CLI is in Configuration mode.

   Note

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

   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 218).

   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. Start the software upgrade/downgrade using one of the following commands:

Command	Description

`admin rox-imaging software-upgrade url { URL }`	{ URL } is the URL for the software package in the form of:
	`protocol://user:password@host:port/path-to-file`
	Supported protocols include: http, https, ftp, ftps, usb
	For example:
	`http://webserver.local.lan/rr2/imagerr2.16.0-armhf.tar.bz2`

`wizard rox_upgrade`	This method requires user input to complete the upgrade. Follow the online instructions.
	When the upgrade process begins, the wizard displays the status of the upgrade. For example:
	`ruggedcom(config)# wizard rox_upgrade`
	`This wizard will install a ROXII image to the inactive partition along with the current configuration. On your`
	`next boot, that partition will become active and you will boot into the installed ROXII version.`
	`If the configuration cannot be upgraded the installation will abort. The current configuration may require to be modified to allow the installation and upgrade to complete.`
	`Do you wish to continue?(y/n): y`
	
	`Enter the url of the ROXII image. The following protocols are supported for file transfer: http, https, ftp, ftps, usb and sd.`
	`The url should take the form of protocol://user:password@host:port/path-to-file.`
	`If the server does not require authentication, you may leave out 'user:password@'. You may omit ':port' when using protocol's default port.`
	
	`Enter url: http://webserver.local.lan/rr2/imagerr2.16.0-armhf.tar.bz2`
	`Checking connectivity to server...`
	`apply failed: /rmf_admin:admin/rox-imaging: A roxflash is in progress. Configurations are locked until the next boot. To unlock, you must decline the upgrade after it completes.`
	`Performing validation of current config against image validation scripts ...`
	`Image ROX version is greater than the current ROX version.`
	`The image gpg signature is valid.`
	`Current configuration passed the validation scripts from the image.`

Command	Description
	Preparing partition #2 to be flashed... Flashing image to partition#2. Please do not discon nect from image source. progress: 100% Image flashed in 6 minutes 52 seconds. rox version:ROX 2.16.0 (2023-01-01 00:01) rc:0 Flashed image detected to be version ROX 2.16.0 (2023-01-01 00:01) Copying configuration to the target software parti tion ... Copying user files to the target software parti tion ... Finishing upgrade settings on the target software par tition. Completed the upgrade on the target software parti tion. The software upgrade was successful. A reboot is required to boot the other partition.

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 115)

6. When the software upgrade is complete, reboot the device.

   For more information about rebooting the device, refer to "Rebooting the Device" (Page 87).

4.13.2.5 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]".
- Make sure the system time and date are current. For more information, refer to "Configuring the System Time and Date" (Page 944).

---

1. Obtain the software package for the target release. For more information, refer to "Obtaining a Software Release" (Page 114).
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. Make sure the CLI is in Configuration mode.

   Note

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

   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 218).

   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. Start the software upgrade using one of the following commands:

Command	Description

`admin rox-imaging roxflash url { URL }`	{ URL } is the URL for the software package in the form of:
	`protocol://user:password@host:port/path-to-file`
	Supported protocols include: http, https, ftp, ftps, usb
	For example:
	`http://webserver.local.lan/rr2/imagerr2.16.0-armhf.tar.bz2`

`wizard rox_flash`	This method requires user input to complete the upgrade. Follow the online instructions.
	When the upgrade process begins, the wizard displays the status of the upgrade. For example:
	`ruggedcom(config)# wizard rox_upgrade`
	`This wizard will flash a ROXII image to the inactive partition.. On your`
	`next boot, that partition will become active and you will boot into the flashed ROXII version. Your configuration will not be transferred.`
	`Do you wish to continue?(y/n): y`
	
	`Enter the url of the ROXII image. The following protocols are supported for file transfer: http, https, ftp, ftps, usb and sd.`
	`The url should take the form of protocol://user:password@host:port/path-to-file.`
	`If the server does not require authentication, you may leave out 'user:password@'. You may omit ':port' when using protocol's default port.`
	
	`Enter url: http://webserver.local.lan/rr2/imagerr2.16.0-armhf.tar.bz2`
	
	`Checking connectivity to server...`
	`apply failed: /rmf_admin:admin/rox-imaging: A roxflash is in progress. Configurations are locked until the next boot. To unlock, you must decline the upgrade after it completes.`
	`Performing validation of current config against image validation scripts ...`
	`Image ROX version is greater than the current ROX version.`
	`The image gpg signature is valid.`
	`Current configuration passed the validation scripts from the image.`
	`Preparing partition #2 to be flashed...`
	`Flashing image to partition#2. Please do not disconnect from image source.`

Command	Description
	progress: 100% Image flashed in 6 minutes 52 seconds. rox version:ROX 2.16.0 (2023-01-01 00:01) rc:0 Flashed image detected to be version ROX 2.16.0 (2023-01-01 00:01) Copying configuration to the target software parti tion ... Copying user files to the target software parti tion ... Finishing upgrade settings on the target software par tition. Completed the upgrade on the target software parti tion. The software upgrade was successful. A reboot is required to boot the other partition.

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 115)

6. When the software upgrade is complete, reboot the device. For more information about rebooting the device, refer to "Rebooting the Device" (Page 87).

4.13.2.6 Downgrading Software

⚠ NOTICE

Restriction

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. Software packages (new and old) are available through Siemens Customer Support.

   For more information about obtaining a software release, refer to "Obtaining a Software Release" (Page 114).

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".

   Note

   For downgrades via HTTPS (SSL), a custom Certificate Authority (CA) must be configured on the device. For more information about adding a CA, refer to "Adding a CA Certificate and CRL" (Page 218).

   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.

3. Launch the ROXflash wizard by typing:

   ```
   wizard rox_flash
   ```

   The wizard will require user input to complete the upgrade. Follow the online instructions.

   When the downgrade process begins, the wizard displays the status of the downgrade. For example:

```
ruggedcom(config)# wizard rox_flash
This wizard will flash a ROXII image to the inactive partition. On your next
 boot, that partition
will become active and you will boot into the flashed ROXII version. Your con
figurations will not be transferred.
Do you wish to continue?(y/n): y


Enter the url of the ROXII image. The following protocols are supported: http,
 https, ftp, ftps, usb and sd.
The url should take the form of protocol://user:password@host/path-to-file.
If the server does not require authentication, you may leave out 'user:pass
word@'.

Enter url: ftp://user:12345@ftpserver.local.lan/debianppc/rr2/image/imager
r2.tar.bz2
Starting download of ROXII image...

######################################################################
 100.0%
Download complete.
Preparing partition #2 to be flashed...
Flashing image to partition#2...
progress: 100%
Flashed image detected to be version ROX 2 (2011-03-29 03:04)

The other partition was imaged successfully.
A reboot is required to boot the other partition.
```

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 115)

4. When the software upgrade is complete, reboot the device.

   For more information about rebooting the device, refer to "Rebooting the Device" (Page 87).

4.13.2.7 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. Make sure the CLI is in Configuration mode.
2. Rollback the software version by typing:

   ```
   admin rox-imaging rollback-reboot
   ```

   The device will automatically reboot. Once the reboot is complete, the previously inactive partition containing the older software version is changed to an active state.

4.13.2.8 Monitoring Software Upgrades/Downgrades

To monitor the real-time progress of an active software upgrade or downgrade, enter the following command:

```
show admin rox-imaging roxflash-progress
```

For example:

```
localhost# show admin rox-imaging roxflash-progress
rox-imaging roxflash-progress
 phase          Inactive
 status message ""
 image flashing 0
```

The following information is displayed:

Parameter	Description
`phase`	**Synopsis:** [Inactive | Downloading image | Imaging partition | Unknown state | Completed successfully | Failed | Validating database | Copying configuration | Declined | Imaging app] The current phase or state of the ROXflash operation. It is always one of the following: Inactive, Imaging partition, Unknown state,

Parameter	Description
	Completed successfully, or Failed. These phrases do not vary, and may be used programatically for ascertaining state.
`status-message`	**Synopsis:** A string up to 1024 characters long Detailed messages about ROXflash progress or errors.
`image-flashing`	**Synopsis:** An integer between 0 and 100 Indicates the imaging progress and the percentage that is complete.

4.14 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.

4.14.1 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. Make sure the CLI is in Configuration mode.
2. Enable or disable the boot time integrity check by typing:

   Enable

   ```
   admin boot-time-firmware-integrity-check
   ```

   Disable

   ```
   no admin boot-time-firmware-integrity-check
   ```

3. Type `commit` and press **Enter** to save the changes.

4.14.2 Checking the Firmware Integrity

To check the firmware integrity manually, type:

```
admin check-integrity
```

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

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

4.14.3 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 161).

4.14.4 Viewing the Status of the Firmware Integrity Check

To view the status of the last firmware integrity check, type:

```
show chassis chassis-status
```

For example:

```
ruggedcom# show chassis chassis-status
chassis-status
 model                      RX1501
 software license           "Layer 3 Security Edition"
 rox release                "ROX 2.12.0-QA1.9 (2018-01-26 12:58)"
```

```
 system serial number        RX1501R-0812-00664
 last integrity check        "2018-02-07 14:31"
 last integrity check result "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."
```

The following parameters detail the integrity check:

Parameter	Description
`last-integrity-check`	**Synopsis:** A string up to 32 characters long The last time the firmware integrity was checked.
`last-integrity-check-result`	**Synopsis:** A string The result of the last integrity check.

If the integrity check as 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 op
erating system files have been modified or tampered with. For assistance, contact
 Siemens Customer Support.
```

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, type:

```
show running-config chassis fixed-modules
```

If fixed modules have been configured, a table or list similar to the following example appears:

```
chassis
 fixed-modules
  fixed-module
SLOT  MODULE TYPE                                        PARTNUMBER
-------------------------------------------------------------------------
cm    RX1501 CM Horizontal 6 LM slots,Layer 3 switch  12-02-0029-003

 !
!
```

4.16 Managing Line Modules

RUGGEDCOM RX1500 series 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 86).
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. Make sure the CLI is in Configuration mode.
2. Set the module type to **none** by typing:

   ```
   chassis line-modules line-module { slot } module-type none
   ```

   Where { slot } is the name of the module location.
3. Type `commit` and press **Enter** to save the changes.
4. Insert the new line module into the empty slot in the chassis.
5. Reboot the device. For more information, refer to "Rebooting the Device" (Page 87).

   After the device is rebooted, the new line module is automatically detected and operational.
6. If the line module is different from the previous module installed in the same slot, add a configuration for the new line module. For more information, refer to "Configuring a Line Module" (Page 128).

4.16.3 Viewing a List of Line Module Configurations

To view a list of line module configurations, type:

```
show running-config chassis line-modules
```

If line modules have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config chassis line-modules | tab
chassis
 line-modules
  line-module
                                                      ADMIN    ADMIN
SLOT  MODULE TYPE                                     ENABLED  BYPASS
-------------------------------------------------------------------------
lm1   1000TX w/ 2x RJ45                               X        -
lm2   none                                            -        -
lm3   6x RS232/RS422/RS485 via RJ45                   X        -
lm4   E1 w/ 2x BNC                                    X        -
lm5   6x 100FX SFP Blank (no optical transceiver)     X        -
lm6   none                                            -        -

 !
!
```

If no line modules have been configured, install line module as needed. For more information, refer to "Installing a New Line Module" (Page 127).

4.16.4 Configuring a Line Module

To configure a line module, do the following:

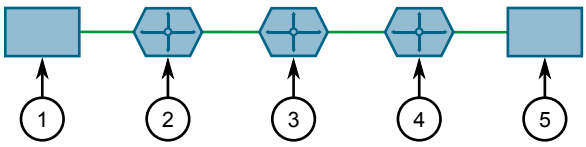
1. Make sure the CLI is in Configuration mode.
2. Navigate to ***chassis » line-modules » line-module » { module }***, where { module } is the line module.
3. Configure the following parameter(s) as required:

Parameter	Description
`detected-module`	**Synopsis:** A string up to 60 characters long The installed module's type specifier.
`module-type { module-type }`	**Synopsis:** A string up to 60 characters long Sets the module type to be used in this slot.
`admin-enabled`	Sets the administrative state for a module. Enabling the module powers it on.

4. Type `commit` and press **Enter** to save the changes.

4.16.5 Enabling/Disabling Controlled Bypass for M12 Line Modules

Controlled bypass is used to allow Ethernet traffic to bypass a defective unit in a network chain while preventing the loss of data.



① Ethernet Traffic Generator
② Router 1
③ Defective Router with M12 Bypass Control
④ Router 2
⑤ Ethernet Traffic Receiver

Figure 4.1 Sample Controlled Bypass Diagram

Note

An M12 line module with bypass control is required for this feature.

To enable or disable controlled bypass for M12 line modules, do the following:

1. Log in to the defective router.
2. Make sure the CLI is in Configuration mode.

   Note

   The default status is *not bypassed*. To view the current status, type:

   ```
   show chassis line-modules line-module { module } bypass
   ```

   Note

   After enabling bypass mode, LED on Port 1 and Port 2 of the M12 Line Module will turn yellow.

3. Enable or disable controlled bypass by typing:

   ```
   chassis line-modules line-module { module } bypass ad
   min-bypass
   ```

   Where:

   - `{ module }` is the M12 line module

4. Type `commit` and press **Enter** to save the changes.

Note

When controlled bypass is enabled, the bypass status changes automatically from *not bypassed* to *forced bypass*.

If controlled bypass is enabled, test the bypass control by doing the following:

1. Start sending Ethernet traffic from the traffic generator. The receiving side will receive traffic without any data loss.
2. Power down the defective router. The receiving side will receive the traffic without any data loss.

4.17 Managing SFP Transceivers

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].

⚠ 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 RX1500PN LMFG50 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 " (Page 132).

4.17.2 Viewing SFP Information

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

Note

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

```
ID: Unknown FF
```

```
interfaces switch { slot } { port } sfp
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

If an SFP transceiver exists in the selected port, details about the transceiver are displayed. For example:

```
ruggedcom# interfaces switch lm1 1 sfp
sfp-info-string
ID: SFP or SFP "Plus"
Extended ID: GBIC/SFP function is defined by serial ID only
Connector: LC
Transceiver:
      Ethernet Compliance: 100Base-FX
      10G Ethernet Compliance: Not specified
      Fibre Channel link length: Not specified
      Fibre Channel transmitter technology: Not specified
      SFP+ cable technology: Not specified
      Fibre Channel transmission media: Not specified
      Fibre Channel speed: Not specified
Baud Rate, nominal: 100 Mbps
Encoding type: 4B5B
Length(SMF): Not specified
Length(SMF): Not specified
Length(50um): 2000 m
Length(62.5um): 2000 m
Length(Copper): Not specified
Length(OM3): Not specified
Vendor: AVAGO
IEEE company ID: 8193
```

```
Part number:
Revision: O
Laser wavelength: 8224 nm
Options: Power Level (see SFF-8431) - level 2
         Linear Receiver Output implemented (see SFF-8431)
         Loss of Signal implemented, inverted (often called Signal Detect)
BRmax: 700 Mbps
BRmin: Not specified
Serial number:
Manufacturing date code: Y:AV M:AG D:O
Monitoring type: Digital diag monitoring - MUST be '1' but is '0'
                 Internally calibrated
                 Received power measurement type - OMA
Enhanced options: Soft TX_FAULT monitoring
SFF-8472 revision compliance: Unknown 20
```

4.17.3 Enabling/Disabling Smart SFP Mode

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 RX1500PN LMFG50 line module.

Note

To determine if an SFP transcever has been marked as *Unidentified*, refer to the **media** parameter under ***interfaces » switch » { slot } » { port }***, where { slot } is the slot number (e.g. lm1) and { port } is the port number of the switched Ethernet port. 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. Make sure the CLI is in Configuration mode.
2. Enable or disable Smart SFP mode by typing:

   Enable

   ```
   interface switch { slot } { port } sfp smart-sfp-mode
   ```

Disable

```
no interface switch lm{ slot } { port } sfp smart-sfp-mode
```

3. If Smart SFP mode is disabled, review the configuration for the SFP transceiver socket. Some settings may need to be adjusted manually to match the capabilities of the installed SFP transceiver. For more information, refer to "Configuring a Switched Ethernet Port" (Page 335).
4. Type `commit` and press **Enter** to save 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, type:

```
show running-config interface eth
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface eth
interface
 eth cm 1
  auton
  no proxyarp
  no on-demand
  no alias
  lldp
   no notify
  !
 !
!
```

4.18.2 Configuring a Routable Ethernet Port

To configure a routable Ethernet port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » eth » { interface }***, where { interface } is the routable Ethernet port.
3. Configure the port settings by configuring the following parameter(s):

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/Disables the network communications on this port.
`auton`	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.
`speed { speed }`	**Synopsis:** [10 | 100 | 1000] 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.
`duplex { duplex }`	**Synopsis:** [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 { link-alarms }`	**Synopsis:** [true | false] **Default:** 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-src { ip-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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.
`proxyarp`	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 { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface

4. Configure the LLDP settings by configuring the following parameter(s):

Parameter	Description
`admin-status { admin-status }`	**Synopsis:** [tx-only | rx-only | rx-tx | no-lldp] **Default:** rx-tx • no-lldp : The local LLDP agent can neither transmit nor receive LLDP frames. • rxTx : The local LLDP agent can both transmit and receive LLDP frames through the port. • txOnly : The local LLDP agent can only transmit LLDP frames. • rxOnly : The local LLDP agent can only receive LLDP frames.
`notify`	Disabling notifications will prevent sending notifications and generating alarms for a particular interface from the LLDP agent.

5. Add a VLAN ID (VID) for the port. For more information, refer to "Adding a VLAN to a Routable Ethernet Port" (Page 136).
6. Type `commit` and press **Enter** to save 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 either a routable Ethernet port or virtual switch, type:

```
show running-config interface { interface } vlan
```

Where:

- { interface } is the type of interface

If VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface eth vlan | tab
                IP
                ADDRESS  ON
SLOT  PORT  VID  SRC      DEMAND  QOS  INGRESS  MARK
-------------------------------------------------------
cm    1
            999  static   -

!
```

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 136).

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. Make sure the CLI is in Configuration mode.
2. Add the new VLAN by typing:

   ```
   interface eth { interface-name } vlan { id }
   ```

   Where:

   - `{ interface-name }` is the name of the interface
   - `{ id }` is the ID of the VLAN
3. Configure the following parameter(s) as required:

Parameter	Description
`ip-address-src { ip-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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.

4. Add a QoS map for the VLAN. For more information, refer to "Adding a QoS Map" (Page 919).
5. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.

2. Delete the traffic control rule by typing:

   ```
   no interface eth { name } vlan { id }
   ```

   Where:

   - `{ name }` is the name of the interface
   - `{ id }` is the ID of the VLAN

3. Type `commit` and press **Enter** to save the changes.

5 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin*** and configure the following parameter(s) as required:

Parameter	Description
`system-name { system-name }`	**Synopsis:** A string up to 255 characters long **Default:** System Name 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.
`location { location }`	**Synopsis:** A string up to 255 characters long **Default:** Location The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string.
`contact { contact }`	**Synopsis:** A string up to 255 characters long **Default:** Contact 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.

3. Type `commit` and press **Enter** to save the changes.

5.2 Configuring the Host Name

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

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » hostname*** and configure the following parameter(s) as required:

⚠ NOTICE
Special characters (i.e. !@#$%^&*()_+-={}[];:',<.>/?|`~) are not permitted in host names.

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

3. Type `commit` and press **Enter** to save 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.

To add a custom welcome message, type:

```
admin authentication banner { message }
```

Where:

- `{ message }` is the custom welcome message

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. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » session-limits*** and configure the following parameter(s) as required:

Parameter	Description
`max-sessions-total { max-sessions-total }`	**Synopsis:** An integer **Default:** 70 Puts a limit on the total number of concurrent sessions to ROX.

3. Type `commit` and press **Enter** to save the changes.

5.5 Enabling and Configuring WWW Interface Sessions

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

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » webui*** and configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Provides the ability to configure WebUI features on the device.
`listen-ip { listen-ip }`	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address the CLI will listen on for WebUI requests.
`port { port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 443 The port on which the WebUI listens for WebUI requests.
`extra-ip-ports { extra-ip-ports }`	**Synopsis:** A string 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.
`max-sessions { max-sessions }`	**Synopsis:** An integer **Default:** 20 The maximum number of concurrent WebUI sessions
`idle-timeout { idle-timeout }`	**Synopsis:** A string **Default:** PT30M 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.
`ssl-redirect-enabled { ssl-redirect-enabled }`	**Synopsis:** [true | false] **Default:** true Redirects traffic from port 80 to port 443. If disabled, port 80 will be closed.

Parameter	Description
`client-certificate-verification { client-certificate-verification }`	**Synopsis:** [none | peer | fail-if-no-peer-cert] **Default:** none Level of verification the server does on client certificates • none - It does not do any verification. • peer - The server will ask the client for a client-certificate but not fail if the client does not supply a client-certificate. • fail-if-no-peer-cert - The server requires the client to supply a client certificate.

3. Type `commit` and press **Enter** to save 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 713).
2. Make sure the CLI is in Configuration mode.
3. Enable remote administration for the desired VRF definition by typing:

   ```
   global vrf definition { name } remote-administration enabled
   ```

   Where { name } is the name of the VRF definition
4. Configure the following parameters:

   Note

   The parameters **snmp-enabled** 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 875).

Parameter	Description
`webui-enabled { webui-enabled }`	**Synopsis:** [true | false] **Default:** true Enables access to the Web user interface over the VRF interface.
`webui-listen-port { webui-listen-port }`	**Synopsis:** An integer between 1 and 65535 **Default:** 443 The port the Web user interface will listen on for incoming connections over a VRF interface.
`cli-enabled { cli-enabled }`	**Synopsis:** [true | false] **Default:** true Enables access to the CLI over the VRF interface.
`cli-listen-port { cli-listen-port }`	**Synopsis:** An integer between 1 and 65535 **Default:** 22 The port the CLI will listen on for incoming connections over a VRF interface.
`snmp-enabled { snmp-enabled }`	**Synopsis:** [true | false] **Default:** true Enables SNMP access over the VRF interface.
`snmp-listen-port { snmp-listen-port }`	**Synopsis:** An integer between 1 and 65535 **Default:** 161 The port SNMP will listen on for incoming connections over a VRF interface.

5. Type `commit` and press **Enter** to save 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 875).

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 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 149).

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.

Name	Severity	Description	Suggested Resolution
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 (For RX1500 and RX1510 Only)	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 (For RX1500 and RX1510 Only)	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.
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		

Name	Severity	Description	Suggested Resolution
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.
Brute Force Attack	Alert	A brute force attack has been attempted.	Review the **Auth.log** 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 166).
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 alarms for a specific alarm type, type:

```
show admin alarms
```

A table or list similar to the following example appears:

```
ruggedcom# show admin alarms | tab
           ALARM  EVENT
SUBSYSTEM  ID     ID     SEVERITY  DESCRIPTION           DATE TIME                USER ACTIONS  AC
TUATORS
-------------------------------------------------------------------------------------------
switch     1      1      notice    Link-up on port lm1/8  Wed Feb  6 16:08:44 2013  clear-or-ack
 none
```

For information on how to clear or acknowledge an active alarm, refer to "Clearing and Acknowledging Alarms" (Page 147).

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, type:

```
admin clear-all-alarms
```

Alternatively, to clear an individual non-conditional alarm, type:

```
admin alarms active-alarms subsystem [ admin | cellmodem |
chassis | eth | services | security | switch | wan ] { id }
{ event } clear
```

Where:

- `{ id }` is the ID for the chosen alarm
- `{ event }` is the ID for the chosen event

5.7.3.2 Acknowledging Alarms

To acknowledge all active alarms, type:

```
admin acknowledge-all-alarms
```

Alternatively, to acknowledge an individual alarm, type:

```
admin alarms active-alarms { type } { id } { event } acknowl
edge
```

Where:

- `{ type }` is the type of alarm. Options include **admin**, **cellmodem**, **chassis**, **eth**, **security**, **switch**, and **wan**.
- `{ id }` is the ID for the chosen alarm.
- `{ event }` is the ID for the chosen event.

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. Make sure the CLI is in Configuration mode.

2. Configure the alarm by typing:

```
admin alarm-config subsystem [ admin | cellmodem | chassis
| eth | services | security | switch | wan ] alarm-list
{ id }
```

Where { id } is the ID for the chosen alarm.

3. Configure the following parameters as required:

Note

Depending on the alarm type, some parameters are not available.

Note

Alarm descriptions are not configurable.

Parameter	Description
`severity { severity }`	**Synopsis:** [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.

4. Type `commit` and press **Enter** to save 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 148).

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

Group	Name	Level	Failrelay Enable	LED Enable	User Configurable	Trap	Log
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	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
WAN	Link Up	Notice	---	---	Yes	No	Yes
WAN	Link Down	Warning	Enabled	Enabled	Yes	Yes	Yes
WAN	Internal Configuration Error	Alert	Enabled	Enabled	Yes	No	Yes
WAN	DS1 Line Status Change	Alert	Enabled	Enabled	Yes	No	Yes
Cellmodem	Link Up	Notice	---	---	Yes	Yes	Yes
Cellmodem	Link Down	Warning	Enabled	Enabled	Yes	Yes	Yes
Cellmodem	Internal Configuration Error	Alert	Enabled	Enabled	Yes	No	Yes
Cellmodem	Firmware update failure	Warning	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	×	✓	✓
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 155).

5.8.1 Viewing a List of Users

To view a list of user accounts, type:

```
show running-config admin users
```

If users have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin users | tab
admin
 users
  userid
NAME   PASSWORD                                ROLE
-----------------------------------------------------------
admin  $1$LmRO$j7/q/wtlwjfUvbOVrbt4o.   administrator
guest  $1$uGztU0$6b7YS6gqwtrelTzA/2noQ. guest
oper   $1$eSsFfFMh$NEHgTHsU1T4RRz8sXNV2F1  operator
```

If no user accounts have been configured, add user accounts as needed. For more information, refer to "Adding a User" (Page 152).

5.8.2 Adding a User

To add a new user account, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the user account by typing:

   ```
   admin users userid { name } role { role }
   ```

   Where:

   - `{ name }` is the name of the user account
   - `{ role }` is the role of the user. The options are `administrator`, `operator`, and `guest`.
3. To set the user password, follow the instructions in "Setting a User Password/ Passphrase" (Page 155).
4. Type `commit` and press **Enter** to save the changes.
5. [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 181).

5.8.3 Deleting a User

To delete a user account, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the user account by typing:

   ```
   no admin users userid { name }
   ```

   Where:

   - `{ name }` is the name of the user account.
3. Type `commit` and press **Enter** to save the changes.

5.8.4 Monitoring Users

Users currently logged in to the device are monitored by RUGGEDCOM ROX II and can be viewed through the CLI. 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, type:

```
who
```

A table or list similar to the following appears:

```
ruggedcom# who
Session User  Context From          Proto Date     Mode
```

```
*147    admin cli     192.168.0.200 ssh   11:04:54 operational
 145    admin webui   192.168.0.200 https 10:51:05 operational
```

5.8.4.1 Logging Out Users from a Session

To log a user out of the device, type:

Type:

```
logout [ [ session | { number } ] [ user | { profile } ] ]
```

Where:

- `{ number }` is the session number
- `{ profile }` is the name of the user profile

5.8.4.2 Sending Messages to Users

To broadcast a message to all users or a specific user, type:

```
send [ { profile } | all ] { message }
```

Where:

- `{ profile }` is the name of the user profile
- `{ message }` is the message

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 25).

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 184) and "Configuring TACACS+ Authentication" (Page 188).

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

To prevent unauthorized access to the device, change the default passwords before commissioning the device.

⚠ NOTICE

Accessibility hazard – risk of data loss

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. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » authentication » password-complexity*** and configure the following parameter(s) as required:

Parameter	Description
`minimum-length { minimum-length }`	**Synopsis:** An integer between 1 and 128 **Default:** 12 Minimum password length.

Parameter	Description
`maximum-length { maximum-length }`	**Synopsis:** An integer between 1 and 128 **Default:** 128 Maximum password length.
`uppercase-required { uppercase-required }`	**Synopsis:** [true | false] **Default:** true Requires the password to have at least one uppercase letter.
`lowercase-required { lowercase-required }`	**Synopsis:** [true | false] **Default:** true Requires the password to have at least one lowercase letter.
`digits-required { digits-required }`	**Synopsis:** [true | false] **Default:** true Requires the password to have at least one numerical digit.
`special-characters-required { special-characters-required }`	**Synopsis:** [true | false] **Default:** true Requires the password to have at least one non-alphanumeric character. Allowed characters include "!@#$%^&*()_+-={}[];:',<.>/?|`~".

3. Type `commit` and press **Enter** to save 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: !@#$%^&*()_+-={}[];:',<.>/?\|`~.

1. Type the following command and then press **Enter**:

   ```
   admin users userid { profile } set-password new-password
   ```

   Where `{ profile }` is the user profile (e.g. admin, oper or guest)

2. At the prompt, type the new password/passphrase and then press **Enter**.

   ```
   Value for 'new-password' (<string, min: 1 chars, max: 128 chars>):
   ```

3. At the next prompt, type the new password/passphrase again and then press **Enter**.

   ```
   Value for 'new-password-repeat' (<string, min: 1 chars, max: 128 chars>):
   ```

The password/passphrase is updated and the following message appears if the password/passphrase complies with the password complexity rules:

```
set-password-result success
```

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 "Accessing Different CLI Modes" (Page 31).

⚠ 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]" available on https://www.siemens.com.

To set the boot password/passphrase, do the following:

1. Issue the following command:

   ```
   admin authentication set-boot-password new-password
   ```

2. At the first prompt, type the new password/passphrase and then press **Enter**.
3. At the second prompt, type the new password/passphrase again and then press **Enter**.
4. At the third prompt, type the old password/passphrase and then press **Enter**. If this is the first time the boot password/passphrase is being set, only press **Enter**.

Example:

```
ruggedcom(config)# admin authentication set-boot-password new-password
Value for 'new-password' (<string, min: 0 chars, max: 128 chars>): ***************
Value for 'new-password-repeat' (<string, min: 0 chars, max: 128 chars>):
 ***************
Value for 'old-password' (<string, min: 0 chars, max: 128 chars>): ***************
set-password-result success
```

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 "Accessing Different CLI Modes" (Page 31).

⚠ NOTICE

Configuration hazard – risk of data corruption

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. Set the maintenance password/passphrase by typing:

   ```
   admin authentication set-maint-password new-password
   ```

2. At the first prompt, type the new password/passphrase and then press **Enter**.
3. At the second prompt, type the new password/passphrase again and then press **Enter**.
4. At the third prompt, type the old password/passphrase and then press **Enter**. If this is the first time the boot password/passphrase is being set, only press **Enter**.

Example:

```
ruggedcom(config)# admin authentication set-maint-password new-password
Value for 'new-password' (<string, min: 0 chars, max: 128 chars>): ***************
Value for 'new-password-repeat' (<string, min: 0 chars, max: 128 chars>):
 ***************
Value for 'old-password' (<string, min: 0 chars, max: 128 chars>): ***************
set-password-result success
```

5.9.5 Resetting the Admin Password/Passphrase

The admin password/passphrase provides access to the Web Interface and Command Line Interface (CLI). If this password is lost, access to these interfaces is impossible until the password/passphrase is reset directly on the device.

Note

The admin password/passphrase must be reset on both partitions.

To reset the admin password/passphrase, do the following:

1. Enter service mode. For more information, refer to "Accessing Service Mode" (Page 67).
2. Type `root` and press **Enter**. The password prompt appears.
3. Type the password/passphrase associated with the root profile and press **Enter**. The default password is *admin*.

4. Type `confd_cli` and press **Enter**.
5. Enable autowizard by typing:

   ```
   autowizard true
   ```

6. Type `config` and press **Enter**.

   ⚠ NOTICE

   Passwords/passphrases that contain special characters, including spaces, must be wrapped in quotes (e.g. "password!2#").

7. Reset the admin password/passphrase by typing:

   ```
   admin users userid admin set-password new-password { new-
   password-passphrase } new-password-repeat { new-pass
   word-passphrase }
   ```

   If special characters are used, make sure to encapsulate the password in double-quotation marks (") as follows:

   Note

   RUGGEDCOM ROX II supports the following special characters in passwords/passphrases: !@#$%^&*()_+-={}[];:',<.>/?\|`~.

   ```
   admin users userid admin set-password new-password { new-
   password-passphrase } new-password-repeat { new-pass
   word-passphrase }
   ```

   Where:

   - `{ new-password-passphrase }` is the new password/passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.

8. Reboot the device. For more information, refer to "Rebooting the Device" (Page 87).
9. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
```

```
'h' Show this help menu
'l' List the available boot targets
'c' Exit to the boot loader command line

Will reboot after 60 seconds of inactivity
:
```

Note

In the example above, the text `Auto booting [4-0]` indicates the active partition is Boot Partition 4.

10. Enter the inactive partition by typing the associated target number. For example, if the active partition is Boot Partition 4, type `6-0` and press **Enter** to enter Boot Partition 6.
11. Repeat step 1 (Page 157) and step 10 (Page 159) to reset the password/passphrase on the inactive partition and switch back to the original partition.

5.9.6 Resetting the Boot Password/Passphrase

The boot password/passphrase provides access to BIST mode (through the `maint-login` command) and service mode. If this password/passphrase is lost, access to these modes is impossible until the password/passphrase is reset directly on the device.

To reset the boot password/passphrase, do the following:

1. Log in to maintenance mode. For more information, refer to "Accessing Maintenance Mode" (Page 69).
2. Delete current boot password/passphrase by typing:

   ```
   rox-delete-bootpwd --force
   ```

3. Type `exit` and press **Enter**.
4. Set a new boot password/passphrase. For more information, refer to "Setting the Boot Password/Passphrase" (Page 156).

5.9.7 Resetting the Maintenance Password/Passphrase

The maintenance password/passphrase grants access to the maintenance mode. If this password/passphrase is lost, access to this mode is impossible until the password/passphrase is reset directly on the device.

⚠ 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.

Note

The maintenance password/passphrase must be reset on both partitions.

To reset the maintenance password/passphrase, do the following:

1. Make sure the CLI is in Configuration mode.
2. Reset the maintenance password by setting a new password. For more information, refer to "Setting the Maintenance Password/ Passphrase" (Page 157).
3. Reboot the device. For more information, refer to "Rebooting the Device" (Page 87).
4. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
 'h' Show this help menu
 'l' List the available boot targets
 'c' Exit to the boot loader command line

 Will reboot after 60 seconds of inactivity
 :
```

Note

In the example above, the text `Auto booting [4-0]` indicates the active partition is Boot Partition 4.

5. Enter the inactive partition by typing the associated target number. For example, if the active partition is Boot Partition 4, type `6-0` and press **Enter** to enter Boot Partition 6.
6. Log in to RUGGEDCOM ROX II. For more information about logging in to RUGGEDCOM ROX II, refer to "Logging In" (Page 25).
7. Repeat step 1 (Page 160) and step 5 (Page 160) to reset the password/ passphrase on the inactive partition and switch back to the original partition.

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, type:

```
show running-config admin scheduler
```

If jobs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin scheduler | tab
admin
 scheduler
  scheduled-jobs
                                          JOB          JOB
SCHEDULER JOB               JOB     JOB   DAY    JOB   DAY
NAME              JOB TYPE  MINUTE  HOUR  MONTH  MONTH WEEK    JOB COMMAND
-------------------------------------------------------------------------------
Backup            periodic  1       -     -      -     Monday  backupconfig
Clear Message Log periodic  5       5:00  1      1     Monday  clearmessagelog
```

If no jobs have been configured, add jobs as needed. For more information, refer to "Adding a Scheduled Job" (Page 161).

5.10.2 Adding a Scheduled Job

To add a scheduled job, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » scheduler***.
3. Configure the following parameter(s) as required:

Parameter	Description
`{ scheduler-job-name }`	**Synopsis:** A string up to 64 characters long The name of the scheduled job. The name can be up to 64 characters in length.
`job-type { job-type }`	**Synopsis:** [configchange | periodic] **Default:** periodic Determines when to launch the scheduled job:

Parameter	Description
	• periodic: The job launches at a set date and time. • configchange: The job launches when the configuration changes.
`job-minute { job-minute }`	**Synopsis:** A string up to 128 characters long **Default:** 0 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. • To specify a single value, enter the value in the field. For example, to launch the job 10 minutes past the hour, enter 10. • 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. • 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. This parameter is not required for configchange jobs.
`job-hour { job-hour }`	**Synopsis:** A string up to 64 characters long 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. • To specify a single value, enter the value in the field. For example, to launch the job at 5:00 pm, enter 17. • 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. • 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. This parameter is not required for configchange jobs.
`job-day-month { job-day-month }`	**Synopsis:** A string up to 64 characters long 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. • 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. • 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. • 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.

Parameter	Description
	This parameter is not required for configchange jobs.
`job-month { job-month }`	**Synopsis:** A string up to 32 characters long For periodic jobs, sets the month in which to run the scheduled job. Valid values are in the rage of 1 to 12. If no value is set, the job launches every day. • To specify a single value, enter the value in the field. For example, to set the month to February, enter 2. • 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. • 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. This parameter is not required for configchange jobs.
`job-day-week { job-day-week }`	**Synopsis:** A string up to 16 characters long 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. • To specify a single value, enter the value in the field. For example, to set the day to Monday, enter 1. • 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. • 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. This parameter is not required for configchange jobs.
`job-command { job-command }`	**Synopsis:** A string up to 1024 characters long 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. Do not use interactive commands or commands that require a manual response or confirmation. 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.

4. Type `commit` and press **Enter** to save the changes.

5.10.3 Deleting a Scheduled Job

To delete a scheduled Job, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the scheduled job by typing:

   ```
   no admin scheduler schedule-jobs { name }
   ```

   Where:

   - `{ name }` is the name of the scheduled job
3. Type `commit` and press **Enter** to save the changes.

6 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » cli*** and configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true 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.
`listen-ip { listen-ip }`	**Synopsis:** A string **Default:** 0.0.0.0 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.
`port { port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 22 The default port on which the CLI will listen for requests from the device. The port corresponds with the IP address specified by the **Listen IP (listen-ip)** parameter.
`extra-ip-ports { extra-ip-ports }`	**Synopsis:** A string 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]). If the **Listen IP (listen-ip)** parameter is set to a value other than **0.0.0.0**, the port specified by the **Listen Port (port)** parameter must not be associated with any additional addresses.

Parameter	Description
`max-sessions { max-sessions }`	**Synopsis:** An integer **Default:** 10 The maximum number of concurrent CLI sessions.
`idle-timeout { idle-timeout }`	**Synopsis:** A string **Default:** PT30M 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). 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.
`greeting { greeting }`	**Synopsis:** A string between 1 and 8192 characters long A greeting message presented to users when they log in to the CLI. The message must be enclosed in quotation marks.

3. Type `commit` and press **Enter** to save 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 Protec
tion
```

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 93).

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.

```
ruggedcom# show admin alarms active-alarms | tab
           ALARM  EVENT
SUBSYSTEM  ID     ID     SEVERITY  DESCRIPTION
--------------------------------------------------------------------------------
security   2      1      alert     BFA from IP 172.30.151.141 is blocked
```

To enable/disable the BFA protection mechanism, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable the BFA protection mechanism by typing:

   ```
   security bruteforce enabled
   ```

   Or disable the BFA protection mechanism by typing:

   ```
   no security bruteforce enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

4. [Optional] Enable or disable the default alarm for brute force attacks. For more information, refer to "Configuring an Alarm" (Page 148).

6.3 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. Make sure the CLI is in Configuration mode.
2. Enable SYN cookies by typing:

   ```
   admin system tcp-syn-cookies
   ```

   Disable SYN cookies by typing:

   ```
   no admin system tcp-syn-cookies
   ```

3. Type `commit` and press **Enter** to save the changes.

6.4 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 1054).

6.4.1 Viewing Active SSH Server Algorithms

To view which algorithms are currently enabled for the SSH server, do the following:

1. Make sure the CLI is in Configuration mode.
2. 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
 !
!
```

6.4.2 Enabling SSH Server and NETCONF Algorithms

To enable an algorithm for the SSH server and NETCONF, do the following:

1. Make sure the CLI is in Configuration mode.
2. 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 1054).
3. 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.
4. Enter `top` to return to the top level of the command hierarchy.
5. 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
```

6.4.3 Enabling TLS Algorithms

To enable an algorithm for TLS, do the following:

1. Make sure the CLI is in Configuration mode.
2. 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 1054).
3. 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.
4. 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
```

6.4.4 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. Make sure the CLI is in Configuration mode.
2. 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.
3. Commit the change.

Setting the Maximal Key Length

To set the maximal key length, do the following:

1. Make sure the CLI is in Configuration mode.
2. 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.
3. Commit the change.

6.5 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.

6.5.1 Enabling and Configuring SFTP Sessions

To enable and configure SFTP server functionality, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » sftp*** and configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false When enabled, a Secure File Transfer Protocol (SFTP) server may be used to transfer files to and from the device.
`listen-ip { listen-ip }`	**Synopsis:** A string **Default:** 0.0.0.0 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
`port { port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 2222 A port on which the SFTP server will listen for requests from clients.
`extra-ip-ports { extra-ip-ports }`	**Synopsis:** A string 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]). If the **Listen IP (listen ip)** parameter is set to a value other than 0.0.0.0, the port specified by the **Listen Port (port)** parameter must not be associated with any additional addresses.
`max-sessions { max-sessions }`	**Synopsis:** An integer **Default:** 10

3. Add the private key from the SFTP server to the device. For more information, refer to "Adding a Private Key" (Page 220).
4. Type `commit` and press **Enter** to save the changes.

6.5.2 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 226).

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 222).
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 227).

6.6 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.

6.6.1 Port Security Concepts

This section describes some of the concepts important to the implementation of port security in RUGGEDCOM ROX II.

6.6.1.1 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.

6.6.1.2 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 851).

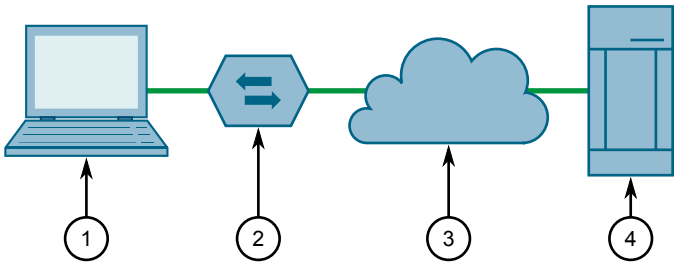
For information about configuring a static MAC address, refer to "Adding a Static MAC Address" (Page 358).

6.6.1.3 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 187).

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.

6.6.1.4 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.

6.6.1.5 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.

6.6.2 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 335).

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » switch » { slot } » { port } » port-security***, where { slot } is the module and { port } is the switched Ethernet port.
3. Configure the port security settings by configuring 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.

   Note

   The parameter **quarantine-vid** is only available when **security-mode** is set to either **dot1x** or **dot1x_max_auth**.

   The parameter **guest-vid** is only available when **security-mode** is set to **dot1x**.

Parameter	Description
`security-mode { security-mode }`	**Synopsis:** [dot1x_mac_auth | dot1x | per_macaddress | off] **Default:** off The security mode for the port. Options include: • **dot1x_mac_auth** - 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. • **dot1x** - 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. • **per_macaddress** - Only packets from authorized MAC addresses are forwarded. Authorized MAC addresses are either preconfigured in the static MAC address table or learned dynamically. • **off** - Disables security on the port
`quarantine-vid { quarantine-vid }`	**Synopsis:** An integer between 1 and 4094 The VLAN identifier for the Quarantine VLAN.

Parameter	Description
	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.
`guest-vid { guest-vid }`	**Synopsis:** An integer between 1 and 4094 The VLAN identifier for the Guest VLAN. 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.
`auto-learn { auto-learn }`	**Synopsis:** An integer between 0 and 16 **Default:** 0 The maximum number of MAC addresses that can be learned dynamically by the port. This includes static MAC addresses defined in the **Static MAC Address** table. Therefore, the actual number of learned MAC addresses is this number minus the number of addresses defined in the **Static MAC Address** table. **Security Mode** must be set to either **per_macaddress** or **dot1x_mac_auth**.
`shutdown-time { shutdown-time }`	**Synopsis:** An integer between 1 and 86400 The time in seconds (s) the port will be disabled if a security violation occurs. **Shutdown Enable** must be enabled.
`admin-shutdown`	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 **Shutdown Time**.

4. Configure the IEEE 802.1x settings by configuring the following parameter(s) as required:

Parameter	Description
`tx-period { tx-period }`	**Synopsis:** An integer between 1 and 65535 **Default:** 30 The maximum time in seconds (s) allowed for one full set of packets to be transferred between the port and its client.
`quiet-period { quiet-period }`	**Synopsis:** An integer between 0 and 65535 **Default:** 60 The time in seconds (s) to wait before retransmitting EAPoL packets to the client after a failed authentication session.
`reauth-enable`	When enabled, the port will attempt to reauthenticate the client periodically. The period of time between each reauthentication attempt is specified by **Reauthentication Period**. The port is considered unauthorized when the maximum number of reauthentication attempts (as defined by **Reauthentication Max Attempts**) is exceeded.

Parameter	Description
`reauth-period { reauth-period }`	**Synopsis:** An integer between 60 and 86400 **Default:** 3600 The period of time in seconds (s) the port will wait before attempting to reauthenticate the client. **Reauthentication** must be enabled.
`reauth-max { reauth-max }`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The maximum number of unsuccessful reauthentication attempts allowed, after which the client is considered unauthorized. **Reauthentication** must be enabled.
`supp-timeout { supp-timeout }`	**Synopsis:** An integer between 1 and 300 **Default:** 30 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.
`server-timeout { server-timeout }`	**Synopsis:** An integer between 1 and 300 **Default:** 30 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.
`max-request { max-request }`	**Synopsis:** An integer between 1 and 10 **Default:** 2 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.

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 187).
6. Type `commit` and press **Enter** to save the changes.

6.6.3 Viewing the Security Status of Switched Ethernet Ports

To view the port security status of all switched Ethernet ports, type:

```
show interfaces switch { slot } port-security
```

Where { slot } is the name of the module location. For example:

```
ruggedcom# show interfaces switch lm1 port-security
SLOT  PORT  STATUS
----------------------
lm1   1     Unsecure
lm1   2     Unsecure
```

To view the port security status of a specific switched Ethernet port, type:

```
show interfaces switch { slot } { port } port-security
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

For example:

```
show interfaces switch lm1 1 port-security
port-security
 status Unsecure
```

6.7 Managing User Authentication

This section describes the various methods for authenticating users.

6.7.1 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.

⚠ NOTICE

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, type:

```
admin authentication mode [ localonly | radius_local | ra
dius_only | radius_then_local | tacacsplus_local | tacac
splus_only ]
```

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 availabled, 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, 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.

6.7.2 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.

6.7.2.1 Determining Which Keys are Associated to a User

To list the user authentication keys associated with a user account, type:

```
show runnging-config admin users userid { name } autho
rized-keys
```

A list similar to the following appears:

```
ruggedcom# show running-config admin users userid admin authorized-keys
```

```
admin
 users
  userid admin
   authorized-keys keyid key1
   !
  !
 !
!
```

For information about associating keys with user accounts, refer to "Associating/ Disassociating a User Authentication Key" (Page 183).

6.7.2.2 Adding a User Authentication Key

To add a user authentication key to the device, do the following:

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

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 by typing
2. Open the public key and copy its contents.
3. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 25).
4. Make sure the CLI is in Configuration mode.
5. Define the new authentication key by typing:

   ```
   security crypto authorized-keys { key }
   ```

   Where { key } is a name assigned to the authentication key for easy identification.
6. Type `contents` and then press **Enter** to enter multi-line mode.
7. Insert the contents of the public key and then press **Ctrl-D**. For example:

   ```
   ruggedcom(config)# security crypto authorized-keys key1 contents
   (<string, min: 1 chars, max: 2048 chars>):
   [Multiline mode, exit with ctrl-D.]
   ```

```
>{--contents--}
```

8. Type `commit` and press **Enter** to save the changes.
9. Associate the new authentication key with one or more user accounts. For more information, refer to "Associating/Disassociating a User Authentication Key" (Page 183).

6.7.2.3 Deleting a User Authentication Key

To delete a user authentication key from the device, do the following::

1. Make sure the CLI is in Configuration mode.
2. Disassociate the chosen authentication key from the associated user account(s). For more information, refer to "Associating/Disassociating a User Authentication Key" (Page 183).
3. Delete the authentication key by typing:

   ```
   no security crypto authorized-keys { key }
   ```

   Where { key } is the name assigned to the authentication key for easy identification.
4. Type `commit` and press **Enter** to save the changes.

6.7.2.4 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. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 25).
2. Make sure the CLI is in Configuration mode.
3. Associate an authentication key with the desired user profile by typing:

   ```
   admin users name { name } authorized-keys key-id { key }
   ```

   Where:

   - { name } is the name of the user account

- { key } is the name assigned to the authentication key

4. Type `commit` and press **Enter** to save the changes.

Disassociating an Authentication Key

To disassociate one of the authentication keys from a user account, do the following:

1. Log in to RUGGEDCOM ROX II. For more information, refer to "Logging In" (Page 25).
2. Make sure the CLI is in Configuration mode.
3. Disassociate the desired authentication key from the desired user profile by typing:

```
no admin users name { name } authorized-keys key-id
{ key }
```

Where:

- { name } is the name of the user account
- { key } is the name assigned to the authentication key

4. Type `commit` and press **Enter** to save the changes.

6.7.3 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].

For more information about the Extensible Authentication Protocol (EAP), refer to RFC 3748 [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 180).

⚠ 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	**Vendor-ID** – 15004 **Type** – 1 **Length** – 11 **String** – 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[a]	{ A message(s) received from the authenticating peer }

[a] EAP-Message is an extension attribute for RADIUS, as defined by RFC 2869 [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/negate 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 93).

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.

6.7.3.1 Configuring RADIUS Authentication for LOGIN Services

To configure RADIUS authentication for LOGIN services, do the following:

⚠ **NOTICE**
Passwords are case-sensitive.

1. Make sure the CLI is in Configuration mode.
2. Type the following:

   ```
   admin authentication radius
   ```

3. [Optional] If port security is enabled on any ports, configuring the following parameter(s) to avoid conflicts with firewall rules/policies:

Parameter	Description
`nas-ip-address { nas-ip-address }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The NAS-IP-Address. Set this to the primary IP address of the unit.
`nas-identifier { nas-identifier }`	**Synopsis:** A string up to 64 characters long The NAS-Identifier. If not set, the hostname will be used as the NAS-Identifier.

4. Configure the primary or secondary RADIUS server by typing either `primary` or `secondary` and configuring the following parameter(s) as required:

Parameter	Description
`address { address }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The IP address of the server.
`port-udp { port-udp }`	**Synopsis:** An integer between 1 and 65535 **Default:** 1812 The network port of the server.

Parameter	Description
`password { password }`	**Synopsis:** A string The password of the RADIUS server.

5. Type `commit` and press **Enter** to save the changes.

6.7.3.2 Configuring RADIUS Authentication for PPP Services

To configure RADIUS authentication for PPP services, do the following:

⚠ NOTICE

Passwords are case-sensitive.

1. Make sure the CLI is in Configuration mode.
2. Type the following:

   ```
   global ppp radius
   ```

3. Configure the primary or secondary RADIUS server by typing either `primary` or `secondary` and configuring the following parameter(s) as required:

Parameter	Description
`address { address }`	**Synopsis:** A string between 7 and 15 characters long The IPv4 address of the server.
`port-udp { port-udp }`	**Synopsis:** An integer between 1 and 65535 **Default:** 1812
`password { password }`	**Synopsis:** A string

4. Type `commit` and press **Enter** to save the changes.

6.7.3.3 Configuring RADIUS Authentication for Switched Ethernet Ports

To configure RADIUS authentication for switched Ethernet ports, do the following:

⚠ NOTICE

Passwords are case-sensitive.

1. Make sure the CLI is in Configuration mode.
2. Type the following:

   ```
   switch port-security radius
   ```

3. Configure the primary or secondary RADIUS server by typing either `primary` or `secondary` and configuring the following parameter(s) as required:

Parameter	Description
`address { address }`	**Synopsis:** A string between 7 and 15 characters long The IPv4 address of the server.
`port-udp { port-udp }`	**Synopsis:** An integer between 1 and 65535 **Default:** 1812 The IPv4 port of the server.
`password { password }`	**Synopsis:** A string The password of the server

4. Type `commit` and press **Enter** to save the changes.

6.7.4 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 180).

To configure TACACS+ authentication, do the following:

⚠ NOTICE

Passwords are case-sensitive.

1. Make sure the CLI is in Configuration mode.
2. Type the following:

```
admin authentication tacacsplus
```

3. Configure the following parameters as required:

Parameter	Description
`admin-priv { admin-priv }`	**Synopsis:** A string up to 5 characters long **Default:** 15 The privilege level(s) for administrator (admin) users. Options include any number between 0 and 15, or a range (e.g. 4-12).
`oper-priv { oper-priv }`	**Synopsis:** A string up to 5 characters long **Default:** 2-14 The privilege level(s) for operator (oper) users. Options include any number between 0 and 15, or a range (e.g. 4-12).
`guest-priv { guest-priv }`	**Synopsis:** A string up to 5 characters long **Default:** 1 The privilege level(s) for guest users. Options include any number between 0 and 15, or a range (e.g. 4-12).

4. Configure the primary or secondary Tacacsplus server by typing either `primary` or `secondary` and configuring the following parameter(s) as required:

Parameter	Description
`address { address }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The IP address of the TACACS+ server.
`port-tcp { port-tcp }`	**Synopsis:** An integer between 1 and 65535 **Default:** 49 The TCP port to use when connecting the TACACS+ server. The default port is 49.
`authentication-key { authentication-key }`	**Synopsis:** A string The authentication key to use for encrypting and decrypting TACACS+ traffic. Use only ASCII characters.

5. Type `commit` and press **Enter** to save the changes.

6.8 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.

6.8.1 Viewing the Local Host SSH/RSA Public Key

To view the local host SSH/RSA public key, type:

```
show security crypto local-host-ssh-rsa-public-key
```

For example:

```
show security crypto local-host-ssh-rsa-public-key
local-host-ssh-rsa-public-key
 contents "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0De8wvPyFpUGph9mwNXP
cY3/dwmQxIelGZe5Pt4laOZpeGOtuMSKqN15jcx29RcBasSdui5muLq8o+iBfDwjJw2q5WB
 BqyweXHgGYQGC58e7PQ5eYWIvu2L/cgTpR3rCs4xTUh+URJYCTGEhh1V6jGOjuY8M3pO/iL
PrwtZ066uyCqNoJLoptYnLfRDJu8AdWNdxLfXQsSv4XOB8hzYKekyg8bqsE/w6b5MyE60X
 c51f413PMicZz6WhBcuaqvutHxoIqCR6oI7fkLGGyWaeCzWUO02FplVfiJe1vT
wAaa5+JAoSdPNzTJKrHvFE18SdEAlwpj4PMVIA7oaEHL9vb"
```

6.8.2 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » session-security*** and configure the following parameter(s) as required:

   Note

   Only SSH RSA private keys can be selected for SSH/SFTP server access.

Parameter	Description
`certificate { certificate }`	**Synopsis:** A string between 1 and 255 characters long The certificate name for SSL connections and associated private keys.
`certificate-private-key { certificate-private-key }`	**Synopsis:** A string between 1 and 255 characters long
`ssh-rsa-private-key { ssh-rsa-private-key }`	**Synopsis:** A string between 1 and 255 characters long The RSA key used for ssh security (SFTP)

Parameter	Description
`ssh-ed25519-private-key { ssh-ed25519-private-key }`	**Synopsis:** A string between 1 and 255 characters long The ED25519 key used for ssh security (CLI, NETCONF, SFTP)
`ssh-dsa-private-key { ssh-dsa-private-key }`	**Synopsis:** 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 225).

For information about adding private keys, refer to "Adding a Private Key" (Page 220).

3. Type `commit` and press **Enter** to save the changes.

6.8.3 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 192).

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 225).

6.8.3.1 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 218).
2. Enable the Trusted Certificate Store. For more information, refer to "Enabling/ Disabling the Trusted Certificate Store" (Page 192).
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 215).

6.8.3.2 Enabling/Disabling the Trusted Certificate Store

⚠ NOTICE

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 215).

The Trusted Certificate Store is disabled by default.

To enable or disable the Trusted Certificate Store, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the Trusted Certificate Store by typing:

   Enable

   ```
   admin system-ca-certificates use-public-ca-store
   ```

   Disable

   ```
   no admin system-ca-certificates use-public-ca-store
   ```

3. Type `commit` and press **Enter** to save the changes.

6.8.3.3 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**

Subject Name:	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)
Fingerprint:	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
Issued:	Dec 24 17:50:51 1999 GMT
Expires:	Jul 24 14:15:12 2029 GMT

- **Go_Daddy_Class_2_CA.crt**

Subject Name:	C = US, O = "The Go Daddy Group, Inc.", OU = Go Daddy Class 2 Certification Authority
Fingerprint:	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
Issued:	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 www.camerfirma.com/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**

Subject Name:	C = IN, OU = emSign PKI, O = eMudhra Technologies Limited, CN = emSign ECC Root CA - G3
Fingerprint:	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
Issued:	Feb 18 18:30:00 2018 GMT
Expires:	Feb 18 18:30:00 2043 GMT

- **AffirmTrust_Premium_ECC.crt**

Subject Name:	C = US, O = AffirmTrust, CN = AffirmTrust Premium ECC
Fingerprint:	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
Issued:	Jan 29 14:20:24 2010 GMT
Expires:	Dec 31 14:20:24 2040 GMT

- **Microsec_e-Szigno_Root_CA_2009.crt**

Subject Name:	C = HU, L = Budapest, O = Microsec Ltd., CN = Microsec e-Szigno Root CA 2009, emailAddress = info@e-szigno.hu
Fingerprint:	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
Issued:	Jun 16 11:30:18 2009 GMT
Expires:	Dec 30 11:30:18 2029 GMT

- **Network_Solutions_Certificate_Authority.crt**

Subject Name:	C = US, O = Network Solutions L.L.C., CN = Network Solutions Certificate Authority
Fingerprint:	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
Issued:	Dec 1 00:00:00 2006 GMT
Expires:	Dec 31 23:59:59 2029 GMT

- **D-TRUST_Root_Class_3_CA_2_EV_2009.crt**

Subject Name:	C = DE, O = D-Trust GmbH, CN = D-TRUST Root Class 3 CA 2 EV 2009
Fingerprint:	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
Issued:	Nov 5 08:50:46 2009 GMT
Expires:	Nov 5 08:50:46 2029 GMT

- **COMODO_RSA_Certification_Authority.crt**

Subject Name:	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority
Fingerprint:	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
Issued:	Jan 19 00:00:00 2010 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **QuoVadis_Root_CA.crt**

Subject Name:	C = BM, O = QuoVadis Limited, OU = Root Certification Authority, CN = QuoVadis Root Certification Authority
Fingerprint:	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
Issued:	Mar 19 18:33:33 2001 GMT
Expires:	Mar 17 18:33:33 2021 GMT

- **IdenTrust_Commercial_Root_CA_1.crt**

Subject Name:	C = US, O = IdenTrust, CN = IdenTrust Commercial Root CA 1
Fingerprint:	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
Issued:	Jan 16 18:12:23 2014 GMT
Expires:	Jan 16 18:12:23 2034 GMT

- **DigiCert_High_Assurance_EV_Root_CA.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert High Assurance EV Root CA
Fingerprint:	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
Issued:	Nov 10 00:00:00 2006 GMT
Expires:	Nov 10 00:00:00 2031 GMT

- **TrustCor_RootCert_CA-2.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-2
Fingerprint:	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
Issued:	Feb 4 12:32:23 2016 GMT
Expires:	Dec 31 17:26:39 2034 GMT

- **USERTrust_RSA_Certification_Authority.crt**

Subject Name:	C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust RSA Certification Authority
Fingerprint:	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
Issued:	Feb 1 00:00:00 2010 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **GlobalSign_Root_CA_-_R3.crt**

Subject Name:	OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
Fingerprint:	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
Issued:	Mar 18 10:00:00 2009 GMT
Expires:	Mar 18 10:00:00 2029 GMT

- **XRamp_Global_CA_Root.crt**

Subject Name:	C = US, OU = www.xrampsecurity.com, O = XRamp Security Services Inc, CN = XRamp Global Certification Authority
Fingerprint:	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
Issued:	Nov 1 17:14:04 2004 GMT
Expires:	Jan 1 05:37:19 2035 GMT

- **GlobalSign_Root_CA_-_R2.crt**

Subject Name:	OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
Fingerprint:	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
Issued:	Dec 15 08:00:00 2006 GMT
Expires:	Dec 15 08:00:00 2021 GMT

- **E-Tugra_Certification_Authority.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Mar 5 12:09:48 2013 GMT
Expires:	Mar 3 12:09:48 2023 GMT

- **EE_Certification_Centre_Root_CA.crt**

Subject Name:	C = EE, O = AS Sertifitseerimiskeskus, CN = EE Certification Centre Root CA, emailAddress = pki@sk.ee
Fingerprint:	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
Issued:	Oct 30 10:10:30 2010 GMT
Expires:	Dec 17 23:59:59 2030 GMT

- **GeoTrust_Primary_Certification_Authority_-_G3.crt**

Subject Name:	C = US, O = GeoTrust Inc., OU = (c) 2008 GeoTrust Inc. - For authorized use only, CN = GeoTrust Primary Certification Authority - G3
Fingerprint:	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
Issued:	Apr 2 00:00:00 2008 GMT
Expires:	Dec 1 23:59:59 2037 GMT

- **Staat_der_Nederlanden_Root_CA_-_G3.crt**

Subject Name:	C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden Root CA - G3
Fingerprint:	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
Issued:	Nov 14 11:28:42 2013 GMT
Expires:	Nov 13 23:00:00 2028 GMT

- **SSL.com_EV_Root_Certification_Authority_ECC.crt**

Subject Name:	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com EV Root Certification Authority ECC
Fingerprint:	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
Issued:	Feb 12 18:15:23 2016 GMT
Expires:	Feb 12 18:15:23 2041 GMT

- **Entrust_Root_Certification_Authority.crt**

Subject Name:	C = US, O = "Entrust, Inc.", OU = www.entrust.net/CPS is incorporated by reference, OU = "(c) 2006 Entrust, Inc.", CN = Entrust Root Certification Authority
Fingerprint:	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
Issued:	Nov 27 20:23:42 2006 GMT
Expires:	Nov 27 20:53:42 2026 GMT

- **QuoVadis_Root_CA_1_G3.crt**

Subject Name:	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 1 G3
Fingerprint:	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
Issued:	Jan 12 17:27:44 2012 GMT
Expires:	Jan 12 17:27:44 2042 GMT

- **Entrust_Root_Certification_Authority_-_EC1.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Dec 18 15:25:36 2012 GMT
Expires:	Dec 18 15:55:36 2037 GMT

- **GTS_Root_R4.crt**

Subject Name:	C = US, O = Google Trust Services LLC, CN = GTS Root R4
Fingerprint:	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
Issued:	Jun 22 00:00:00 2016 GMT
Expires:	Jun 22 00:00:00 2036 GMT

- **thawte_Primary_Root_CA_-_G2.crt**

Subject Name:	C = US, O = "thawte, Inc.", OU = "(c) 2007 thawte, Inc. - For authorized use only", CN = thawte Primary Root CA - G2
Fingerprint:	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
Issued:	Nov 5 00:00:00 2007 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **GeoTrust_Universal_CA_2.crt**

Subject Name:	C = US, O = GeoTrust Inc., CN = GeoTrust Universal CA 2
Fingerprint:	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
Issued:	Mar 4 05:00:00 2004 GMT
Expires:	Mar 4 05:00:00 2029 GMT

- **Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Oct 1 00:00:00 1999 GMT
Expires:	Jul 16 23:59:59 2036 GMT

- **GlobalSign_Root_CA_-_R6.crt**

Subject Name:	OU = GlobalSign Root CA - R6, O = GlobalSign, CN = GlobalSign
Fingerprint:	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
Issued:	Dec 10 00:00:00 2014 GMT
Expires:	Dec 10 00:00:00 2034 GMT

- **Buypass_Class_3_Root_CA.crt**

Subject Name:	C = NO, O = Buypass AS-983163327, CN = Buypass Class 3 Root CA
Fingerprint:	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
Issued:	Oct 26 08:28:58 2010 GMT
Expires:	Oct 26 08:28:58 2040 GMT

- **GTS_Root_R3.crt**

Subject Name:	C = US, O = Google Trust Services LLC, CN = GTS Root R3
Fingerprint:	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
Issued:	Jun 22 00:00:00 2016 GMT
Expires:	Jun 22 00:00:00 2036 GMT

- **VeriSign_Universal_Root_Certification_Authority.crt**

Subject Name:	C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2008 VeriSign, Inc. - For authorized use only", CN = VeriSign Universal Root Certification Authority
Fingerprint:	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
Issued:	Apr 2 00:00:00 2008 GMT
Expires:	Dec 1 23:59:59 2037 GMT

- **Entrust_Root_Certification_Authority_-_G4.crt**

Subject Name:	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
Fingerprint:	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
Issued:	May 27 11:11:16 2015 GMT
Expires:	Dec 27 11:41:16 2037 GMT

- **GlobalSign_ECC_Root_CA_-_R5.crt**

Subject Name:	OU = GlobalSign ECC Root CA - R5, O = GlobalSign, CN = GlobalSign
Fingerprint:	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
Issued:	Nov 13 00:00:00 2012 GMT
Expires:	Jan 19 03:14:07 2038 GMT

- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Nov 8 00:00:00 2006 GMT
Expires:	Jul 16 23:59:59 2036 GMT

- **NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Dec 11 15:08:21 2008 GMT
Expires:	Dec 6 15:08:21 2028 GMT

- **SSL.com_Root_Certification_Authority_RSA.crt**

Subject Name:	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com Root Certification Authority RSA
Fingerprint:	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
Issued:	Feb 12 17:39:39 2016 GMT
Expires:	Feb 12 17:39:39 2041 GMT

- **Amazon_Root_CA_1.crt**

Subject Name:	C = US, O = Amazon, CN = Amazon Root CA 1
Fingerprint:	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
Issued:	May 26 00:00:00 2015 GMT
Expires:	Jan 17 00:00:00 2038 GMT

- **thawte_Primary_Root_CA_-_G3.crt**

Subject Name:	C = US, O = "thawte, Inc.", OU = Certification Services Division, OU = "(c) 2008 thawte, Inc. - For authorized use only", CN = thawte Primary Root CA - G3
Fingerprint:	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
Issued:	Apr 2 00:00:00 2008 GMT
Expires:	Dec 1 23:59:59 2037 GMT

- **QuoVadis_Root_CA_2_G3.crt**

Subject Name:	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2 G3
Fingerprint:	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
Issued:	Jan 12 18:59:32 2012 GMT
Expires:	Jan 12 18:59:32 2042 GMT

- **DigiCert_Global_Root_CA.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root CA
Fingerprint:	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
Issued:	Nov 10 00:00:00 2006 GMT
Expires:	Nov 10 00:00:00 2031 GMT

- **OISTE_WISeKey_Global_Root_GC_CA.crt**

Subject Name:	C = CH, O = WISeKey, OU = OISTE Foundation Endorsed, CN = OISTE WISeKey Global Root GC CA
Fingerprint:	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
Issued:	May 9 09:48:34 2017 GMT
Expires:	May 9 09:58:33 2042 GMT

- **Security_Communication_Root_CA.crt**

Subject Name:	C = JP, O = SECOM Trust.net, OU = Security Communication RootCA1
Fingerprint:	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
Issued:	Sep 30 04:20:49 2003 GMT
Expires:	Sep 30 04:20:49 2023 GMT

- **TeliaSonera_Root_CA_v1.crt**

Subject Name:	O = TeliaSonera, CN = TeliaSonera Root CA v1
Fingerprint:	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
Issued:	Oct 18 12:00:50 2007 GMT
Expires:	Oct 18 12:00:50 2032 GMT

- **DigiCert_Global_Root_G2.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
Fingerprint:	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
Issued:	Aug 1 12:00:00 2013 GMT
Expires:	Jan 15 12:00:00 2038 GMT

- **AffirmTrust_Commercial.crt**

Subject Name:	C = US, O = AffirmTrust, CN = AffirmTrust Commercial
Fingerprint:	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
Issued:	Jan 29 14:06:06 2010 GMT
Expires:	Dec 31 14:06:06 2030 GMT

- **GeoTrust_Universal_CA.crt**

Subject Name:	C = US, O = GeoTrust Inc., CN = GeoTrust Universal CA
Fingerprint:	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
Issued:	Mar 4 05:00:00 2004 GMT
Expires:	Mar 4 05:00:00 2029 GMT

- **Secure_Global_CA.crt**

Subject Name:	C = US, O = SecureTrust Corporation, CN = Secure Global CA
Fingerprint:	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
Issued:	Nov 7 19:42:28 2006 GMT
Expires:	Dec 31 19:52:06 2029 GMT

- **Sonera_Class_2_Root_CA.crt**

Subject Name:	C = FI, O = Sonera, CN = Sonera Class2 CA
Fingerprint:	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
Issued:	Apr 6 07:29:40 2001 GMT
Expires:	Apr 6 07:29:40 2021 GMT

- **ACCVRAIZ1.crt**

Subject Name:	CN = ACCVRAIZ1, OU = PKIACCV, O = ACCV, C = ES
Fingerprint:	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
Issued:	May 5 09:37:37 2011 GMT
Expires:	Dec 31 09:37:37 2030 GMT

- **SecureTrust_CA.crt**

Subject Name:	C = US, O = SecureTrust Corporation, CN = SecureTrust CA
Fingerprint:	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 www.camerfirma.com/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**

Subject Name:	C = US, O = GeoTrust Inc., CN = GeoTrust Primary Certification Authority
Fingerprint:	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
Issued:	Nov 27 00:00:00 2006 GMT
Expires:	Jul 16 23:59:59 2036 GMT

- **QuoVadis_Root_CA_3.crt**

Subject Name:	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 3
Fingerprint:	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
Issued:	Nov 24 19:11:23 2006 GMT
Expires:	Nov 24 19:06:44 2031 GMT

- **GlobalSign_ECC_Root_CA_-_R4.crt**

Subject Name:	OU = GlobalSign ECC Root CA - R4, O = GlobalSign, CN = GlobalSign
Fingerprint:	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
Issued:	Nov 13 00:00:00 2012 GMT
Expires:	Jan 19 03:14:07 2038 GMT

- **COMODO_Certification_Authority.crt**

Subject Name:	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO Certification Authority
Fingerprint:	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
Issued:	Dec 1 00:00:00 2006 GMT
Expires:	Dec 31 23:59:59 2029 GMT

- **OISTE_WISeKey_Global_Root_GB_CA.crt**

Subject Name:	C = CH, O = WISeKey, OU = OISTE Foundation Endorsed, CN = OISTE WISeKey Global Root GB CA
Fingerprint:	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
Issued:	Dec 1 15:00:32 2014 GMT
Expires:	Dec 1 15:10:31 2039 GMT

- **USERTrust_ECC_Certification_Authority.crt**

Subject Name:	C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust ECC Certification Authority
Fingerprint:	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
Issued:	Feb 1 00:00:00 2010 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **DigiCert_Assured_ID_Root_G3.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root G3
Fingerprint:	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
Issued:	Aug 1 12:00:00 2013 GMT
Expires:	Jan 15 12:00:00 2038 GMT

- **GlobalSign_Root_CA.crt**

Subject Name:	C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
Fingerprint:	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
Issued:	Sep 1 12:00:00 1998 GMT
Expires:	Jan 28 12:00:00 2028 GMT

- **Hongkong_Post_Root_CA_1.crt**

Subject Name:	C = HK, O = Hongkong Post, CN = Hongkong Post Root CA 1
Fingerprint:	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
Issued:	May 15 05:13:14 2003 GMT
Expires:	May 15 04:52:29 2023 GMT

- **Entrust_Root_Certification_Authority_-_G2.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Jul 7 17:25:54 2009 GMT
Expires:	Dec 7 17:55:54 2030 GMT

- **T-TeleSec_GlobalRoot_Class_3.crt**

Subject Name:	C = DE, O = T-Systems Enterprise Services GmbH, OU = T-Systems Trust Center, CN = T-TeleSec GlobalRoot Class 3
Fingerprint:	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
Issued:	Oct 1 10:29:56 2008 GMT
Expires:	Oct 1 23:59:59 2033 GMT

- **SecureSign_RootCA11.crt**

Subject Name:	C = JP, O = "Japan Certification Services, Inc.", CN = SecureSign RootCA11
Fingerprint:	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
Issued:	Apr 8 04:56:47 2009 GMT
Expires:	Apr 8 04:56:47 2029 GMT

- **DigiCert_Trusted_Root_G4.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Trusted Root G4
Fingerprint:	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
Issued:	Aug 1 12:00:00 2013 GMT
Expires:	Jan 15 12:00:00 2038 GMT

- **LuxTrust_Global_Root_2.crt**

Subject Name:	C = LU, O = LuxTrust S.A., CN = LuxTrust Global Root 2
Fingerprint:	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
Issued:	Mar 5 13:21:57 2015 GMT
Expires:	Mar 5 13:21:57 2035 GMT

- **SwissSign_Silver_CA_-_G2.crt**

Subject Name:	C = CH, O = SwissSign AG, CN = SwissSign Silver CA - G2
Fingerprint:	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
Issued:	Oct 25 08:32:46 2006 GMT
Expires:	Oct 25 08:32:46 2036 GMT

- **CFCA_EV_ROOT.crt**

Subject Name:	C = CN, O = China Financial Certification Authority, CN = CFCA EV ROOT
Fingerprint:	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
Issued:	Aug 8 03:07:01 2012 GMT
Expires:	Dec 31 03:07:01 2029 GMT

- **certSIGN_ROOT_CA.crt**

Subject Name:	C = RO, O = certSIGN, OU = certSIGN ROOT CA
Fingerprint:	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
Issued:	Jul 4 17:20:04 2006 GMT
Expires:	Jul 4 17:20:04 2031 GMT

- **Starfield_Services_Root_Certificate_Authority_-_G2.crt**

Subject Name:	C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Services Root Certificate Authority - G2
Fingerprint:	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
Issued:	Sep 1 00:00:00 2009 GMT
Expires:	Dec 31 23:59:59 2037 GMT

- **emSign_Root_CA_-_C1.crt**

Subject Name:	C = US, OU = emSign PKI, O = eMudhra Inc, CN = emSign Root CA - C1

Fingerprint:	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
Issued:	Feb 18 18:30:00 2018 GMT
Expires:	Feb 18 18:30:00 2043 GMT

- **AffirmTrust_Networking.crt**

Subject Name:	C = US, O = AffirmTrust, CN = AffirmTrust Networking
Fingerprint:	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
Issued:	Jan 29 14:08:24 2010 GMT
Expires:	Dec 31 14:08:24 2030 GMT

- **DST_Root_CA_X3.crt**

Subject Name:	O = Digital Signature Trust Co., CN = DST Root CA X3
Fingerprint:	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
Issued:	Sep 30 21:12:19 2000 GMT
Expires:	Sep 30 14:01:15 2021 GMT

- **SSL.com_EV_Root_Certification_Authority_RSA_R2.crt**

Subject Name:	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com EV Root Certification Authority RSA R2
Fingerprint:	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
Issued:	May 31 18:14:37 2017 GMT
Expires:	May 30 18:14:37 2042 GMT

- **UCA_Extended_Validation_Root.crt**

Subject Name:	C = CN, O = UniTrust, CN = UCA Extended Validation Root
Fingerprint:	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
Issued:	Mar 13 00:00:00 2015 GMT
Expires:	Dec 31 00:00:00 2038 GMT

- **emSign_ECC_Root_CA_-_C3.crt**

Subject Name:	C = US, OU = emSign PKI, O = eMudhra Inc, CN = emSign ECC Root CA - C3
Fingerprint:	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
Issued:	Feb 18 18:30:00 2018 GMT
Expires:	Feb 18 18:30:00 2043 GMT

- **D-TRUST_Root_Class_3_CA_2_2009.crt**

Subject Name:	C = DE, O = D-Trust GmbH, CN = D-TRUST Root Class 3 CA 2 2009
Fingerprint:	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
Issued:	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**

Subject Name:	C = US, O = Google Trust Services LLC, CN = GTS Root R1
Fingerprint:	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
Issued:	Jun 22 00:00:00 2016 GMT
Expires:	Jun 22 00:00:00 2036 GMT

- **Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt**

Subject Name:	C = GR, L = Athens, O = Hellenic Academic and Research Institutions Cert. Authority, CN = Hellenic Academic and Research Institutions ECC RootCA 2015
Fingerprint:	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
Issued:	Jul 7 10:37:12 2015 GMT
Expires:	Jun 30 10:37:12 2040 GMT

- **ePKI_Root_Certification_Authority.crt**

Subject Name:	C = TW, O = "Chunghwa Telecom Co., Ltd.", OU = ePKI Root Certification Authority
Fingerprint:	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
Issued:	Dec 20 02:31:27 2004 GMT
Expires:	Dec 20 02:31:27 2034 GMT

- **GTS_Root_R2.crt**

Subject Name:	C = US, O = Google Trust Services LLC, CN = GTS Root R2
Fingerprint:	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
Issued:	Jun 22 00:00:00 2016 GMT
Expires:	Jun 22 00:00:00 2036 GMT

- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Nov 5 00:00:00 2007 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **DigiCert_Global_Root_G3.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G3
Fingerprint:	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
Issued:	Aug 1 12:00:00 2013 GMT
Expires:	Jan 15 12:00:00 2038 GMT

- **Starfield_Class_2_CA.crt**

Subject Name:	C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification Authority
Fingerprint:	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
Issued:	Jun 29 17:39:16 2004 GMT
Expires:	Jun 29 17:39:16 2034 GMT

- **IdenTrust_Public_Sector_Root_CA_1.crt**

Subject Name:	C = US, O = IdenTrust, CN = IdenTrust Public Sector Root CA 1
Fingerprint:	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
Issued:	Jan 16 17:53:32 2014 GMT
Expires:	Jan 16 17:53:32 2034 GMT

- **Baltimore_CyberTrust_Root.crt**

Subject Name:	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
Fingerprint:	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
Issued:	May 12 18:46:00 2000 GMT
Expires:	May 12 23:59:00 2025 GMT

- **EC-ACC.crt**

Subject Name:	C = ES, O = Agencia Catalana de Certificacio (NIF Q-0801176-I), OU = Serveis Publics de Certificacio, OU = Vegeu https://www.catcert.net/verarrel (c)03, OU = Jerarquia Entitats de Certificacio Catalanes, CN = EC-ACC
Fingerprint:	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
Issued:	Jan 7 23:00:00 2003 GMT
Expires:	Jan 7 22:59:59 2031 GMT

- **TWCA_Root_Certification_Authority.crt**

Subject Name:	C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Root Certification Authority
Fingerprint:	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
Issued:	Aug 28 07:24:33 2008 GMT
Expires:	Dec 31 15:59:59 2030 GMT

- **DigiCert_Assured_ID_Root_G2.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root G2
Fingerprint:	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
Issued:	Aug 1 12:00:00 2013 GMT
Expires:	Jan 15 12:00:00 2038 GMT

- **Staat_der_Nederlanden_EV_Root_CA.crt**

Subject Name:	C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden EV Root CA
Fingerprint:	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
Issued:	Dec 8 11:19:29 2010 GMT
Expires:	Dec 8 11:10:28 2022 GMT

- **TWCA_Global_Root_CA.crt**

Subject Name:	C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Global Root CA
Fingerprint:	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
Issued:	Jun 27 06:28:33 2012 GMT
Expires:	Dec 31 15:59:59 2030 GMT

- **Trustis_FPS_Root_CA.crt**

Subject Name:	C = GB, O = Trustis Limited, OU = Trustis FPS Root CA
Fingerprint:	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
Issued:	Dec 23 12:14:06 2003 GMT
Expires:	Jan 21 11:36:54 2024 GMT

- **Certigna_Root_CA.crt**

Subject Name:	C = FR, O = Dhimyotis, OU = 0002 48146308100036, CN = Certigna Root CA
Fingerprint:	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
Issued:	Oct 1 08:32:27 2013 GMT
Expires:	Oct 1 08:32:27 2033 GMT

- **Hongkong_Post_Root_CA_3.crt**

Subject Name:	C = HK, ST = Hong Kong, L = Hong Kong, O = Hongkong Post, CN = Hongkong Post Root CA 3
Fingerprint:	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
Issued:	Jun 3 02:29:46 2017 GMT
Expires:	Jun 3 02:29:46 2042 GMT

- **GeoTrust_Primary_Certification_Authority_-_G2.crt**

Subject Name:	C = US, O = GeoTrust Inc., OU = (c) 2007 GeoTrust Inc. - For authorized use only, CN = GeoTrust Primary Certification Authority - G2
Fingerprint:	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
Issued:	Nov 5 00:00:00 2007 GMT
Expires:	Jan 18 23:59:59 2038 GMT

- **TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Nov 25 08:25:55 2013 GMT
Expires:	Oct 25 08:25:55 2043 GMT

- **GDCA_TrustAUTH_R5_ROOT.crt**

Subject Name:	C = CN, O = "GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.", CN = GDCA TrustAUTH R5 ROOT
Fingerprint:	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
Issued:	Nov 26 05:13:15 2014 GMT
Expires:	Dec 31 15:59:59 2040 GMT

- **Atos_TrustedRoot_2011.crt**

Subject Name:	CN = Atos TrustedRoot 2011, O = Atos, C = DE
Fingerprint:	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
Issued:	Jul 7 14:58:30 2011 GMT
Expires:	Dec 31 23:59:59 2030 GMT

- **Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt**

Subject Name:	C = GR, L = Athens, O = Hellenic Academic and Research Institutions Cert. Authority, CN = Hellenic Academic and Research Institutions RootCA 2015
Fingerprint:	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
Issued:	Jul 7 10:11:21 2015 GMT
Expires:	Jun 30 10:11:21 2040 GMT

- **Go_Daddy_Root_Certificate_Authority_-_G2.crt**

Subject Name:	C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", CN = Go Daddy Root Certificate Authority - G2
Fingerprint:	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
Issued:	Sep 1 00:00:00 2009 GMT
Expires:	Dec 31 23:59:59 2037 GMT

- **OISTE_WISeKey_Global_Root_GA_CA.crt**

Subject Name:	C = CH, O = WISeKey, OU = Copyright (c) 2005, OU = OISTE Foundation Endorsed, CN = OISTE WISeKey Global Root GA CA
Fingerprint:	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
Issued:	Dec 11 16:03:44 2005 GMT
Expires:	Dec 11 16:09:51 2037 GMT

- **SSL.com_Root_Certification_Authority_ECC.crt**

Subject Name:	C = US, ST = Texas, L = Houston, O = SSL Corporation, CN = SSL.com Root Certification Authority ECC
Fingerprint:	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
Issued:	Feb 12 18:14:03 2016 GMT
Expires:	Feb 12 18:14:03 2041 GMT

- **GeoTrust_Global_CA.crt**

Subject Name:	C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
Fingerprint:	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
Issued:	May 21 04:00:00 2002 GMT
Expires:	May 21 04:00:00 2022 GMT

- **Buypass_Class_2_Root_CA.crt**

Subject Name:	C = NO, O = Buypass AS-983163327, CN = Buypass Class 2 Root CA
Fingerprint:	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
Issued:	Oct 26 08:38:03 2010 GMT
Expires:	Oct 26 08:38:03 2040 GMT

- **Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt**

Subject Name:	C = ES, CN = Autoridad de Certificacion Firmaprofesional CIF A62634068
Fingerprint:	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
Issued:	May 20 08:38:15 2009 GMT
Expires:	Dec 31 08:38:15 2030 GMT

- **Amazon_Root_CA_3.crt**

Subject Name:	C = US, O = Amazon, CN = Amazon Root CA 3
Fingerprint:	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
Issued:	May 26 00:00:00 2015 GMT
Expires:	May 26 00:00:00 2040 GMT

- **CA_Disig_Root_R2.crt**

Subject Name:	C = SK, L = Bratislava, O = Disig a.s., CN = CA Disig Root R2
Fingerprint:	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
Issued:	Jul 19 09:15:30 2012 GMT
Expires:	Jul 19 09:15:30 2042 GMT

- **Security_Communication_RootCA2.crt**

Subject Name:	C = JP, O = "SECOM Trust Systems CO.,LTD.", OU = Security Communication RootCA2

Fingerprint:	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
Issued:	May 29 05:00:39 2009 GMT
Expires:	May 29 05:00:39 2029 GMT

- **DigiCert_Assured_ID_Root_CA.crt**

Subject Name:	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root CA
Fingerprint:	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
Issued:	Nov 10 00:00:00 2006 GMT
Expires:	Nov 10 00:00:00 2031 GMT

- **QuoVadis_Root_CA_3_G3.crt**

Subject Name:	C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 3 G3
Fingerprint:	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
Issued:	Jan 12 20:26:32 2012 GMT
Expires:	Jan 12 20:26:32 2042 GMT

- **Certum_Trusted_Network_CA.crt**

Subject Name:	C = PL, O = Unizeto Technologies S.A., OU = Certum Certification Authority, CN = Certum Trusted Network CA
Fingerprint:	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
Issued:	Oct 22 12:07:37 2008 GMT
Expires:	Dec 31 12:07:37 2029 GMT

- **emSign_Root_CA_-_G1.crt**

Subject Name:	C = IN, OU = emSign PKI, O = eMudhra Technologies Limited, CN = emSign Root CA - G1
Fingerprint:	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
Issued:	Feb 18 18:30:00 2018 GMT
Expires:	Feb 18 18:30:00 2043 GMT

- **AffirmTrust_Premium.crt**

Subject Name:	C = US, O = AffirmTrust, CN = AffirmTrust Premium
Fingerprint:	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
Issued:	Jan 29 14:10:36 2010 GMT
Expires:	Dec 31 14:10:36 2040 GMT

- **thawte_Primary_Root_CA.crt**

Subject Name:	C = US, O = "thawte, Inc.", OU = Certification Services Division, OU = "(c) 2006 thawte, Inc. - For authorized use only", CN = thawte Primary Root CA

Fingerprint:	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
Issued:	Nov 17 00:00:00 2006 GMT
Expires:	Jul 16 23:59:59 2036 GMT

- **NetLock_Arany_=Class_Gold=_Fotanúsítvány.crt**

Subject Name:	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
Fingerprint:	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
Issued:	Dec 11 15:08:21 2008 GMT
Expires:	Dec 6 15:08:21 2028 GMT

6.8.4 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.

6.8.4.1 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, type:

```
show admin system-ca-certificates configured-cas
```

If CA certificates have been added to the Store, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin system-ca-certificates configured-cas | tab
NAME
------
cert

!
```

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 215).

6.8.4.2 Adding a CA Certificate to the Trusted Certificate Store

To add a CA certificate to the Trusted Certificate Store, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the CA certificate by typing:

```
admin system-ca-certificates configured-cas { certifi
cate }
```

Where { certificate } is the chosen CA certificate.

3. Type `commit` and press **Enter** to save the changes.

6.8.4.3 Deleting a CA Certificate from the Trusted Certificate Store

To delete a CA certificate from the Trusted Certificate Store, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the CA certificate from the store by typing:

   ```
   no admin system-ca-certificates configured-cas { certifi
   cate }
   ```

   Where { certificate } is the chosen CA certificate.
3. Type `commit` and press **Enter** to save the changes.

6.8.5 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.

6.8.5.1 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, type:

```
show running-config security crypto ca
```

If certificates have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security crypto ca security crypto ca ca-cert key-
cert-sign-certificate
```

If no certificates have been configured, add certificates as needed. For more information, refer to "Adding a CA Certificate and CRL" (Page 218).

6.8.5.2 Viewing the Status of a CA Certificate and CRL

To view the status of a CA certificate, type:

```
show security crypto ca { certificate } key-cert-sign-cer
tificate-status
```

Where:

- `{ certificate }` is the name of the certificate

The table or list provides the following information:

Parameter	Description
`issuer`	**Synopsis:** A string
`subject`	**Synopsis:** A string
`not-before`	**Synopsis:** A string This certificate is not valid before this date.
`not-after`	**Synopsis:** A string This certificate is not valid after this date.

To view the status of a Certificate Revocation List (CRL) that was signed by a separate certificate, type:

```
show security crypto ca { certificate } crl-sign-certifi
cate-status
```

Where:

- `{ certificate }` is the name of the certificate

The table or list provides the following information:

Parameter	Description
`issuer`	**Synopsis:** A string
`subject`	**Synopsis:** A string
`not-before`	**Synopsis:** A string This certificate is not valid before this date.
`not-after`	**Synopsis:** A string This certificate is not valid after this date.

To view the status of a Certificate Revocation List (CRL) that was not signed by a separate certificate, type:

```
show security crypto ca { certificate } crl-status
```

Where:

- `{ certificate }` is the name of the certificate

The table or list provides the following information:

Parameter	Description
`issuer`	**Synopsis:** A string
`this-update`	**Synopsis:** A string This CRL was updated at this date and time.
`next-update`	**Synopsis:** A string This CRL must be updated by this date and time.

6.8.5.3 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. Enable auto-wizard by typing:

   ```
   autowizard true
   ```

2. Make sure the CLI is in Configuration mode.

   Note

   Before inserting the contents of the certificate, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the certificate has been added.

3. Add the CA certificate by typing:

   ```
   security crypto ca { certificate } key-cert-sign-certifi
   cate { contents }
   ```

   Where:

   - `{ certificate }` is the name of the certificate
   - `{ contents }` is the contents of the certificate

4. Add the associated Certificate Revocation List (CRL).

   Note

   Large CRLs (bigger than 100KB) are not currently supported and may be difficult to add/view in the configuration.

Note

Before inserting the contents of the CRL, enter multi-line mode by pressing **Esc +m**. Press **Ctrl+d** to exit multi-line mode after the CRL has been added.

- If the CRL is signed by a separate certificate, type:

  ```
  security crypto ca { certificate } crl-sign-certificate
  { contents }
  ```

  Where:

  - `{ certificate }` is the name of the certificate
  - `{ contents }` is the contents of the signed CRL
- If the CRL is not signed, type:

  ```
  security crypto ca { certificate } crl { contents }
  ```

  Where:

  - `{ certificate }` is the name of the certificate
  - `{ contents }` is the contents of the CRL

5. Type `commit` and press **Enter** to save the changes.

6.8.5.4 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. Make sure the CLI is in Configuration mode.
2. Delete the CA certificate and its associated Certificate Revocation List (CRL) by typing:

   ```
   no security crypto ca { certificate }
   ```

   Where:

   - `{ certificate }` is the name of the certificate
3. Type `commit` and press **Enter** to save the changes.

6.8.6 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.

6.8.6.1 Viewing a List of Private Keys

To view a list of unsigned private keys, type:

```
show running-config security crypto private-key
```

If private keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security crypto private-key
security
 crypto
  private-key key
   algorithm rsa
   contents
   "{--contents--}"
  !
 !
!
```

If no private keys have been configured, add keys as needed. For more information, refer to "Adding a Private Key" (Page 220).

6.8.6.2 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. Make sure the CLI is in Configuration mode.
2. Add the private key by typing:

   ```
   security crypto private-key { name }
   ```

   Where:

   - `{ name }` is the name of the private key
3. Configure the following parameter(s) as required:

   Note

   Before inserting the contents of the key, enter multi-line mode by pressing **Esc +m**. Press **Ctrl+d** to exit multi-line mode after the key has been added.

Parameter	Description
`algorithm { algorithm }`	**Synopsis:** [rsa | dsa | ssh-rsa | ssh-ed25519] The type of key.
`contents { contents }`	**Synopsis:** A string between 1 and 8192 characters long The contents of the unsigned private key.

4. Type `commit` and press **Enter** to save the changes.

6.8.6.3 Deleting a Private Key

To delete an unsigned private key, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the private key by typing:

   ```
   no security crypto private-key { name }
   ```

   Where { name } is the name of the private key
3. Type `commit` and press **Enter** to save the changes.

6.8.7 Managing Public Keys

This section describes how to manage public keys on the device.

6.8.7.1 Viewing a List of Public Keys

To view a list of unsigned public keys, type:

```
show running-config security crypto public-key
```

If public keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security crypto public-key
security
crypto
  public-key ipsec-generated
   algorithm        rsa
   contents         "{--contents--}"
   private-key-name ipsec-generated
  !
!
!
```

If no public keys have been configured, add keys as needed. For more information, refer to "Adding a Public Key" (Page 222).

6.8.7.2 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 220).
2. Enable auto-wizard by typing:

   ```
   autowizard true
   ```
3. Make sure the CLI is in Configuration mode.
4. Add the public key by typing:

   ```
   security crypto public-key { name }
   ```

   Where:

   - `{ name }` is the name of the public key
5. Configure the following parameter(s) as required:

   Note

   Before inserting the contents of the key, enter multi-line mode by pressing **Esc +m**. Press **Ctrl+d** to exit multi-line mode after the key has been added.

   Note

   For added security, consider adding an IPSec-formatted public key. For more information, refer to "Adding an IPSec-Formatted Public Key" (Page 223).

   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 { algorithm }`	**Synopsis:** [rsa | dsa | ssh-rsa | ssh-ed25519] The algorithm of the key.
`contents { contents }`	**Synopsis:** A string between 1 and 8192 characters long The contents of the key.
`private-key-name { private-key-name }`	**Synopsis:** A string between 1 and 255 characters long The private key name associated with this public key.

6. Type `commit` and press **Enter** to save the changes.

6.8.7.3 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. Make sure the desired public key has been added. For more information about adding a public key, refer to "Adding a Public Key" (Page 222).
2. Enable auto-wizard by typing:

   ```
   autowizard true
   ```

3. Make sure the CLI is in Configuration mode.
4. Type the following command:

   ```
   security crypto public-key { name } add-ipsec-format
   ted-public-key content
   ```

   Where:

   - `{ name }` is the name of the public key

   The CLI enters multi-line mode.
5. Enter the contents of the public key, pressing **Enter** for each new line. When finished, press **Ctrl-D**. The public keys is converted to PEM format and added to RUGGEDCOM ROX II.
6. Type `commit` and press **Enter** to save the changes.

6.8.7.4 Deleting a Public Key

To delete an unsigned public key, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the public key by typing:

   ```
   no security crypto public-key { name }
   ```

   Where { name } is the name of the public key
3. Type `commit` and press **Enter** to save the changes.

6.8.8 Managing Certificates

This section describes how to manage certificates on the device.

6.8.8.1 Viewing a List of Certificates

To view a list of certificates, type:

```
show running-config security crypto certificate
```

If certificates have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security crypto certificate
security
 crypto
  certificate cert
   contents         "{--contents--}"
   private-key-name key
   ca-name          ca-cert
  !
 !
!
```

If no certificates have been configured, add certificates as needed. For more information, refer to "Adding a Certificate" (Page 225).

6.8.8.2 Viewing the Status of a Certificate

To view the status of a certificate, type:

```
show security crypto certificate { certificate } status
```

Where:

- `{ certificate }` is the name of the certificate

```
ruggedcom# show security crypto certificate ssl-cert status
status
 issuer     /C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=localhost.localdo
main
 subject    /C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=localhost.localdo
main
 not before 2017-01-06T18:45:49-00:00
 not after  2037-01-03T18:45:49-00:00
```

The table or list provides the following information:

Parameter	Description
`issuer`	**Synopsis:** A string
`subject`	**Synopsis:** A string

Parameter	Description
`not-before`	**Synopsis:** A string This certificate is not valid before this date.
`not-after`	**Synopsis:** A string This certificate is not valid after this date.

6.8.8.3 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 218)
   - For more information about adding private keys, refer to "Adding a Private Key" (Page 220)
2. Make sure the CLI is in Configuration mode.
3. Add the certificate by typing:

   ```
   security crypto certificate { certificate }
   ```

   Where { certificate } is the name of the certificate.
4. Configure the following parameter(s) as required:

   Note

   Before inserting the contents of the certificate, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the certificate has been added.

Parameter	Description
`contents { contents }`	**Synopsis:** A string between 1 and 8192 characters long The contents of the certificate.
`private-key-name { private-key-name }`	**Synopsis:** A string between 1 and 255 characters long The private key associated with this certificate.
`ca-name { ca-name }`	**Synopsis:** A string between 1 and 255 characters long The optional CA certificate for this certificate.

5. [Optional] Select the certificate as the certificate to use for SSL/SSH connections. For more information, refer to "Configuring Session Security" (Page 190).
6. Type `commit` and press **Enter** to save the changes.

6.8.8.4 Deleting a Certificate

To delete a certificate, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the certificate by typing:

   ```
   no security crypto certificate { certificate }
   ```

   Where:

   - `{ certificate }` is the name of the certificate.
3. Type `commit` and press **Enter** to save the changes.

6.8.9 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.

6.8.9.1 Viewing a List of Known Hosts

To view a list of servers defined in the Known Hosts list, type:

```
show running-config admin known-hosts
```

If servers have been defined, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin known-hosts | tab
admin
 known-hosts
  server-identification
                                SERVER
                         SERVER  PUBLIC
NAME    SERVER ID        PORT    KEY     ENABLED
-------------------------------------------------
server  172.30.145.203   34      server  X

 !
!
```

If no servers have been configured, add servers as needed. For more information, refer to "Adding a Known Host" (Page 227).

6.8.9.2 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 221).
2. Make sure the CLI is in Configuration mode.
3. Add the server by typing:

   ```
   admin known-hosts server-identification { name } server-id
   { id } server-port { port } server-public-key { key } en
   abled
   ```

   Where:

   - { name } is the unique name of the server.
   - { id } is the name to identify the server. The name may be host name or the server's IP address.
   - { port } is a specific port on the server configured for SSH communications. If no port is specified, RUGGEDCOM ROX II will access any port on the server that supports SSH.
   - { key } is the authorized SSH/RSA public key associated with the server.
4. Type `commit` and press **Enter** to save the changes.

6.8.9.3 Deleting a Known Host

To delete a server from the Known Hosts list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the desired server by typing:

   ```
   no admin known-hosts server-identification { name }
   ```

   Where { name } is the unique name of the server.
3. Type `commit` and press **Enter** to save the changes.

6.8.10 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.

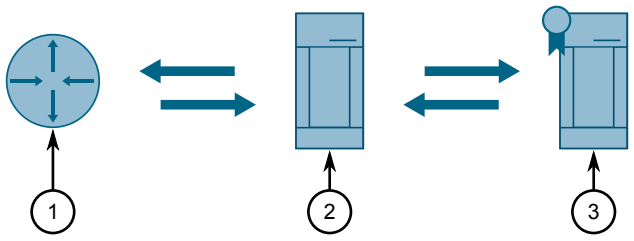
SCEP is used by network administrators to quickly and automatically issue Public Key Infrastructure (PKI) certificates to devices, as opposed to manually managing certificates for each individual device.

SCEP is an open-source protocol described in RFC 8894 [https://tools.ietf.org/html/rfc8894].

6.8.10.1 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.

6.8.10.2 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]" 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 230).

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 231).

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 233).

6. **Retrieve the SCEP certificate from the server.**

   For more information, refer to "Retrieving an SCEP Certificate" (Page 233).

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 234).

8. **[Optional] Verify the CA certificate was added to the device.**

   For more information, refer to "Viewing the Status of a Certificate" (Page 224).

6.8.10.3 Configuring the SCEP Client

To configure the SCEP client, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***security » crypto » scep » scep-config*** and 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 { server-url }`	**Synopsis:** A string between 1 and 1024 characters long The URL of the SCEP server.
`ca-certificate-name { ca-certificate-name }`	**Synopsis:** A string between 1 and 255 characters long **Default:** scep-ca The name of the SCEP CA certificate.
`ca-certificate-hash-value { ca-certificate-hash-value }`	**Synopsis:** 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 { ca-certificate-hash-type }`	**Synopsis:** [sha256 | sha1 | md5] **Default:** md5 The type of the hash value of the CA certificate obtained from the SCEP server.
`maximum-number-of-requests { maximum-number-of-requests }`	**Synopsis:** An integer between 1 and 256 **Default:** 60 The maximum number of SCEP certificate polling requests. Default is 60.
`max-polling-time { max-polling-time }`	**Synopsis:** An integer between 1 and 28800 **Default:** 3600 The maximum SCEP certificate polling time in seconds. Default is 3600.
`polling-interval { polling-interval }`	**Synopsis:** An integer between 1 and 3600 **Default:** 60 The interval in seconds between SCEP certificate polling attempts. Default is 60 seconds.

3. Type `commit` and press **Enter** to save the changes.

6.8.10.4 Configuring the SCEP Certificate Signing Requests

To configure information that will be included in SCEP Certificate Signing Requests (CSRs), do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***security » crypto » scep*** and 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 { subject-alternative-name }`	**Synopsis:** A string between 1 and 128 characters long The subject alternative name associated with the SCEP certificate.
`subject-alternative-name-type { subject-alternative-name-type }`	**Synopsis:** [ip | email | dns] **Default:** dns The subject alternative name type associated with the SCEP certificate. Default is 'dns'.
`country { country }`	**Synopsis:** A string The country associated with the SCEP certificate.
`state-or-province { state-or-province }`	**Synopsis:** A string up to 128 characters long The state or province name associated with the SCEP certificate.
`locality { locality }`	**Synopsis:** A string up to 128 characters long The locality associated with the SCEP certificate.
`organization { organization }`	**Synopsis:** A string up to 64 characters long The organization associated with the SCEP certificate.
`organizational-unit { organizational-unit }`	**Synopsis:** A string up to 64 characters long The organizational unit associated with the SCEP certificate
`key-size { key-size }`	**Synopsis:** [4096 | 2048 | 1024] **Default:** 2048 The key size in bits, default is 2048
`certificate-name { certificate-name }`	**Synopsis:** A string between 1 and 255 characters long **Default:** scep-cert The name of the SCEP certificate.
`private-key-name { private-key-name }`	**Synopsis:** A string between 1 and 255 characters long **Default:** scep-rsa The name of the private key.

Parameter	Description
`encryption-algorithm { encryption-algorithm }`	**Synopsis:** [aes256 | aes192 | aes128 | 3des] **Default:** aes128 The encryption algorithm.
`signature-algorithm { signature-algorithm }`	**Synopsis:** [sha512 | sha384 | sha256 | sha224 | sha1] **Default:** sha256 The signature algorithm.

3. Type `commit` and press **Enter** to save the changes.

6.8.10.5 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. Make sure the CLI is in Configuration mode.
2. Request the SCEP certificate by entering the following command:

```
security crypto scep get-ca fingerprint-algorithm [ sha1 | sha224 | sha256 | sha384 | sha512 ]
```

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.

6.8.10.6 Retrieving an SCEP Certificate

To retrieve an SCEP certificate, do the following:

1. Make sure the CLI is in Configuration mode.
2. Request the SCEP certificate by entering the following command:

```
security crypto scep get-certificate challenge-password { password }
```

Where { password } is the challenge password (up to 128 characters long) 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.

Upon entering the challenge password, 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.

6.8.10.7 Configuring Automatic Certificate Renewal

To configure automatic certificate renewal, do the following:

Note

SCEP certificates cannot be renewed once they have expired.

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » crypto » scep*** and configure the following parameter(s) as required:

Parameter	Description
`enable { enable }`	**Synopsis:** [true | false] When enabled, the SCEP certificate will be automatically renewed at the configured time. Default is false.
`time-before-expiry { time-before-expiry }`	**Synopsis:** An integer between 1 and 365 **Default:** 14 The number of days or hours before expiry when the SCEP certificate will be automatically renewed. Default is 14.
`unit-of-time { unit-of-time }`	**Synopsis:** [hours | days] **Default:** days The unit of time in which the time before the SCEP certificate expiry is displayed. Default is 'days'.

3. Type `commit` and press **Enter** to save the changes.

6.8.10.8 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 233).

6.8.10.9 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 233).

6.9 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 235).

6.9.1 Firewall Concepts

This section describes some of the concepts important to the implementation of firewalls in RUGGEDCOM ROX II.

6.9.1.1 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.

6.9.1.2 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.

6.9.1.3 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.

6.9.1.4 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.

6.9.1.5 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.

6.9.1.6 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 **routefilter** and **logmartians** for the firewall interface.

For information about enabling **routefilter** and **logmartians**, refer to "Adding an Interface" (Page 246).

6.9.1.7 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.

⚠ NOTICE

Configuration hazard – risk of authorized access

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.

6.9.2 Viewing a List of Firewalls

To view a list of firewalls, type:

```
show running-config security firewall fwconfig
```

If firewalls have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig
security
 firewall
  fwconfig firewall1
  !
  fwconfig firewall2
  !
 !
```

```
!
```

If no firewalls have been configured, add firewalls as needed. For more information, refer to "Adding a Firewall" (Page 239).

6.9.3 Adding a Firewall

To add a new firewall, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the firewall by typing:

   ```
   security firewall fwconfig { firewall }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
3. Configure the following parameter(s) as required:

Parameter	Description
`description { description }`	**Synopsis:** A string An optional description string.

4. Add interfaces associated with the firewall. For more information about adding interfaces, refer to "Adding an Interface" (Page 246).
5. 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 244).
6. Associate an interface with each zone. For more information about associating interfaces with zones, refer to "Associating an Interface with a Zone" (Page 247).
7. 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 250).
8. 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 254). For more information about configuring masquerading and/or SNAT settings, refer to "Managing Masquerade and SNAT Settings" (Page 256).
9. 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 248).
10. If required, configure rules that override the default policies. For more information about configuring rules, refer to "Managing Rules" (Page 258).
11. If required, configure support for a VPN. For more information, refer to:

- "Configuring the Firewall for a VPN" (Page 241)
- "Configuring the Firewall for a VPN in a DMZ" (Page 242)

12. Validate the configuration. For more information about validating a firewall configuration, refer to "Validating a Firewall Configuration" (Page 263).
13. Enable the firewall. For more information, refer to "Enabling/Disabling a Firewall" (Page 263).
14. Type `commit` and press **Enter** to save the changes.

6.9.4 Deleting a Firewall

To delete a firewall, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the firewall by typing:

   ```
   no security firewall fwconfig { firewall }
   ```

   Where { firewall } is the name of the firewall.
3. Type `commit` and press **Enter** to save the changes.

6.9.5 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. Make sure the CLI is in Configuration mode.
2. Specify the work configuration by typing:

   ```
   security firewall work-config { name }
   ```

   Where:

   - `{ name }` is the name of a firewall configuration
3. Specify the active configuration by typing:

   ```
   security firewall active-config { name }
   ```

   Where:

   - `{ name }` is the name of a firewall configuration
4. Type `commit` and press **Enter** to save the changes.

6.9.6 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 239).
2. Make sure zones for local, network and VPN traffic have been configured. For more information about managing zones, refer to "Managing Zones" (Page 243).
3. Make sure a zone called *Any* exists and is of the type IPsec . For more information about managing zones, refer to "Managing Zones" (Page 243).
4. 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 247).
5. 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 248).
6. 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 248).

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

7. 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 258).

8. 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 258).

6.9.7 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 239).
2. Make sure a zone called *dmz* exists. For more information about managing zones, refer to "Managing Zones" (Page 243).
3. 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 258).

6.9.8 Configuring Netfilter

To configure Netfilter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the time in seconds (s) a stale TCP connection can reside in the connection tracking table by typing:

   ```
   admin system tcp-est-conn-track-timeout { value }
   ```

   Where { value } is a number between 300 and 432000. The default value is 432000 s, or five days.
3. Type `commit` and press **Enter** to save the changes.

6.9.9 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.

6.9.9.1 Viewing a List of Zones

To view a list of zones, type:

```
show running-config security firewall fwconfig { firewall }
fwzone
```

Where:

- `{ firewall }` is the name of the firewall

If zones have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig fwzone
security
 firewall
  fwconfig firewall
   fwzone fw
    type        firewall
    description FirewallZone
   !
   fwzone man
    description IPv4Zone
   !
  !
 !
!
```

If no zones have been configured, add zones as needed. For more information, refer to "Adding a Zone" (Page 244).

6.9.9.2 Adding a Zone

To add a new zone for a firewall, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the zone by typing:

   `security firewall fwconfig { firewall } fwzone { zone }`

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ zone }` is the name of the zone
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`type { type }`	**Synopsis:** [ipv4 | ipsec | firewall] **Default:** ipv4 Zone types are plain IPv4, firewall, or IPSec
`description { description }`	**Synopsis:** A string (Optional) The description string for this zone

4. Type `commit` and press **Enter** to save the changes.

6.9.9.3 Deleting a Zone

To delete a zone, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the zone by typing:

   ```
   no security firewall fwconfig { firewall } fwzone { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the zone
3. Type `commit` and press **Enter** to save the changes.

6.9.10 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

6.9.10.1 Viewing a List of Interfaces

To view a list of interfaces, type:

```
show running-config security firewall fwconfig { firewall }
fwinterface
```

Where { firewall } is the name of the firewall.

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig fwinterface
security
 firewall
  fwconfig firewall
   fwinterface fe-cm-1
    zone man
    description Interface
```

```
    !
   !
  !
 !
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an Interface" (Page 246).

6.9.10.2 Adding an Interface

To configure an interface for a firewall, do the following:

1. Display the list of available interfaces by typing:

   ```
   show running-config ip
   ```

2. Record the name of the chosen interface.
3. Enter Configuration mode by typing:

   ```
   config
   ```

4. Add the interface by typing:

   ```
   security firewall fwconfig { firewall } fwinterface
   { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the interface

5. Configure the interface settings by typing the following commands:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`description { description }`	**Synopsis:** A string (Optional) The description string for this interface
`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.
`tcpflags`	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.

Parameter	Description
`norfc1918`	Not currently implemented
`routefilter`	IPv4 and IPv6 - Enables /rpfilter/ spoofing protection
`proxyarp`	IPv4 ONLY - Enables proxy ARP.
`maclist`	Not currently implemented
`nosmurfs`	IPv4 ONLY - Packets with broadcast address as source dropped and logged at info level.
`logmartians`	IPv4 ONLY - Logging of packets with impossible source addresses.

6. 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 247).
7. Configure a broadcast address for the interface. For more information configuring a broadcast address, refer to "Configuring a Broadcast Address" (Page 247).
8. Type `commit` and press **Enter** to save the changes.

6.9.10.3 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » { firewall } » fwinterface » { interface } » zone***, where { firewall } is the name of the firewall and { interface } is the name of the interface.
3. Configure one of the following options:

Parameter	Description
`predefined-zone { predefined-zone }`	**Synopsis:** A string between 0 and 5 characters long The interface is associated with the specified zone.
`undefined-zone`	The zone is marked as undefined.

4. Type `commit` and press **Enter** to save the changes.

6.9.10.4 Configuring a Broadcast Address

To configure a broadcast address for an interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***security » firewall » fwconfig » { firewall } » fwinterface » { interface } » broadcast-addr***, where { firewall } is the name of the firewall and { interface } is the name of the interface.
3. Configure one of the following options:

Parameter	Description
`ipv4-address { ipv4-address }`	**Synopsis:** A string An IPv4 address for a broadcast address.
`detect`	The broadcast address(es) is detected automatically.
`none`	A broadcast address is not defined. This is the default option.

4. Type `commit` and press **Enter** to save the changes.

6.9.10.5 Deleting an Interface

To delete an interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the interface by typing:

   ```
   no security firewall fwconfig { firewall } fwinterface
   { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

6.9.11 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

6.9.11.1 Viewing a List of Hosts

To view a list of hosts, type:

```
show running-config security firewall fwconfig { firewall }
fwhost
```

Where:

- `{ firewall }` is the name of the firewall

If hosts have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwhost
security
 firewall
  fwconfig firewall1
   fwhost host1
    zone      man
    interface fe-cm-1
    no ipaddress
    no description
   !
  !
 !
!
```

If no hosts have been configured, add hosts as needed. For more information, refer to "Adding a Host" (Page 249).

6.9.11.2 Adding a Host

To add a new host for a firewall, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the host by typing:

   ```
   security firewall fwconfig { firewall } fwhost { name }
   ```

   Where:

   - { firewall } is the name of the firewall
   - { name } is the name of the host
3. Configure the host by typing the following commands:

Parameter	Description
`ipsec { ipsec }`	**Synopsis:** [true | false] **Default:** false

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`zone { zone }`	**Synopsis:** A string between 0 and 5 characters long A pre-defined zone
`interface { inter face }`	**Synopsis:** A string between 1 and 15 characters long A pre-defined interface to which optional IPs and/or networks can be added.
`ipaddress { ipad dress }`	**Synopsis:** A string Additional IP addresses or networks - comma separated, or a range in the form of low.address-high.address
`description { descrip tion }`	**Synopsis:** A string (Optional) The description string for this host.

4. Type `commit` and press **Enter** to save the changes.

6.9.11.3 Deleting a Host

To delete a host, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the host by typing:

   ```
   no security firewall fwconfig { firewall } fwhost { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the host
3. Type `commit` and press **Enter** to save the changes.

6.9.12 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 243).

Note

Policies for specific hosts or types of traffic can be overridden by rules. For more information about rules, refer to "Managing Rules" (Page 258).

6.9.12.1 Viewing a List of Policies

To view a list of policies, type:

```
show running-config security firewall fwconfig { firewall }
fwpolicy
```

Where:

- `{ firewall }` is the name of the firewall

If policies have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwpolicy
security
 firewall
  fwconfig firewall1
   fwpolicy p1
    description Policy
   !
  !
 !
!
```

If no policies have been configured, add policies as needed. For more information, refer to "Adding a Policy" (Page 252).

6.9.12.2 Adding a Policy

To configure a policy for the firewall, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the policy by typing:

   ```
   security firewall fwconfig { firewall } fwpolicy { poli
   cy }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ policy }` is the name of the policy
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`policy { policy }`	**Synopsis:** [accept | drop | reject | continue] **Default:** reject A default action for connection establishment between different zones.
`log-level { log-lev el }`	**Synopsis:** [none | debug | info | notice | warning | error | critical | alert | emergency] **Default:** none (Optional) Determines whether or not logging will take place and at which logging level.
`description { descrip tion }`	**Synopsis:** A string (Optional) The description string for this policy.

4. Configure the source zone for the policy. For more information, refer to "Configuring the Source Zone" (Page 252).
5. Configure the destination zone for the policy. For more information, refer to "Configuring the Destination Zone" (Page 253).
6. Type `commit` and press **Enter** to save the changes.

6.9.12.3 Configuring the Source Zone

To configure the source zone for a firewall policy, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***security » firewall » fwconfig » { firewall } » fwpolicy » { policy } » source-zone***, where { firewall } is the name of the firewall and { policy } is the name of the policy.
3. Configure one of the following options:

Parameter	Description
`predefined-zone { predefined-zone }`	**Synopsis:** A string between 0 and 5 characters long The firewall policy applies to the specified zone.
`all`	The firewall policy applies to all zones.

4. Type `commit` and press **Enter** to save the changes.

6.9.12.4 Configuring the Destination Zone

To configure the destination zone for a firewall policy, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » { firewall } » fwpolicy » { policy } » destination-zone***, where { firewall } is the name of the firewall and { policy } is the name of the policy. The **Destination Zone** form appears.
3. Configure one of the following options:

Parameter	Description
`predefined-zone { predefined-zone }`	**Synopsis:** A string between 0 and 5 characters long The firewall policy applies to the specified zone.
`all`	The firewall policy applies to all zones.

4. Type `commit` and press **Enter** to save the changes.

6.9.12.5 Deleting a Policy

To delete a policy, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the policy by typing:

```
no security firewall fwconfig { firewall } fwpolicy { policy }
```

Where:

- { firewall } is the name of the firewall
- { policy } is the name of the policy

3. Type `commit` and press **Enter** to save the changes.

6.9.13 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 258).

6.9.13.1 Viewing a List of NAT Settings

To view a list of NAT settings, type:

```
show running-config security firewall { firewall } fwnat
```

Where:

- `{ firewall }` is the name of the firewall

If NAT settings have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwnat
security
 firewall
  fwconfig firewall1
   fwnat n1
    external-addr 172.30.150.10
    interface     fe-cm-1
    internal-addr 192.168.1.100
    no description
   !
   fwnat fwmasq
    external-addr 172.30.159.5
    interface     fe-cm-1
    internal-addr 193.168.1.1
    no description
   !
  !
 !
!
```

If no NAT settings have been configured, add NAT settings as needed. For more information, refer to "Adding a NAT Setting" (Page 254).

6.9.13.2 Adding a NAT Setting

To configure a Network Address Translation (NAT) entry, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the entry by typing:

   ```
   security firewall fwconfig { firewall } fwnat { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the network address translation entry

3. Configure the following parameter(s) as required:

Parameter	Description
`external-addr { external-addr }`	**Synopsis:** 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 { interface }`	**Synopsis:** A string between 1 and 15 characters long An interface that has an external IP address.
`ipalias`	Create IP Alias for NAT rule.
`internal-addr { internal-addr }`	**Synopsis:** 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 { description }`	**Synopsis:** A string (Optional) The description string for this NAT entry.

4. Type `commit` and press **Enter** to save the changes.

6.9.13.3 Deleting a NAT Setting

To delete a network address translation entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:

   ```
   no security firewall fwconfig { firewall } fwnat { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the network address translation entry

3. Type `commit` and press **Enter** to save the changes.

6.9.14 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.

6.9.14.1 Viewing a List of Masquerade and SNAT Settings

To view a list of masquerade and SNAT settings, type:

```
show running-config security firewall fwconfig { firewall }
fwmasq
```

Where:

- `{ firewall }` is the name of the firewall

If masquerade and SNAT settings have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig firewall2 fwmasq
security
 firewall
  fwconfig firewall2
   fwmasq SNAT
    out-interface fe-cm-1
    no out-interface-specifics
    source-hosts  192.168.1.0/24
    address       172.30.15.10
    no description
   !
   fwmasq Masq
    out-interface fe-cm-1
    no out-interface-specifics
    source-hosts  192.168.0.0/24
    no address
    no description
   !
  !
 !
!
```

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 257).

6.9.14.2 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. Make sure the CLI is in Configuration mode.
2. Add the masquerade or SNAT setting by typing:

   ```
   security firewall fwconfig { firewall } fwmasq { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the masquerade or SNAT setting
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`out-interface { out-interface }`	**Synopsis:** A string An outgoing interface list - usually the internet interface.
`out-interface-specifics { out-interface-specifics }`	**Synopsis:** A string (Optional) An outgoing interface list - specific IP destinations for the out-interface.
`ipalias`	Create IP Alias for NAT rule.
`source-hosts { source-hosts }`	**Synopsis:** A string Subnet range or comma-separated list of hosts (IPs)
`address { address }`	**Synopsis:** A string (Optional) By specifying an address here, SNAT will be used and this will be the source address.
`description { description }`	**Synopsis:** A string (Optional) The description string for this masq entry.

4. Type `commit` and press **Enter** to save the changes.

6.9.14.3 Deleting a Masquerade or SNAT Setting

To delete a masquerade or SNAT setting, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the masquerade or SNAT setting by typing:

   ```
   no security firewall fwconfig { firewall } fwmasq { name }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ name }` is the name of the masquerade or SNAT setting
3. Type `commit` and press **Enter** to save the changes.

6.9.15 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.

6.9.15.1 Viewing a List of Rules

To view a list of rules, type:

```
show running-config security firewall fwconfig { firewall }
fwrule
```

Where:

- `{ firewall }` is the name of the firewall

If rules have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwrule
security
 firewall
  fwconfig firewall1
   fwrule Rule1
    action accept
    source-zone man
    destination-zone man
    no description
   !
   fwrule Rule2
    action accept
    source-zone man
    destination-zone man
    no description
   !
  !
 !
!
```

If no rules have been configured, add rules as needed. For more information, refer to "Adding a Rule" (Page 259).

6.9.15.2 Adding a Rule

To configure a rule for a firewall, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the rule by typing:

   ```
   security firewall fwconfig { firewall } fwrule { rule }
   ```

   Where:

   - `{ firewall }` is the name of the firewall
   - `{ rule }` is the name of the rule
3. 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
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`action { action }`	**Synopsis:** [accept | drop | reject | continue | redirect | dnat- | dnat | copy-dnat] **Default:** reject The final action to take on incoming packets matching this rule. Options include: • accept: Allows the connection request to proceed. • continue: Passes the connection request past any other rules.

Parameter	Description
	• 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. • dnat: Forwards the request to another system and (optionally) another port. • dnat-: Only generates the DNAT IPtables rule and not the companion ACCEPT rule. • drop: The connection request is ignored. No notification is sent. • redirect: Redirects the request to a local TCP port number on the local firewall. • reject: Rejects the connection with an RST (TCP) or ICMP destination-unreachable.
`source-zone-hosts { source-zone-hosts }`	**Synopsis:** A string (Optional) Add comma-separated host IPs to a predefined source-zone.
`destination-zone-hosts { destination-zone-hosts }`	**Synopsis:** A string (Optional) Add comma-separated host IPs to the destination-zone - may include :port for DNAT or REDIRECT.
`log-level { log-level }`	**Synopsis:** [none | debug | info | notice | warning | error | critical | alert | emergency] **Default:** none (Optional) Determines whether or not logging will take place and at which logging level.
`protocol { protocol }`	**Synopsis:** A string or [tcp | udp | icmp | all] **Default:** all The protocol to match for this rule - must be 'udp' for rules using copy-dnat actions.
`source-ports { source-ports }`	**Synopsis:** A string **Default:** none (Optional) The TCP/UDP port(s) the connection originated from. Default: all ports. Add a single port or a list of comma-separated ports
`destination-ports { destination-ports }`	**Synopsis:** A string **Default:** none (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

Parameter	Description
`original-destination { original-destination }`	**Synopsis:** A string or [None] **Default:** none (Optional) The destination IP address in the connection request as it was received by the firewall - (mandatory) for rules using copy-dnat actions.
`helper { helper }`	**Synopsis:** [none | ftp] **Default:** none The Netfilter Helper to associate with this rule.
`description { description }`	**Synopsis:** A string (Optional) The description string for this rule.

4. Configure the source zone for the rule. For more information, refer to "Configuring the Source Zone" (Page 261).
5. Configure the destination zone for the rule. For more information, refer to "Configuring the Destination Zone" (Page 262).
6. Type `commit` and press **Enter** to save the changes.

6.9.15.3 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » { firewall } » fwrule{ rule } » source-zone***, where { firewall } is the name of the firewall and { rule } is the name of the rule.

⚠ 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.

3. Configure one of the following options:

Parameter	Description
`predefined-zone { predefined-zone }`	**Synopsis:** A string between 0 and 5 characters long The firewall policy applies to the specified zone.

Parameter	Description
`other { other }`	**Synopsis:** A string The firewall policy applies to select zones.
`all`	The firewall policy applies to all zones.

4. Type `commit` and press **Enter** to save the changes.

6.9.15.4 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » { firewall } » fwrule{ rule } » destination-zone***, where { firewall } is the name of the firewall and { rule } is the name of the rule. The **Destination Zone** form appears.

⚠ 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.

3. Configure one of the following options:

Parameter	Description
`predefined-zone { predefined-zone }`	**Synopsis:** A string between 0 and 5 characters long The firewall policy applies to the specified zone.
`other { other }`	**Synopsis:** A string The firewall policy applies to select zones.
`all`	The firewall policy applies to all zones.

4. Type `commit` and press **Enter** to save the changes.

6.9.15.5 Deleting a Rule

To delete a rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the rule by typing:

```
no security firewall fwconfig { firewall } fwrule { rule }
```

Where:

- `{ firewall }` is the name of the firewall
- `{ rule }` is the name of the rule

3. Type `commit` and press **Enter** to save the changes.

6.9.16 Validating a Firewall Configuration

To validate a firewall configuration, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the firewall as the working configuration by typing:

```
security firewall work-config { name }
```

Where:

- `{ name }` is the name of the firewall configuration

3. Type `commit` and press **Enter** to save the changes. The system validates the firewall configuration and displays the results.

6.9.17 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. Make sure the CLI is in Configuration mode.
2. Enable the firewall by typing:

```
security firewall enable
```

Or disable the firewall by using the *no* version of the command:

```
no security firewall enable
```

3. Type `commit` and press **Enter** to save the changes.

6.10 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 165).

```
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 165).

For more information about configuring the Listen IP for available services, refer to "Restricting Management Access to Specific Interfaces" (Page 263).

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 269) or "Adding an IPv6 Address" (Page 270).

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
    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 239).

7 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. Make sure the CLI is in Configuration mode.
2. Set the costing by typing:

   ```
   ip { interface } bandwidth { cost }
   ```

   Where:

   - `{ interface }` is the name of the routable interface
   - `{ cost }` is the value used in auto-cost calculations for the routable logical interface in kbps
3. Type `commit` and press **Enter** to save the changes.

7.1.2 Viewing Statistics for Routable Interfaces

To view statistics for all routable interfaces, type:

```
show interfaces ip
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces ip
interfaces ip dummy0
 admin state down
 state       down
 pointopoint false
 receive
  bytes   0
  packets 0
  errors  0
  dropped 0
 transmit
```

```
  bytes      0
  packets    0
  errors     0
  dropped    0
  collisions 0
interfaces ip fe-cm-1
.
.
.
```

The table or list displays the following information:

Parameter	Description
admin-state	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] The port's administrative status.
state	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] Shows whether the link is up or down.
pointopoint	**Synopsis:** [true | false] The point-to-point link.
bytes	**Synopsis:** An integer The number of bytes received.
packets	**Synopsis:** An integer The number of packets received.
errors	**Synopsis:** An integer The number of error packets received.
dropped	**Synopsis:** An integer The number of packets dropped by the receiving device.
bytes	**Synopsis:** An integer The number of bytes transmitted.
packets	**Synopsis:** An integer The number of packets transmitted.
errors	**Synopsis:** An integer The number of error packets transmitted.
dropped	**Synopsis:** An integer The number of packets dropped by the transmitting device.
collisions	**Synopsis:** 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 IPv4 address for a routable interface, type:

```
show running-config ip { interface } ipv4
```

Where:

- `{ interface }` is the name of the interface

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config ip ipv4 | tab
IFNAME       IPADDRESS         PEER
-------------------------------------
dummy0
             1.1.1.1/32        -
fe-cm-1
             192.168.0.12/24   -
             172.30.150.12/19  -
switch.0001
switch.0011
             192.168.11.1/24   -
switch.0012
             192.168.12.1/24   -
switch.0014
             192.168.14.1/24   -
```

If no addresses have been configured, add addresses as needed. For more information, refer to "Adding an IPv4 Address" (Page 269).

7.1.3.2 Adding an IPv4 Address

To add an IPv4 address to a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address by typing:

   ```
   ip { interface } ipv4 address { address } peer { peer }
   ```

   Where:

   - { interface } is the name of the interface
   - { address } is the IPv4 address and prefix
   - { peer } is the peer IPv4 address
3. Type `commit` and press **Enter** to save the changes.

7.1.3.3 Deleting an IPv4 Address

To delete an IPv4 address for a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no ip { interface } ipv4 address { address }
   ```

   Where:

   - `{ address }` is the IPv4 address
3. Type `commit` and press **Enter** to save 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

To view a list of IPv6 address for a routable interface, type:

```
show running-config ip { interface } ipv6 address
```

Where:

- `{ interface }` is the name of the interface

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config ip dummy0 ipv6 address
ip dummy0
 ipv6
  address 2001:db8:a0b:12f0::1/24
  !
  address 2001:db9:a2C:25f0::2/24
  !
 !
!
```

If no addresses have been configured, add addresses as needed. For more information, refer to "Adding an IPv6 Address" (Page 270).

7.1.4.2 Adding an IPv6 Address

To add an IPv6 address to a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address by typing:

   ```
   ip { interface } ipv6 address { address }
   ```

Where:

- `{ interface }` is the name of the interface
- `{ address }` is the IPv6 address

3. Type `commit` and press **Enter** to save the changes.

7.1.4.3 Deleting an IPv6 Address

To delete an IPv6 address for a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

```
no ip { interface } ipv6 address { address }
```

Where:

- `{ interface }` is the name of the interface
- `{ address }` is the IPv6 address

3. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Type the following command:

   ```
   ip { interface } ipv6 nd
   ```

   Where:

   - `{ interface }` is the name of the interface
3. Configure neighbor discovery by configuring the following parameter(s) as required:

Parameter	Description
`enable-ra`	Enable to send router advertisement messages.
`adv-interval-option`	Includes an Advertisement Interval option which indicates to hosts the maximum time in milliseconds, between successive unsolicited router advertisements.
`home-agent-config-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 { home-agent-life time }`	**Synopsis:** An integer between 0 and 65520 **Default:** 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 { home-agent-prefer ence }`	**Synopsis:** An integer between 0 and 65535 **Default:** 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.
`managed-config-flag`	The flag in IPv6 router advertisements, which indicates to hosts that they should use the managed (stateful) protocol for addresses autoconfiguraiton in addition to any addresses autoconfigured using stateless address autoconfiguration.

Parameter	Description
`other-config-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.
`ra-lifetime { ra-life time }`	**Synopsis:** An integer between 0 and 9000 **Default:** 1800 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.
`reachable-time-msec { reachable-time-msec }`	**Synopsis:** An integer between 0 and 3600000 **Default:** 0 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 neightbors. The value zero means unspecified (by this router).

4. Configure the router advertisement interval by configuring the following parameter(s) as required:

Parameter	Description
`value { value }`	**Synopsis:** An integer between 3 and 1800 The interval value.
`unit { unit }`	**Synopsis:** [sec | msec] The interval unit.

5. Type `commit` and press **Enter** to save 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:

1. Make sure the CLI is in Configuration mode.
2. Add the network prefix by typing:

```
ip { interface } ipv6 nd prefix { prefix }
```

Where:

- `{ interface }` is the name of the interface
- `{ prefix }` is the IPv6 address and prefix

3. Configure the lifetime settings by configuring the following parameter(s):

Parameter	Description
`valid { valid }`	**Synopsis:** 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 { preferred }`	**Synopsis:** An integer between 0 and 4294967295 or [infinite] The length of time in seconds during which addresses generated from the prefix remain preferred.

4. Configure the prefix settings by configuring the following parameter(s):

Parameter	Description
`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.
`router-address`	Indicates to hosts on the local link that the specified prefix contains a complete IP address by setting the R flag.

5. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no ip { interface } ipv6 address { address }
   ```

   Where:

   - `{ interface }` is the name of the interface
   - `{ address }` is the IPv6 address

3. Type `commit` and press **Enter** to save 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 276).

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 276).

7.2.2 Assigning a DHCP Server Address

To assign a DHCP server address to the DHCP relay agent, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
`dhcp-server-address { dhcp-server-address }`	**Synopsis:** A string The IP address of the DHCP server to which DHCP queries will be forwarded from this relay agent.

3. Add client ports. For more information, refer to "Adding a DHCP Client Port" (Page 276).
4. Type `commit` and press **Enter** to save the changes.

7.2.3 Viewing a List of DHCP Client Ports

To view a list of DHCP relay agent client ports, type:

```
show running-config switch dhcp-relay-agent dhcp-client-ports
```

If client ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch dhcp-relay-agent dhcp-client-ports
switch dhcp-relay-agent
 dhcp-client-ports lm1 1
 !
!
```

If no client ports have been configured, add client ports as needed. For more information, refer to "Adding a DHCP Client Port" (Page 276).

7.2.4 Adding a DHCP Client Port

To add a client port for the DHCP relay agent, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the client port by typing:

   ```
   switch dhcp-relay-agent  dhcp-client-ports { slot }
   { port }
   ```

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.

3. Type `commit` and press **Enter** to save the changes.

7.2.5 Deleting a DHCP Client Port

To delete a client port for the DHCP relay agent, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the client port by typing:

   ```
   no switch dhcp-relay-agent  dhcp-client-ports { slot }
   { port }
   ```

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.

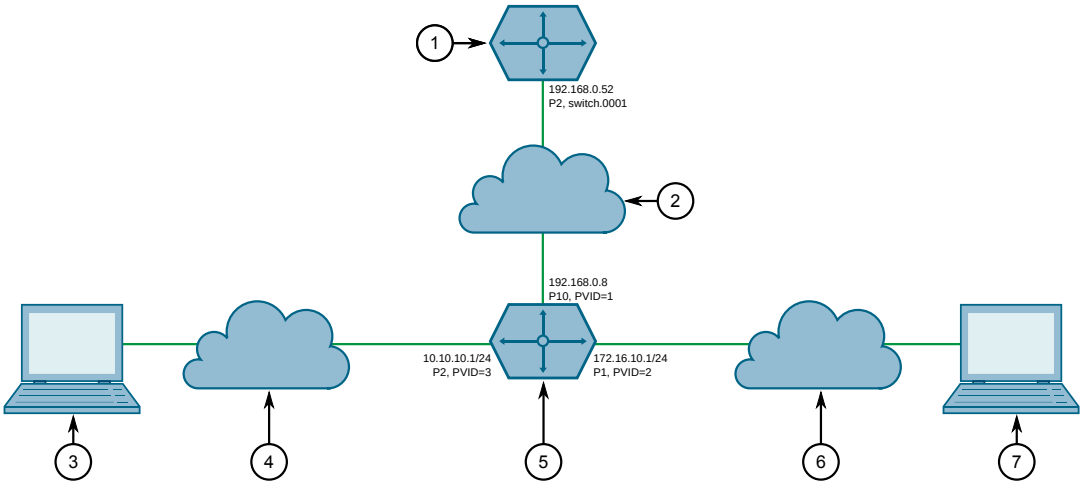
3. Type `commit` and press **Enter** to save the changes.

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 386).
   b. Assign IP address *192.168.0.8* to VLAN 1. For more information, refer to "Adding an IPv4 Address" (Page 269) or "Adding an IPv6 Address" (Page 270).
   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 335) 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 320) 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, type:

- **For IPv4**

  ```
  services dhcpserver show-active-leases
  ```

- **For IPv6**

  ```
  services dhcpserver6 show-active-leases
  ```

If certificates have been configured, a table or list similar to the following example appears:

```
ruggedcom# services dhcpserver show-active-leases
dhcpActionResult
lease 192.168.0.9 {
  starts 2 2012/11/13 20:35:47;
  ends 2 2012/11/13 20:45:47;
  hardware Ethernet 00:01:c0:0c:8b:a4;
  client-hostname "ape2-PC";
}

lease 192.168.0.11 {
  starts 2 2012/11/13 20:38:37;
  ends 2 2012/11/13 20:48:37;
  hardware Ethernet 00:01:c0:0b:b7:70;
}

lease 192.168.0.8 {
  starts 2 2012/11/13 20:38:47;
  ends 2 2012/11/13 20:48:47;
  hardware Ethernet 00:01:c0:0c:8b:a3;
  client-hostname "ape2-PC";
}

lease 192.168.0.22 {
  starts 2 2012/11/13 20:36:14;
  ends 2 2012/11/13 20:46:14;
  hardware Ethernet 00:01:c0:0b:b7:71;
}
```

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 320).

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 277) for more information.
2. Enable the DHCP server. For more information, refer to "Enabling/Disabling the DHCP Server" (Page 281).
3. Add a DHCP listen interface. For more information, refer to "Adding a DHCP Listen Interface" (Page 288).
4. Assign an IP address to the listen interface. For more information, refer to "Adding a Subnet" (Page 293).
5. Create a shared network and enable Option82. For more information, refer to "Adding a Shared Network" (Page 290) and "Configuring Shared Network Options" (Page 290).
6. Create a subnet for each LAN that has DHCP clients. For more information about creating subnets, refer to "Adding a Subnet" (Page 293).
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 293).
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 304) or "Adding an Address Pool (IPv6)" (Page 306).

      For more information about IP ranges, refer to "Adding an IP Range (IPv4)" (Page 308) or "Adding an IP Range (IPv6)" (Page 310).

   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 319).
9. [Optional] Add and configure hosts and host-groups. For more information, refer to "Adding a Host" (Page 300).

7.3.3 Enabling/Disabling the DHCP Server

To enable or disable the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the DHCP server by typing:
   - **Enable for IPv4**
     `services dhcpserver enabled`
   - **Disable for IPv4**
     `no services dhcpserver enabled`
   - **Enable for IPv6**
     `services dhcpserver6 enabled`
   - **Disable for IPv6**
     `no services dhcpserver6 enabled`
3. Type `commit` and press **Enter** to save the changes.

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.

1. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » options
   - **For IPv6**
     services » dhcpserver6 » options
3. Configure the following parameter(s) 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 293).

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [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.
`option82`	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 282) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 284).
5. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.

2. Navigate to ***services » dhcpserver » { path } » options***, where *path* is the path to and name of the desired shared network, subnet, host group or host. For example, to access the options for a shared network named *Shared*, navigate to:

   services » dhcpserver » shared-network » Shared » options

   To access the global options, navigate to:

   services » dhcpserver » options

3. Set the client options by configuring the following parameters as required:

Parameter	Description
`hostname { hostname }`	**Synopsis:** A string between 1 and 32 characters long The unique name to refer to the host within a DHCP configuration.
`subnetmask { subnet mask }`	**Synopsis:** A string between 7 and 15 characters long Subnet mask
`default-route { default-route }`	**Synopsis:** 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 { broadcast }`	**Synopsis:** 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 { domain }`	**Synopsis:** 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 { dns-server }`	**Synopsis:** 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 { static-route }`	**Synopsis:** 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.

4. Define the NIS server settings by configuring the following parameters as required:

Parameter	Description
`server { server }`	**Synopsis:** 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.
`domain { domain }`	**Synopsis:** 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.

5. Define the NetBios server settings by configuring the following parameters as required:

Parameter	Description
`scope { scope }`	**Synopsis:** A string between 1 and 256 characters long **Default:** netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
`nameserver { nameserver }`	**Synopsis:** A string between 1 and 256 characters long **Default:** 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

6. [Optional] Add custom options. For more information, refer to "Adding a Custom DHCP Client Configuration Option" (Page 286).
7. Type `commit` and press **Enter** to save 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:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » dhcpserver6 » { path } » { name } » options***, where *path* is the path to and name of the desired shared network, subnet6, host group or host and *name* is the user-added name.

   For example, to access the options for a shared network named *Shared*, navigate to:

   services » dhcpserver6 » shared-network » Shared » options

   To access the global options, navigate to:

   services » dhcpserver6 » options
3. Set the client options by configuring the following parameters as required:

Parameter	Description
`domain { domain }`	**Synopsis:** 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 { dns-server }`	**Synopsis:** 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 { domain-search }`	**Synopsis:** 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.

4. Define the NIS server settings by configuring the following parameters as required:

Parameter	Description
`server { server }`	**Synopsis:** 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.
`domain { domain }`	**Synopsis:** 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 286).
6. Type `commit` and press **Enter** to save the changes.

7.3.5.3 Viewing a List of Custom DHCP Client Configuration Options

To view a list of custom DHCP client configuration options set at the global level or for a specific shared network, type:

- **For IPv4**

  ```
  show running-config services dhcpserver { path } options client custom
  ```

- **For IPv6**

  ```
  show running-config services dhcpserver6 options client custom
  ```

Where { path } is the path to and name of the desired shared network, subnet, host group or host.

If custom configurations have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver options client custom
services
 dhcpserver
  options
   client
    custom 120 500
```

```
    !
   !
  !
 !
!
```

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 286).

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].

1. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » { path } » options » client » custom
   - **For IPv6**
     services » dhcpserver6 » options » client » custom

   where *path* is the path to and name of the desired shared network, subnet, host group or host.

   Note

   Custom options at the **{ path }** level are only available for IPv4.

   For example, to access the custom IPv4 options for a shared network named *Shared*, navigate to:

   services » dhcpserver » shared-network » Shared » options » client » custom

   To access custom IPv4 options at the global level, navigate to:

   services » dhcpserver » options » client » custom
3. Configure the following parameter(s) as required:

Parameter	Description
`number { number }`	**Synopsis:** An integer
`value { value }`	**Synopsis:** An integer The value of the custom option.

4. Type `commit` and press **Enter** to save the changes.

7.3.5.5 Deleting a Custom DHCP Client Configuration Option

To delete a custom client option, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » { path } » options » client » custom
   - **For IPv6**
     services » dhcpserver6 » options » client » custom

   where *path* is the path to and name of the desired shared network, subnet, host group or host.

   Note

   Custom options at the **{ path }** level are only available for IPv4.

   For example, to access the custom IPv4 options for a shared network named *Shared*, navigate to:

   services » dhcpserver » shared-network » Shared » options » client » custom

   To access custom IPv4 options at the global level, navigate to:

   services » dhcpserver » options » client » custom
3. Delete the custom option by typing:
   - **For IPv4**

     ```
     no services dhcpserver { path } options client custom
     { number }
     ```
   - **For IPv6**

     ```
     no services dhcpserver6 options client custom { num
     ber }
     ```

   Where:
   - { path } is the path to and name of the desired shared network, subnet, host group or host
   - { number } is the option number
4. Type `commit` and press **Enter** to save 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, type:

- **For IPv4**
  `show running-config services dhcpserver interface`
- **For IPv6**
  `show running-config services dhcpserver6 interface`

If DHCP listen interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver interface | tab
NAME
-------------
switch.0001

 !
!
```

If no DHCP listen interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a DHCP Listen Interface" (Page 288).

7.3.6.2 Adding a DHCP Listen Interface

To add a DHCP listen interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the interface by typing:
   - **For IPv4**
     `services dhcpserver interface { name }`
   - **For IPv6**
     `services dhcpserver6 interface { name }`

   Where:
   - `{ name }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

7.3.6.3 Deleting a DHCP Listen Interface

To delete a DHCP listen interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the interface by typing:
   - **For IPv4**
     `no services dhcpserver interface { name }`

- **For IPv6**

  ```
  no services dhcpserver6 interface { name }
  ```

  Where:

  - `{ name }` is the name of the interface

3. Type `commit` and press **Enter** to save the changes.

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, type:

- **For IPv4**

  ```
  show running-config services dhcpserver shared-network
  ```

- **For IPv6**

  ```
  show running-config services dhcpserver6 shared-network
  ```

If shared networks have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver shared-network
services
 dhcpserver
  shared-network Shared
   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
   !
  !
 !
!
```

If no shared networks have been configured, add shared networks as needed. For more information, refer to "Adding a Shared Network" (Page 290).

7.3.7.2 Adding a Shared Network

To add a shared network to the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the shared network by typing:
   - **For IPv4**
     ```
     services dhcpserver shared-network { name }
     ```
   - **For IPv6**
     ```
     services dhcpserver6 shared-network { name }
     ```

   Where:
   - `{ name }` is the name of the shared network
3. Configure options for the shared network. For more information, refer to "Configuring Shared Network Options" (Page 290).
4. Type `commit` and press **Enter** to save the changes.

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. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For IPv4**
     ```
     services dhcpserver shared-network { shared network }
     options
     ```
   - **For IPv6**
     ```
     services dhcpserver6 shared-network { shared network }
     options
     ```
3. Configure the leased time settings by configuring the following parameter(s) as required:

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.

Parameter	Description
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. Configure the client by configuring the following parameter(s) 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 293).

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [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.
`option82`	Enables/disables the NAK of option 82 clients for this subnet.

5. [Optional] Configure configuration options for DHCP clients at the shared network level. For more information, refer to refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 282) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 284).
6. Type `commit` and press **Enter** to save the changes.

7.3.7.4 Deleting a Shared Network

To delete a shared network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the shared network by typing:
   - **For IPv4**
     ```
     no services dhcpserver shared-network { name }
     ```
   - **For IPv6**
     ```
     no services dhcpserver6 shared-network { name }
     ```

   Where:
   - `{ name }` is the name of the shared network
3. Type `commit` and press **Enter** to save the changes.

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, type:

- **For IPv4**
  ```
  show running-config services dhcpserver subnet-name
  ```
- **For IPv6**
  ```
  show running-config services dhcpserver6 subnet6-name
  ```

If subnets have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver subnet-name network-ip | tab
NAME  NETWORK IP
----------------------
SUB1  192.168.0.0/27
SUB2  192.168.0.32/27

 !
!
```

If no subnets have been configured, add subnets as needed. For more information, refer to "Adding a Subnet" (Page 293).

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 290).

1. Make sure the CLI is in Configuration mode.
2. Add the subnet by typing:
   - **For IPv4**

     ```
     services dhcpserver subnet-name { name }
     ```

   - **For IPv6**

     ```
     services dhcpserver6 subnet6-name { name }
     ```

   Where:

   - `{ name }` is the name of the subnet
3. Configure the following parameter(s) as required:

Parameter	Description
`network-ip { network-ip }`	**Synopsis:** A string between 9 and 18 characters long The network IP address for this subnet.
`shared-network { shared-network }`	**Synopsis:** A string between 1 and 32 characters long The shared-network that this host belongs to.
`network-ip { network-ip }`	**Synopsis:** A string between 4 and 43 characters long The network IPv6 address for this subnet.
`shared-network { shared-network }`	**Synopsis:** A string between 1 and 32 characters long The shared-network that this host belongs to.

4. Configure the options for the subnet. For more information, refer to "Configuring Subnet Options" (Page 293).
5. Type `commit` and press **Enter** to save the changes.

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. Make sure the CLI is in Configuration mode.

2. Navigate to:
   - **For IPv4**
     ```
     services dhcpserver subnet-name { name } options
     ```
   - **For IPv6**
     ```
     services dhcpserver6 subnet6-name { name } options
     ```

   Where:
   - `{ name }` is the name of the subnet
3. Configure the leased time settings by configuring the following parameter(s):
   - **For IPv4:**

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

   - **For IPv6:**

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. Configure the client settings by configuring the following parameter(s):

⚠ 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 IPv4**

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients
`option82`	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.

- **For IPv6**

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [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.

5. [Optional] Configure configuration options for DHCP clients at the subnet level. For more information, refer to refer to "Configuring Standard DHCP Client Configuration Options (IPv4)" (Page 282) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 284).
6. Configure one or more address pools to the subnet. For more information, refer to "Adding an Address Pool (IPv4)" (Page 304) or "Adding an Address Pool (IPv6)" (Page 306).
7. Configure one or more IP ranges to the subnet. For more information, refer to "Adding an IP Range (IPv4)" (Page 308) or "Adding an IP Range (IPv6)" (Page 310).
8. Type `commit` and press **Enter** to save the changes.

7.3.8.4 Deleting a Subnet

To delete a subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the subnet by typing:
   - **For IPv4**
     ```
     no services dhcpserver subnet-name { name }
     ```
   - **For IPv6**
     ```
     no services dhcpserver6 subnet6-name { name }
     ```

   Where:
   - `{ name }` is the name of the subnet
3. Type `commit` and press **Enter** to save the changes.

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, type:

- **For IPv4**
  ```
  show running-config services dhcpserver host-groups
  ```
- **For IPv6**
  ```
  show running-config services dhcpserver6 host-groups
  ```

If host groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver host-groups
services
 dhcpserver
  host-groups "Local Group"
   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
    !
   !
```

```
  !
 !
!
```

If no host groups have been configured, add host groups as needed. For more information, refer to "Adding a Host Group" (Page 297).

7.3.9.2 Adding a Host Group

To add a host group to the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For IPv4**
     `services dhcpserver host-groups`
   - **For IPv6**
     `services dhcpserver6 host-groups`
3. Configure the following parameter(s) as required:

Parameter	Description
`name { name }`	**Synopsis:** A string between 1 and 32 characters long The description of the host groups.

4. Configure the options for the host group. For more information, refer to "Configuring Host Group Options" (Page 297).
5. Type `commit` and press **Enter** to save the changes.

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. Make sure the CLI is in Configuration mode.
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to:
   - **For IPv4**
     services » dhcpserver » host-groups » { host } » options
   - **For IPv6**
     services » dhcpserver6 » host-groups » { host } » options

   Where { host } is the name of the host group.

4. Configure the leased time settings by configuring the following parameter(s):
   - **For IPv4:**

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

   - **For IPv6:**

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

5. Configure the client settings by configuring the following parameter(s):
   - **For IPv4**

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients
`shared-network { shared-network }`	**Synopsis:** A string between 1 and 32 characters long The shared-network that this host belongs to.
`subnet { subnet }`	**Synopsis:** A string between 1 and 32 characters long The subnet that this host belongs to.

   - **For IPv6**

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients
`shared-network { shared-network }`	**Synopsis:** A string between 1 and 32 characters long The shared-network that this host belongs to.

Parameter	Description
`subnet6 { subnet6 }`	**Synopsis:** A string between 1 and 32 characters long The subnet that this host belongs to.

6. [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 282) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 284).
7. Type `commit` and press **Enter** to save the changes.

7.3.9.4 Deleting a Host Group

To delete a host group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the host group by typing:
   - **For IPv4**
     ```
     no services dhcpserver host-groups { name }
     ```
   - **For IPv6**
     ```
     no services dhcpserver6 host-groups { name }
     ```

   Where:
   - `{ name }` is the name of the host group
3. Type `commit` and press **Enter** to save the changes.

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, type:

- **For IPv4**
  ```
  show running-config services dhcpserver host
  ```
- **For IPv6**
  ```
  show running-config services dhcpserver6 host
  ```

If hosts have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver host APE-INT
```

```
services
 dhcpserver
  host APE-INT
   options
    hardware mac 00:01:C0:0B:B7:71
    fixed-ip       192.168.0.60
    unknown-client allow
    subnet         SUB2
    client
     hostname APE-INT
     no subnetmask
     no default-route
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
   !
  !
 !
!
```

If no hosts have been configured, add hosts as needed. For more information, refer to "Adding a Host" (Page 300).

7.3.10.2 Adding a Host

To add a host to the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the host by typing:
   - **For IPv4**
     `services dhcpserver host { name }`
   - **For IPv6**
     `services dhcpserver6 host { name }`

   Where:
   - `{ name }` is the name of the host
3. Configure options for the host. For more information, refer to "Configuring Host Options" (Page 300).
4. Type `commit` and press **Enter** to save the changes.

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. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » hosts » { host } » options
   - **For IPv6**
     services » dhcpserver6 » hosts » { host } » options

   Where { host } is the name of the host.
3. Configure the hardware settings by configuring the following parameter(s):

Parameter	Description
`type { type }`	**Synopsis:** [fddi | token-ring | ethernet] **Default:** ethernet The type of network hardware used by the client, associated with the host entry.
`mac { mac }`	**Synopsis:** A string up to 17 characters long The physical network address of the client. Note that this corresponds to the hardware type; for example, the MAC address for the ethernet.

4. Configure the leased time settings by configuring the following parameter(s):

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

5. Configure the client settings by configuring the following parameter(s):
   - **For IPv4**

Parameter	Description
`fixed-ip { fixed-ip }`	**Synopsis:** A string between 7 and 15 characters long The IP address that the server assigns to the matching client.
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients
`shared-network { shared-network }`	**Synopsis:** A string between 1 and 32 characters long The shared-network that this host belongs to.

Parameter	Description
`subnet { subnet }`	**Synopsis:** A string between 1 and 32 characters long The subnet that this host belongs to.
`host-groups { host-groups }`	**Synopsis:** A string between 1 and 32 characters long The host groups that this host belongs to.

- **For IPv6**

Parameter	Description
`fixed-ip { fixed-ip }`	**Synopsis:** A string between 6 and 40 characters long The IPv6 address that the server assigns to the matching client.
`fixed-prefix6 { fixed-prefix6 }`	**Synopsis:** A string between 4 and 43 characters long The IPv6 prefix delegation that the server assigns to the matching client.
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients
`shared-network { shared-network }`	**Synopsis:** A string between 1 and 32 characters long The shared-network that this host belongs to.
`subnet6 { subnet6 }`	**Synopsis:** A string between 1 and 32 characters long The subnet that this host belongs to.
`host-groups { host-groups }`	**Synopsis:** A string between 1 and 32 characters long The host groups that this host belongs to.

6. [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 282) or "Configuring Standard DHCP Client Configuration Options (IPv6)" (Page 284).
7. Type `commit` and press **Enter** to save the changes.

7.3.10.4 Deleting Hosts

To delete a host, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the host by typing:
   - **For IPv4**

     ```
     no services dhcpserver host { name }
     ```

- **For IPv6**

  ```
  no services dhcpserver6 host { name }
  ```

  Where:

  - `{ name }` is the name of the host

3. Type `commit` and press **Enter** to save the changes.

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)

To view a list of address pools configured for a DHCP subnet, type:

```
show running-config services dhcpserver subnet-name { name }
options ippool
```

Where:

- `{ name }` is the name of the subnet

If pools have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver subnet-name Local options ip
pool
services
 dhcpserver
  subnet Local
   options
    ippool pool1
     no unknown-client
     iprange 172.0.0.0
      end 172.0.0.1
     !
     option82 class1
      remote-id  00:00:00:01:03:01
      circuit-id 00:00:00:01:01:01
     !
    !
   !
  !
 !
!
```

If no IP pools have been configured, add pools as needed. For more information, refer to "Adding an Address Pool (IPv4)" (Page 304).

7.3.11.2 Adding an Address Pool (IPv4)

To add an address pool to a DHCP subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address pool by typing:

   ```
   services dhcpserver subnet-name { name } options ippool
   { description }
   ```

   Where:

   - `{ name }` is the name of the subnet
   - `{ description }` is the name of the IP pool
3. Configure the leased time settings by configuring the following parameter(s):

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. Configure the client and failover settings by configuring the following parameter(s):

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients
`failover-peer { failover-peer }`	**Synopsis:** A string between 7 and 15 characters long The IP address of a DHCP peer server if a failover pool is created.

5. Add one or more IP ranges to the pool. For more information, refer to "Adding an IP Range (IPv4)" (Page 308).
6. Add one or more Option82 classes to the pool. For more information, refer to "Adding an Option 82 Class to an Address Pool" (Page 319).
7. Type `commit` and press **Enter** to save the changes.

7.3.11.3 Deleting an Address Pool (IPv4)

To delete an address pool, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the address pool by typing:

   ```
   no services dhcpserver subnet-name { name } options ippool
   { description }
   ```

   Where:

   - `{ name }` is the name of the subnet
   - `{ description }` is the name of the IP pool

3. Type `commit` and press **Enter** to save the changes.

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)

To view a list of address pools configured for a DHCP subnet, type:

```
show running-config services dhcpserver6 subnet6-name
{ name } options ippool6
```

Where:

- `{ name }` is the name of the subnet

If pools have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name options ippool6
services
 dhcpserver6
  subnet6-name Sub
   options
    ippool6 Pool1
     iprange6 2001:db8:2728::2221
      end 2001:db8:2728::2230
     !
    !
   !
  !
 !
!
!
```

If no IP pools have been configured, add pools as needed. For more information, refer to "Adding an Address Pool (IPv6)" (Page 306).

7.3.12.2 Adding an Address Pool (IPv6)

To add an address pool to a DHCP subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address pool by typing:

   ```
   services dhcpserver6 subnet6-name { name } options ippool6
   { ippoolname }
   ```

   Where:

   - `{ name }` is the name of the subnet
   - `{ ippoolname }` is the name of the IPv6 pool
3. Configure the leased time settings by configuring the following parameter(s):

Parameter	Description
`default { default }`	**Synopsis:** An integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
`maximum { maximum }`	**Synopsis:** An integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. Configure the client and failover settings by configuring the following parameter(s):

Parameter	Description
`unknown-client { unknown-client }`	**Synopsis:** [allow | deny | ignore] The action to take for previously unregistered clients

5. [Optional] Add one or more IP ranges to the pool. For more information, refer to "Adding an IP Range (IPv6)" (Page 310).
6. [Optional] Add one or more subnets to the pool. For more information, refer to "Adding a IPv6 Subnet" (Page 316).
7. [Optional] Add one or more temporary subnets to the pool. For more information, refer to "Adding a Temporary Subnet" (Page 314).
8. [Optional] Add one or more prefixes to the pool. For more information, refer to "Adding an IPv6 Prefix" (Page 312).
9. Type `commit` and press **Enter** to save the changes.

7.3.12.3 Deleting an Address Pool (IPv6)

To delete an address pool, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address pool by typing:

   ```
   no services dhcpserver subnet6-name { name } options ip
   pool6 { ippoolname }
   ```

   Where:

   - `{ name }` is the name of the subnet
   - `{ ippoolname }` is the name of the IPv6 pool
3. Type `commit` and press **Enter** to save the changes.

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:

Enter one of the following commands:

Note

A DHCP subnet or one of its associated address pools must be configured to view a list of IP ranges.

- **For DHCP subnets**

  ```
  show running-config services dhcpserver subnet-name
  { name } options iprange
  ```

- **For an address pool**

  ```
  show running-config services dhcpserver subnet-name
  { name } options ippool { description } iprange
  ```

Where:

- { name } is the name of the subnet
- { description } (if applicable) is the name of the address pool

If ranges have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver subnet-name Local options
 iprange
services
 dhcpserver
  subnet Local
   options
    iprange 172.30.144.251
     end 172.30.144.254
    !
   !
  !
 !
!
```

If no IP ranges have been configured, add ranges as needed. For more information, refer to "Adding an IP Range (IPv4)" (Page 308) or "Adding an IP Range (IPv6)" (Page 310).

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 the CLI is in Configuration mode.
2. Make sure a DHCP subnet or one of its associated address pools have been configured.
3. Add the IP range by typing:
   - **For a DHCP subnet**

     ```
     services dhcpserver subnet-name { name } options
     iprange { start } end { end }
     ```

   - **For an address pool**

     ```
     services dhcpserver subnet-name { name } options ippool
     { description } iprange { start } end { end }
     ```

   Where:
   - { name } is the name of the subnet
   - { description } (if applicable) is the name of the address pool
   - { start } is the starting IP address pool the server uses to offer to the client
   - { end } is the ending IP address pool the server uses to offer to the client
4. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Make sure a DHCP subnet or one of its associated address pools have been configured.
3. Delete the IP range by typing:
   - **For a DHCP subnet**

     ```
     no dhcpserver subnet-name { name } options iprange
     { start } end { end }
     ```

   - **For an address pool**

     ```
     no services dhcpserver subnet-name { name } options ip
     pool { description } iprange { start } end { end }
     ```

   Where:
   - { name } is the name of the subnet
   - { description } (if applicable) is the name of the address pool
   - { start } is the starting IP address pool the server uses to offer to the client
   - { end } is the ending IP address pool the server uses to offer to the client
4. Type `commit` and press **Enter** to save the changes.

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:

Enter one of the following commands:

Note

A DHCP subnet or one of its associated address pools must be configured to view a list of IP ranges.

- **For DHCP IPv6 subnets**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options iprange6
  ```

- **For an IPv6 address pool**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options ippool6 { description } iprange6
  ```

Where:

- { name } is the name of the subnet
- { description } (if applicable) is the name of the address pool

If ranges have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub options
 iprange6
services
 dhcpserver6
  subnet6-name sub
   options
    iprange6 2001:db8:2728::2200
     end 2001:db8:2728::2220
    !
   !
  !
 !
!
!
```

If no IP ranges have been configured, add ranges as needed. For more information, refer to "Adding an IP Range (IPv6)" (Page 310).

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 the CLI is in Configuration mode.
2. Make sure a DHCP subnet or one of its associated address pools have been configured.
3. Add the IP range by typing:

   - **For a DHCP IPv6 subnet**

     ```
     services dhcpserver6 subnet6-name { name } options
     iprange6 { start } end { end }
     ```

   - **For an IPv6 address pool**

     ```
     services dhcpserver6 subnet6-name { name } options ip
     pool6 { description } iprange6 { start } end { end }
     ```

   Where:

- { name } is the name of the subnet
- { description } (if applicable) is the name of the address pool
- { start } is the starting IP address pool the server uses to offer to the client
- { end } is the ending IP address pool the server uses to offer to the client

4. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Delete the IP range by typing:
   - **For a DHCP IPv6 subnet**

     ```
     no dhcpserver6 subnet6-name { name } options iprange6
     { start } end { end }
     ```

   - **For an IPv6 address pool**

     ```
     no services dhcpserver6 subnet6-name { name } options
     ippool6 { description } iprange6 { start } end { end }
     ```

   Where:
   - { name } is the name of the subnet
   - { description } (if applicable) is the name of the address pool
   - { start } is the starting IP address pool the server uses to offer to the client
   - { end } is the ending IP address pool the server uses to offer to the client
3. Type `commit` and press **Enter** to save the changes.

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:

Enter the following command:

Note

A DHCP subnet must be configured to view a list of prefixes.

- **For DHCP IPv6 subnets**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options prefix6
  ```

- **For an IPv6 address pool**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options ippool6 { description } prefix6
  ```

Where:

- { name }is the name of the subnet
- { description }(if applicable) is the name of the address pool

If prefixes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub2 options pre
fix6
services
 dhcpserver6
  subnet6-name sub2
   options
    prefix6 2001:db8:28d2:f0::
     end  2001:db8:28d2:f0::
     bits 60
    !
   !
  !
 !
!
```

If no prefixes have been configured, add ranges as needed. For more information, refer to"Adding an IPv6 Prefix" (Page 312).

7.3.15.2 Adding an IPv6 Prefix

To add a prefix, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a DHCP subnet has been configured.
3. Add the prefix by typing:
   - **For a DHCP IPv6 subnet**

     ```
     services dhcpserver6 subnet6-name { name } options pre
     fix6 { prefix }
     ```

   - **For an IPv6 address pool**

     ```
     services dhcpserver6 subnet6-name { name } options ip
     pool6 { description } prefix6 { prefix }
     ```

Where:

- { name }is the name of the subnet
- { description }(if applicable) is the name of the address pool
- { prefix }is the starting IPv6 prefix delegation

4. Configure the IPv6 Range Configuration by configuring the following parameter(s) as required:

Parameter	Description
`end { end }`	**Synopsis:** A string between 6 and 40 characters long The ending IPv6 prefix delegation that the server uses to offer to the client.
`bits { bits }`	**Synopsis:** An integer between 1 and 64 Prefix delegations of bits length that are offered to the client.

5. Type `commit` and press **Enter** to save the changes.

7.3.15.3 Deleting an IPv6 Prefix

To delete a prefix, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the prefix by typing:
   - **For a DHCP IPv6 subnet**

     ```
     no services dhcpserver6 subnet6-name { name } options
     prefix6 { prefix }
     ```

   - **For an IPv6 address pool**

     ```
     no services dhcpserver6 subnet6-name { name } options
     ippool6 { description } prefix6 { prefix }
     ```

   Where:

   - { name }is the name of the subnet
   - { description }(if applicable) is the name of the address pool
   - { prefix }is the starting IPv6 prefix delegation
3. Type `commit` and press **Enter** to save the changes.

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:

Enter the following command:

Note

A DHCP subnet must be configured to view a list of temporary subnets.

- **For DHCP IPv6 subnets**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options temporarysubnet6
  ```

- **For an IPv6 address pool**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options ippool6 { description } temporarysubnet6
  ```

Where:

- { name } is the name of the subnet
- { description }(if applicable) is the name of the address pool

If temporary subnets have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub2 options tem
porarysubnet6
services
 dhcpserver6
  subnet6-name sub2
   options
    temporarysubnet6 2001:db8:28d2::/112
    !
   !
  !
 !
!
!
```

If no prefixes have been configured, add ranges as needed. For more information, refer to "Adding an IPv6 Prefix" (Page 312).

7.3.16.2 Adding a Temporary Subnet

To add a temporary subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a DHCP subnet has been configured.
3. Add the prefix by typing:
   - **For a DHCP IPv6 subnet**

     ```
     services dhcpserver6 subnet6-name { name } options tem
     porarysubnet6 { temporaryname }
     ```

- **For an IPv6 address pool**

  ```
  services dhcpserver6 subnet6-name { name } options ip
  pool6 { description } temporarysubnet6 { temporary IPv4
  subnet }
  ```

  Where:

  - { name } is the name of the subnet
  - { description }(if applicable) is the name of the address pool
  - { temporaryname } is the name of the temporary subnet

4. Type `commit` and press **Enter** to save the changes.

7.3.16.3 Deleting a Temporary Subnet

To delete a prefix, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the prefix by typing:

   - **For a DHCP IPv6 subnet**

     ```
     no services dhcpserver6 subnet6-name { name } options
     temporarysubnet6 { temporaryname }
     ```

   - **For an IPv6 address pool**

     ```
     no services dhcpserver6 subnet6-name { name } options
     ippool6 { description } temporarysubnet6 { temporary
     name }
     ```

   Where:

   - { name } is the name of the subnet
   - { description }(if applicable) is the name of the address pool
   - { temporaryname } is the name of the temporary subnet

3. Type `commit` and press **Enter** to save the changes.

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:

Enter the following command:

Note

A DHCP subnet must be configured to view a list of IPv6 subnets.

- **For DHCP IPv6 subnets**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options subnet6
  ```

- **For an IPv6 address pool**

  ```
  show running-config services dhcpserver6 subnet6-name
  { name } options ippool6 { description } subnet6
  ```

Where:

- { name }is the name of the subnet
- { description }(if applicable) is the name of the address pool

If IPv6 subnets have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub2 options sub
net6
services
 dhcpserver6
  subnet6-name sub2
   options
    subnet6 2001:db8:28d2::/64
    !
   !
  !
 !
!
```

If no prefixes have been configured, add ranges as needed. For more information, refer to"Adding an IPv6 Prefix" (Page 312).

7.3.17.2 Adding a IPv6 Subnet

To add a IPv6 subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a DHCP subnet has been configured.
3. Add the IPv6 subnet by typing:
   - **For a DHCP IPv6 subnet**

     ```
     services dhcpserver6 subnet6-name { name } options sub
     net6 { subnet6name }
     ```

   - **For an IPv6 address pool**

     ```
     services dhcpserver6 subnet6-name { name } options ip
     pool6 { description } subnet6 { IPv6 subnet }
     ```

   Where:

- { name }is the name of the subnet
- { description }(if applicable) is the name of the address pool
- { subnet6name }is the name of the IPv6 subnet

4. Configure the following parameter(s) as required:

Parameter	Description
`subnet-number { subnet-number }`	**Synopsis:** A string between 4 and 43 characters long The IPv6 subnet that the server uses to offer to the client.

5. Type `commit` and press **Enter** to save the changes.

7.3.17.3 Deleting an IPv6 Subnet

To delete an IPv6 subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the prefix by typing:
   - **For a DHCP IPv6 subnet**

     ```
     no services dhcpserver6 subnet6-name { name } options
     subnet6 { subnet6name }
     ```

   - **For an IPv6 address pool**

     ```
     no services dhcpserver6 subnet6-name { name } options
     ippool6 { description } subnet6 { subnet6name }
     ```

   Where:
   - { name }is the name of the subnet
   - { description }(if applicable) is the name of the address pool
   - { subnet6name }is the name of the IPv6 subnet
3. Type `commit` and press **Enter** to save the changes.

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 281) or "Configuring Subnet Options" (Page 293).

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:

Type:

Note

An address pool must be configured to view a list of Option 82 classes.

```
show running-config services dhcpserver subnet-name { name }
options ippool { description } option82
```

Where:

- `{ name }` is the name of the subnet
- `{ description }` is the name of the address pool

If classes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services dhcpserver subnet Local options ippool
 pool1 option82
services
 dhcpserver
  subnet Local
   options
    ippool pool1
     option82 class1
      remote-id  00:00:00:01:03:01
      circuit-id 00:00:00:01:01:01
     !
    !
   !
  !
 !
!
```

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 319).

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 the CLI is in Configuration mode.
2. Make sure an address pool has been configured.
3. Add the pool by typing:

```
services dhcpserver subnet-name { name } options ippool
{ description } option82 { class }
```

Where:

- `{ name }` is the name of the subnet
- `{ description }` is the name of the address pool
- `{ class }` is the name of the Option82 class

4. Configure the following parameter(s) as required:

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 { remote-id }`	**Synopsis:** A string up to 17 characters long Specifies the information relating to the remote host end of the circuit.
`circuit-id { circuit-id }`	**Synopsis:** A string up to 17 characters long Specifies the local information to which circuit the request came in on (ie. 00:02:03:02)

5. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Delete the class by typing:

```
no services dhcpserver subnet-name { name } options ippool
{ description } option82 { class }
```

Where:

- `{ name }` is the name of the subnet
- `{ description }` is the name of the address pool

- `{ class }` is the name of the Option82 class

3. Type `commit` and press **Enter** to save the changes.

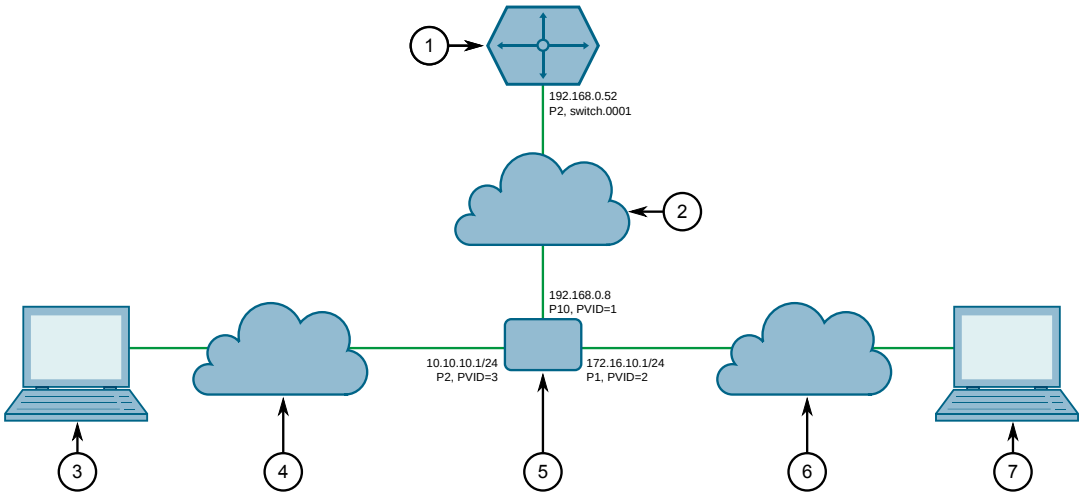
7.3.19 Example: Configuring the Device as a DHCP Server to Support a Relay Agent

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.



① DHCP Server (RUGGEDCOM ROX II Device)
② LAN A
③ Client 2
④ LAN B
⑤ DHCP Relay Agent
⑥ LAN C
⑦ Client 1

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 277) for more information.

2. Enable the DHCP server. For more information, refer to "Enabling/Disabling the DHCP Server" (Page 281).
3. Add the management interface (switch.0001) as a DHCP listen interface. For more information, refer to "Adding a DHCP Listen Interface" (Page 288).
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 269) or "Adding an IPv6 Address" (Page 270).
5. Create a shared network named *LAN.10-LAN.172* and enable Option82. For more information, refer to "Configuring Shared Network Options" (Page 290).
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 293).

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 282).
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 304) or "Adding an Address Pool (IPv6)" (Page 306).

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 319).

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 282).
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 304) or "Adding an Address Pool (IPv6)" (Page 306).

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 319).

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, type:

```
show running-config dns search
```

If domain names have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin dns search
admin
 dns
  search ruggedcom.com
  !
 !
!
```

If no domain names have been configured, add names as needed. For more information, refer to "Adding a Domain Name" (Page 325).

7.4.1.2 Adding a Domain Name

To add a domain name, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the domain name by typing:

   ```
   admin dns search { name }
   ```

   Where:

   - `{ name }` is the name of the domain
3. Type `commit` and press **Enter** to save the changes.

7.4.1.3 Deleting a Domain Name

To delete a domain name, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the domain name by typing:

   ```
   no admin dns search { name }
   ```

   Where:

   - `{ name }` is the name of the domain
3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config dns server
```

If domain name servers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin dns server
admin
 dns
  server 10.1.1.1
  !
 !
!
```

If no domain name servers have been configured, add servers as needed. For more information, refer to "Adding a Domain Name Server" (Page 326).

7.4.2.2 Adding a Domain Name Server

To add a domain name server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the domain name server by typing:

   ```
   admin dns server { address }
   ```

   Where:

   - `{ address }` is the IP address of the domain name server.
3. Type `commit` and press **Enter** to save the changes.

7.4.2.3 Deleting a Domain Name Server

To delete a domain name server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the domain name server by typing:

   ```
   no admin dns server { address }
   ```

   Where:

   - `{ address }` is the IP address of the domain name server.
3. Type `commit` and press **Enter** to save the changes.

7.5 Managing Dynamic DNS

Enable the Dynamic Domain Name Server (DNS) service in RUGGEDCOM ROX II to allow remote hosts to connect with the device's default interface via a fixed host name. The Dynamic DNS service uses a DNS client to log into a DNS service provider and register the assigned host name(s) that can be used to access the device via the Internet.

An account is required with one of the supported dynamic DNS service providers:

- noip.com [http://www.noip.com]
- dyn.com [http://www.dyn.com]

Responses from each Dynamic DNS service provider are validated by the Dynamic DNS client. If a response is determined to be invalid, a *DDNS Bad Response* alarm is raised and the service is temporarily disabled. Service can only be restored once the alarm has been cleared. For information about how to configure this alarm, refer to "Configuring an Alarm" (Page 148).

7.5.1 Enabling and Configuring Dynamic DNS

To enable and configure dynamic DNS, do the following:

⚠ NOTICE

Update requests are sent to the selected service provider via HTTPS. Before enabling Dynamic DNS, the Public CA Store must be enabled, or a CA for DDNS must be added to the store.

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 215).

For more information about enabling the Public CA Store, refer to "Enabling/ Disabling the Trusted Certificate Store" (Page 192).

1. Make sure the CLI is in Configuration mode.
2. Enable the dynamic DNS client by typing:

   ```
   services ddns enabled true
   ```

3. Type `options` and then configure the following parameter(s) as required:

Parameter	Description
`ip-check-interval { ip-check-interval }`	**Synopsis:** An integer between 600 and 864000 **Default:** 1800 The time in seconds to wait before the IP address of the device is queried. If the address has changed, the new address is updated on the domain name service (DNS) server. The value of **IP Address Check Interval** should be less than the value of **Force Update Interval.**
`force-update-interval { force-update-interval }`	**Synopsis:** An integer between 600 and 2592000 **Default:** 86400 The time in seconds to wait before the IP address of the device is updated on the domain name service (DNS) server, even if the address has not changed. The value of **Force Update Interval** should be greater than the value of **IP Address Check Interval.**

4. Type `commit` and press **Enter** to save the changes.

7.5.2 Managing Dynamic DNS Servers

This section describes how to configure a connection with one or more of the supported dynamic DNS service providers.

7.5.2.1 Viewing a List of Dynamic DNS Servers

To view a list of WLAN aliases, type:

```
show running-config services ddns servers
```

```
ruggedcom# show running-config services ddns servers | tab
SERVER  ENABLED  USERNAME  PASSWORD                    HOSTNAME
-----------------------------------------------------------------
dyndns  true     admin     $4$wIo7Yd068FRwhYYI0d4IDw==
                                                      host1
noip    true     admin     $4$wIo7Yd068FRwhYYI0d4IDw==
                                                      host2

 !
!
```

If no dynamic DNS servers have been configured, add servers as needed. For more information, refer to "Adding a Dynamic DNS Server" (Page 329).

7.5.2.2 Viewing the Status of a Dynamic DNS Server

To view the status of a dynamic DNS server, type:

```
show services ddns servers [ noip | dyndns ] status
```

If the selected dynamic DNS server is enabled, a table or list similar to the following example appears:

```
ruggedcom# show services ddns servers dyndns status
status
 ddns state Enabled
 details
  ddns last success        "Wed Jan 25 11:18:39 2017"
  ddns last ip address     205.206.34.228
  ddns last failure        "Not available"
  ddns last failure reason "Not available"
```

The table/list provides the following information:

Parameter	Description
`ddns-state`	**Synopsis:** A string Displays DDNS state
`ddns-last-success`	**Synopsis:** A string Last successful update date and time
`ddns-last-ip-address`	**Synopsis:** A string Last successful update IP address
`ddns-last-failure`	**Synopsis:** A string Last failed update attempt date and time

Parameter	Description
`ddns-last-failure-reason`	**Synopsis:** A string Last failed update attempt reason

7.5.2.3 Adding a Dynamic DNS Server

To add a dynamic DNS server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the dynamic DNS server by typing:

   ```
   services ddns servers [ dyndns | noip ]
   ```

3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false Enables / disables DDNS updates for the server
`username { username }`	**Synopsis:** A string between 2 and 24 characters long The username of the DDNS server
`password { password }`	**Synopsis:** A string The password of the DDNS server

4. Define one or more host names for the server. For more information, refer to "Adding a Host Name" (Page 330).
5. Type `commit` and press **Enter** to save the changes.

7.5.2.4 Deleting a Dynamic DNS Server

To delete a dynamic DNS server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the dynamic DNS server by typing:

   ```
   no services ddns servers [ dyndns | noip ]
   ```

3. Type `commit` and press **Enter** to save the changes.

7.5.3 Managing Dynamic DNS Server Host Names

This section describes how to manage host names for the configured dynamic DNS servers.

⚠ NOTICE
At least one host name is required for each configured dynamic DNS server.

7.5.3.1 Viewing a List of Host Names

To view a list of WLAN aliases, type:

```
show running-config services ddns servers [ dyndns | noip ]
hostnames
```

If host names have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services ddns servers noip hostnames
services
 ddns
  servers noip
   hostnames host1
   !
  !
 !
!
```

If no host names have been configured, add host names as needed. For more information, refer to "Adding a Host Name" (Page 330).

7.5.3.2 Adding a Host Name

To add a host name for a dynamic DNS server, do the following:

⚠ NOTICE
At least one host name is required for each configured dynamic DNS server.

1. Make sure the CLI is in Configuration mode.
2. Add the host name by typing:

   ```
   services ddns servers [ dyndns | noip ] hostnames { name }
   ```

   Where { name } is the host name to be updated by the dynamic DNS server.
3. Type `commit` and press **Enter** to save the changes.

7.5.3.3 Deleting a Host Name

To delete a host name, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the dynamic DNS server by typing:

   ```
   no services ddns servers [ dyndns | noip ] hostnames
   { name }
   ```

   Where { name } is the desired host name.

3. Type `commit` and press **Enter** to save the changes.

8 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » link-detect***.
3. Configure the following parameters as needed:

Parameter	Description
`fast-link-detect { fast-link-detect }`	**Synopsis:** [on | off | portguard] **Default:** portguard The state of fast link detection. Options include: • **portguard** (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. • **on**: 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

Parameter	Description
	detection on the port in question. If excessive link state changes persist for more than 2 minutes, an alarm will be 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. • **off**: 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.
`link-detect-time` `{ link-detect-time }`	**Synopsis:** An integer between 100 and 1000 **Default:** 100 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.

4. Type `commit` and press **Enter** to save 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, type:

```
show running-config interface switch
```

If switched Ethernet ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface switch
interface
 switch lm1 1
  auton      on
  speed      auto
  duplex     auto
  switchport
  no flow-control
  no alias
  rate-limiting
   no ingress-limit
   no egress-limit
  !
  port-security
   no shutdown-time
   no admin-shutdown
   dot1x
```

```
    no reauth-enable
   !
  !
  lldp
   no notify
  !
  mcast-filtering
   no gmrp
  !
  cos
   no inspect-tos
  !
  vlan
   pvid 1
   no gvrp-mode
  !
  spanning-tree
   no restricted-role
   no restricted-tcn
  !
 !
.
.
.
```

8.2.2 Configuring a Switched Ethernet Port

To configure a switched Ethernet port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » switch » { slot } » { port }***, where { slot } is the module and { port } is the switched Ethernet port.
3. Configure the port settings by configuring 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.

Note

For information about configuring port rate limiting, refer to "Configuring Port Rate Limiting" (Page 940).

Note

For information about configuring RMON threshold alerts, refer to "Configuring RMON Threshold Alerts" (Page 340).

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true 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.
`auton { auton }`	**Synopsis:** [on | off] 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.
`speed { speed }`	**Synopsis:** [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). 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.
`duplex { duplex }`	**Synopsis:** [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 { link-alarms }`	**Synopsis:** [true | false] **Default:** true Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link

Parameter	Description
	alarms may also be controlled for the whole system under admin / alarm-cfg.
`switchport { switch port }`	**Synopsis:** [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-src { ip-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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.
`proxyarp`	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface). **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1500 bytes (jumbo frames) up to 9216 bytes on Gigabit Ethernet ports only.
`alias { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface

4. Configure the LLDP settings by configuring the following parameter(s) as required:

Parameter	Description
`admin-status { admin-status }`	**Synopsis:** [tx-only | rx-only | rx-tx | no-lldp] **Default:** rx-tx • no-lldp : The local LLDP agent can neither transmit nor receive LLDP frames.

Parameter	Description
	• rxTx : The local LLDP agent can both transmit and receive LLDP frames through the port. • txOnly : The local LLDP agent can only transmit LLDP frames. • rxOnly : The local LLDP agent can only receive LLDP frames.
`notify`	Disabling notifications will prevent sending notifications and generating alarms for a particular interface from the LLDP agent.

Note

Multicast filtering, CoS and VLAN parameters are only available when the port is in switchport mode.

5. Configure the Multicast filtering settings by configuring the following parameter(s) as required:

Parameter	Description
`gmrp { gmrp }`	**Synopsis:** [advertise_only | learn_advertise] GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: • DISABLED : the port is not capable of any GMRP processing. • ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

6. Configure the CoS settings by configuring the following parameter(s) as required:

Parameter	Description
`default-priority { default-priority }`	**Synopsis:** An integer between 0 and 7 **Default:** 0 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).
`inspect-tos`	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.

7. Configure the VLAN settings by configuring the following parameter(s) as required:

Parameter	Description
`pvid { pvid }`	**Synopsis:** An integer between 1 and 4094 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.
`type { type }`	**Synopsis:** [edge | trunk | pvlanedge] **Default:** edge How the port determines its membership in VLANs. There are a few types of ports: • EDGE : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter). • PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN. • 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.
`format { format }`	**Synopsis:** [untagged | tagged] **Default:** untagged Whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.
`gvrp-mode { gvrp-mode }`	**Synopsis:** [advertise_only | learn_advertise] GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED : the port is not capable of any GVRP processing. • ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

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***.

8. 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 385).
9. Configure the port security settings. For more information, refer to "Configuring Port Security" (Page 177).

10. Configure the spanning tree settings. For more information, refer to "Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces" (Page 836).
11. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » switch » { slot } » { port }***, where { slot } is the module and { port } is the Ethernet port.
3. Configure the RMON threshold alerts settings by configuring 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 { enabled }`	**Synopsis:** [true | false] **Default:** false 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
`direction { direc tion }`	**Synopsis:** [ingress | egress | both] **Default:** both The direction of traffic to be monitored. Possible values include: • Ingress - Monitors only the received bytes. • Egress - Monitors only the transmitted bytes. • Both - Monitors both the received and transmitted bytes.
`monitoring-type { mon itoring-type }`	**Synopsis:** [absolute | delta | percentage] **Default:** absolute The type of monitoring to perform on the threshold value. Possible values include: • Absolute - The current absolute value of the monitored value is compared with the threshold value. • Delta - The difference between the current value and the last recorded value (previous interval) of the monitored variable is compared with the threshold value. • Percentage - The percentage of the total port bandwidth being utilized.
`threshold-value { threshold-value }`	**Synopsis:** An integer between 1 and 18446744073709551615 **Default:** 1000 The value of data throughput (in bytes per interval period) to be compared.
`threshold-percentage { threshold-percent age }`	**Synopsis:** An integer between 1 and 100 **Default:** 80 The percentage of total data throughput to check for bandwidth threshold.
`interval { interval }`	**Synopsis:** An integer between 10 and 65535 **Default:** 60 The number of seconds over which the data is sampled and compared with the threshold

4. Type `commit` and press **Enter** to save the changes.

8.2.4 Viewing Switched Ethernet Port Statistics

To view statistics collected for a specific switched Ethernet port, type:

```
show interfaces switch { slot } { port } port-stats
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

A table or list similar to the following example appears:

```
ruggedcom# show interfaces switch lm1 1 port-stats
port-stats
 in octets  6820
 out octets 3086
 in pkts    33
 out pkts   18
 error pkts 0
```

The following information is provided:

Parameter	Description
`in-octets`	**Synopsis:** An integer The number of octets in received good packets. (Unicast+Multicast +Broadcast) and dropped packets.
`out-octets`	**Synopsis:** An integer The number of octets in transmitted good packets.
`in-pkts`	**Synopsis:** An integer The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.
`out-pkts`	**Synopsis:** An integer The number of transmitted good packets.
`error-pkts`	**Synopsis:** 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, type:

```
show interfaces switch { slot } { port }
```

Where:

- `{ slot }` is the name of the module location (e.g. lm1)
- `{ port }` is the port number for the switched Ethernet port

A table or list similar to the following example appears:

```
interfaces switch lm1 1
 name   ge-1-1
 state  up
 media  1000T
 speed  100M
 duplex full
 mtu    1500
 mac    00:0a:dc:f6:c6:21
 .
 .
 .
```

The following information is provided:

Parameter	Description
`name`	**Synopsis:** A string between 1 and 10 characters long A descriptive name that may be used to identify the device connected on that port.
`state`	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] The port's link status.
`media`	**Synopsis:** 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`	**Synopsis:** [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`	**Synopsis:** [auto | half | full] Duplex Setting: { Auto, Half, Full }
`mtu`	**Synopsis:** An integer The Maximum Transmission Unit of frame (in bytes) permitted on the interface.
`mac`	**Synopsis:** 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, type:

```
show interfaces switch { slot } { port } rmon-stats
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

A table or list similar to the following example appears:

```
ruggedcom# show interfaces switch lm1 1 rmon-stats | tab
rmon-stats
 in octets              10107903
 in pkts                53903
 in bcast pkts          607
 in mcast pkts          42103
 total in octets        10107903
 total in pkts          53903
 out octets             4974162
 out pkts               14356
 drop events            0
 out bcast pkts         0
 out mcast pkts         405
 crc align errors       0
 undersize pkts         0
 oversize pkts          0
 fragments              0
 jabbers                0
 collisions             0
 late collisions        0
 pkts 64 octets         10978
 pkts 65to127 octets    24792
 pkts 128to255 octets   19970
 pkts 256to511 octets   2469
 pkts 512to1023 octets  8410
 pkts 1024to1518 octets 1640
```

The following information is provided:

Parameter	Description
`in-octets`	**Synopsis:** An integer The number of octets in received good packets (Unicast+Multicast +Broadcast) and dropped packets.
`in-pkts`	**Synopsis:** An integer The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.
`in-bcast-pkts`	**Synopsis:** An integer The number of good broadcast packets received.
`in-mcast-pkts`	**Synopsis:** An integer The number of good multicast packets received.

Parameter	Description
`total-in-octets`	**Synopsis:** 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.
`total-in-pkts`	**Synopsis:** 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.
`out-octets`	**Synopsis:** An integer The number of octets in transmitted good packets.
`out-pkts`	**Synopsis:** An integer The number of transmitted good packets.
`drop-events`	**Synopsis:** An integer The number of received packets that are dropped due to lack of receive buffers.
`out-bcast-pkts`	**Synopsis:** An integer The number of transmitted broadcast packets.
`out-mcast-pkts`	**Synopsis:** An integer The number of transmitted multicast packets. This does not include broadcast packets.
`crc-align-errors`	**Synopsis:** 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.
`undersize-pkts`	**Synopsis:** 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.
`oversize-pkts`	**Synopsis:** An integer The number of packets received with data length greater than 1536 octets and valid CRC.
`fragments`	**Synopsis:** 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

Parameter	Description
	Collision Event has not been detected. 3. A Late Collision Event has not been detected. 4. The packet has invalid CRC.
jabbers	**Synopsis:** An integer The number of packets which meet all the following conditions: 1. The packet data length is greater that 1536 octets. 2. The packet has invalid CRC.
collisions	**Synopsis:** An integer The number of received packets for which a Collision Event has been detected.
late-collisions	**Synopsis:** An integer The number of received packets for which a Late Collision Event has been detected.
pkts-64-octets	**Synopsis:** 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.
pkts-65to127-octets	**Synopsis:** 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
pkts-128to255-octets	**Synopsis:** An integer The number of received and transmitted packets with a size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets
pkts-256to511-octets	**Synopsis:** 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.
pkts-512to1023-octets	**Synopsis:** 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
pkts-1024to1518-octets	**Synopsis:** 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, type:

```
switch clear-all-switch-stats
```

Clearing Statistics for a Specific Switched Ethernet Port

To clear the statistics collected for a specific switched Ethernet port, type:

```
interfaces switch { slot } { port } clear-port-stats
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

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, type:

```
switch reset-all-switch-ports
```

Resetting a Specific Switched Ethernet Port

To reset a specific switched Ethernet port, type:

```
interfaces switch { slot } { port } reset-port
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

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, type:

⚠ NOTICE

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.

```
interfaces switch { slot } { port } diagnostics start-ca
ble-test run { runs } calibration { calibration }
```

Where:

- `{ slot }` is the name of the module location.
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.
- `{ runs }` is the total number of times cable diagnostics should be performed on the selected port. When set to 0, cable diagnostics will be performed continuously on the selected port.
- `{ calibration }` is the value used to adjust or calibrate the estimated distance to fault. To calibrate the determine estimated distance to fault, do the following:
  1. Connect an Ethernet cable with a known length (e.g. 50m) to the port that requires calibration. Do not connect the other end of the cable to any link partner.
  2. Run a cable diagnostic test a few times on the port. An OPEN fault should be detected.
  3. Find the average distance to the OPEN fault recorded in the log and compare it to the known length of the cable. The difference can be used as the calibration value.
  4. Enter the calibration value and run the cable diagnostic test a few more times. The distance to the OPEN fault should now be similar to the cable length. Use the distance value to determine the calibration value.

For information about how to view the test results, refer to "Viewing Cable Diagnostic Statistics" (Page 349).

8.2.9.2 Viewing Cable Diagnostic Statistics

To view the statistics collected for a switched Ethernet port after a cable diagnostic test, type:

```
show interfaces switch { slot } { port } diagnostics ca
ble-diagnostic-results
```

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

A list similar to the following example appears:

```
ruggedcom# show interfaces switch lm1 1 diagnostics cable-diagnostic-results
diagnostics cable-diagnostic-results
 running         false
 good            20
 open            0
 short           20
 imped           0
 pass fail total "   10/    0/   10  "
 run count       0
 pass count      0
 fail count      0
```

The following information is provided:

Parameter	Description
`running`	**Synopsis:** [true | false] Whether or not a cable test is currently running on this port
`good`	**Synopsis:** An integer The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
`open`	**Synopsis:** An integer The number of times OPEN is detected on the cable pairs of the selected port.
`short`	**Synopsis:** An integer The number of times SHORT is detected on the cable pairs of the selected port.
`imped`	**Synopsis:** An integer The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
`pass-fail-total`	**Synopsis:** A string between 1 and 19 characters long This field summarizes the results of the cable diagnostics performed so far. • Pass : the number of times cable diagnostics were successfully completed on the selected port.

Parameter	Description
	• Fail : the number of times cable diagnostics failed to complete on the selected port. • Total : the total number of times cable diagnostics have been attempted on the selected port.
`run-count`	**Synopsis:** An integer Run Count : The total number of iterations
`pass-count`	**Synopsis:** An integer Pass Count
`fail-count`	**Synopsis:** 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, type:

```
switch clear-cable-stats-all
```

Clearing Cable Diagnostic Statistics for a Specific Switchport

To clear only the statistics for a specific switchport, type:

```
interfaces switch { slot } { port } diagnostics clear-ca
ble-stats-port
interfaces switch swport { port } diagnostics clear-ca
ble-stats-port
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

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, type:

```
show running-config interface trunk
```

If trunks have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface trunks
interface
 trunks 1
  switchport
  no alias
  no mcast-filtering gmrp
  no cos inspect-tos
  vlan pvid 1
  no vlan gvrp-mode
  trunk-ports lm6 1
  !
  trunk-ports lm6 2
  !
  no spanning-tree restricted-role
  no spanning-tree restricted-tcn
 !
!
```

If no Ethernet trunk interfaces have been configured, add trunks as needed. For more information, refer to "Adding an Ethernet Trunk Interface" (Page 351).

8.3.2 Adding an Ethernet Trunk Interface

To add an Ethernet trunk interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the interface by typing:

   ```
   interface trunks { id }
   ```

   Where:

   - `{ id }` is the ID given to the trunk
3. Configure the interface by typing the following commands:

Parameter	Description
`switchport { switch port }`	**Synopsis:** [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-src { ip-address-src }`	**Synopsis:** [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

Parameter	Description
	and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
`ipv6-address-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** 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.
`proxyarp`	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface). **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1500 bytes (jumbo frames) up to 9216 bytes on Gigabit Ethernet ports only. Ports at each end of the trunk must be Gigabit Ethernet ports. Jumbo frames are not supported if either port is a Fast Ethernet port.
`alias { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface

4. Configure the multicast filtering settings by typing the following commands:

Parameter	Description
`gmrp { gmrp }`	**Synopsis:** [advertise_only | learn_advertise] GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: • DISABLED : the port is not capable of any GMRP processing. • ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

5. Configure the CoS settings by typing the following commands:

Parameter	Description
`default-priority { default-priority }`	**Synopsis:** An integer between 0 and 7 **Default:** 0 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).
`inspect-tos`	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.

6. Configure the VLAN settings by typing the following commands:

Parameter	Description
`pvid { pvid }`	**Synopsis:** An integer between 1 and 4094 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.
`type { type }`	**Synopsis:** [edge | trunk | pvlanedge] **Default:** edge How the port determines its membership in VLANs. There are the following port types: • EDGE : the port is only a member of one VLAN (its native VLAN specified by the'PVID' parameter). • PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN. • 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 VLANconfiguration.
`format { format }`	**Synopsis:** [untagged | tagged] **Default:** untagged Whether frames transmitted out of the port on its native VLAN(specified by the 'PVID' parameter) will be tagged or untagged.
`gvrp-mode { gvrp-mode }`	**Synopsis:** [advertise_only | learn_advertise] GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED : the port is not capable of any GVRP processing. • ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.

Parameter	Description
	• ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

7. Type `commit` and press **Enter** to save the changes.

8.3.3 Deleting an Ethernet Trunk Interface

To delete an Ethernet trunk interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the interface by typing:

   ```
   no interface trunks { id }
   ```

   Where:

   - `{ id }` is the ID given to the trunk
3. Type `commit` and press **Enter** to save the changes.

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 interfaces, type:

```
show running-config interface trunks { id } trunk-ports
```

Where:

- `{ id }` is the ID given to the interface

If trunk ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface trunks 1 trunk-ports
interface
 trunks 1
  trunk-ports lm1 1
  !
  trunk-ports lm1 2
  !
 !
!
```

If no Ethernet trunk ports have been configured, add ports as needed. For more information, refer to "Adding an Ethernet Trunk Port" (Page 355).

8.3.4.2 Adding an Ethernet Trunk Port

To add an Ethernet trunk port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the port by typing:

   ```
   interface trunks { id } trunk-ports { slot } { port }
   ```

   Where:

   - `{ id }` is the ID given to the trunk
   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

8.3.4.3 Deleting an Ethernet Trunk Port

To delete an Ethernet trunk port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the port by typing:

   ```
   no interface trunks { id } trunk-ports { slot } { port }
   ```

   Where:

   - `{ id }` is the ID given to the trunk
   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

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 MAC addresses, type:

```
show switch mac-tables mac-table
```

A table or list similar to the following example appears:

```
ruggedcom# show switch mac-tables mac-table
MAC               VID   SLOT  PORT  TYPE     COS
-----------------------------------------------------
00:0a:dc:78:f3:20  1     lm1   1     dynamic  normal
00:0a:dc:78:fc:45  1     lm1   1     dynamic  normal
00:0a:dc:f6:8b:ff  4085  lm1   2     static   normal
00:10:94:00:24:01  4084  lm1   1     static   normal
00:10:94:00:30:01  1     lm1   2     static   normal
00:10:94:00:40:01  4086  lm1   2     static   normal
00:13:3b:00:04:1a  1     lm1   1     dynamic  normal
00:13:3b:00:06:b5  1     lm1   1     dynamic  normal
```

The following information is provided:

Parameter	Description
`slot`	**Synopsis:** [sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport] The slot containing the module including the port.
`port`	**Synopsis:** An integer between 1 and 16 The port on which the MAC address has been learned.
`type`	**Synopsis:** [static | dynamic] How the MAC address has been learned by the switch: • STATIC: 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. • DYNAMIC: The address has been automatically learned by the switch and can be automatically unlearned.
`cos`	**Synopsis:** [N/A | normal | medium | high | crit] The Class Of Service (CoS) that is assigned to frames carrying this address as a source or destination address.

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 357).
- Configure the address on the device as a static MAC address. For more information, refer to "Adding a Static MAC Address" (Page 358).

8.4.2 Purging the Dynamic MAC Address List

To purge the dynamic MAC address list of all entries, type:

```
switch mac-tables purge-mac-table
```

Once the table is purged, the following message appears:

```
purge-mac-table-string Success
```

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. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » mac-tables*** and configure the following parameter(s) as required:

Parameter	Description
`mac-aging-time { mac-aging-time }`	**Synopsis:** An integer between 15 and 800 **Default:** 300 The time a learned MAC address is held before being aged out.
`mac-age-on-loss { mac-age-on-loss }`	**Synopsis:** [true | false] **Default:** true 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.

3. Type `commit` and press **Enter** to save 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, type:

```
show running-config switch mac-tables static-mac-table
```

If static MAC addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mac-tables static-mac-table | tab
MAC               VID   LEARNED  SLOT  PORT  COS
-----------------------------------------------------
00:0a:dc:f6:8b:ff  4085  -        lm1   2     normal
00:10:94:00:24:01  4084  -        lm1   1     normal
00:10:94:00:30:01  1     -        lm1   2     normal
00:10:94:00:40:01  4086  -        lm1   2     normal

!
```

If no static MAC addresses have been configured, add addreses as needed. For more information, refer to "Adding a Static MAC Address" (Page 358).

8.4.4.2 Adding a Static MAC Address

To add a static MAC address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static MAC address by typing:

   Note

   Letters in MAC addresses must be lowercase.

   ```
   switch mac-tables static-mac-table static-mac { address }
   { vlan }
   ```

   Where:

   - `{ address }` is the Unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
   - `{ vlan }` is the ID of the VLAN upon which the MAC address operates.
3. 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.

Parameter	Description
`slot { slot }`	**Synopsis:** [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 { port }`	**Synopsis:** An integer between 1 and 16 The selected ports on the module installed in the indicated slot.
`cos { cos }`	**Synopsis:** [N/A | normal | medium | high | crit] **Default:** normal The priority of traffic for a specified address.

4. Type `commit` and press **Enter** to save the changes.

8.4.4.3 Deleting a Static MAC Address

To delete a static MAC address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the static MAC address by the typing:

   ```
   no switch mac-tables static-mac-table static-mac { ad
   dress } { vlan }
   ```

   Where:

   - `{ address }` is the Unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
   - `{ vlan }` is the ID of the VLAN upon which the MAC address operates.
3. Type `commit` and press **Enter** to save the changes.

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

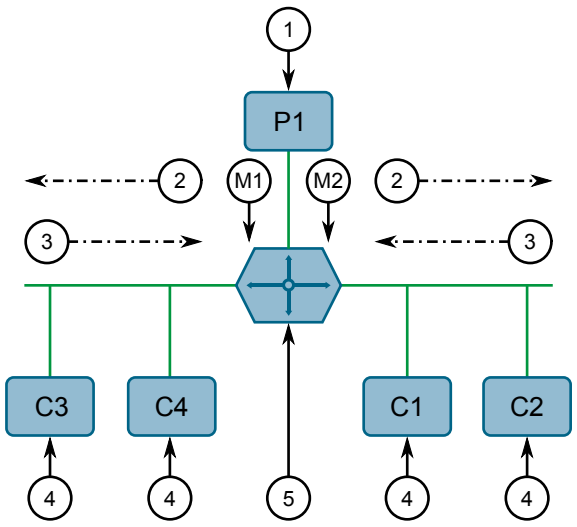
IGMP is used by IP hosts to report their host group memberships with multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host.

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 Mulicast 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.

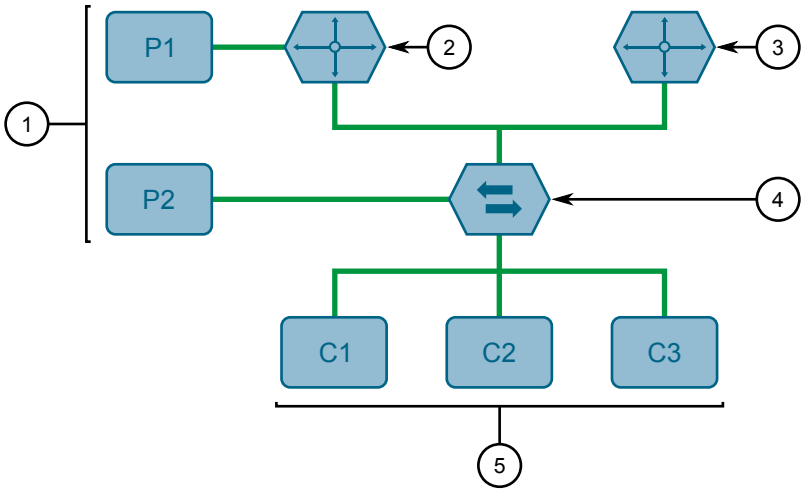
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- 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:

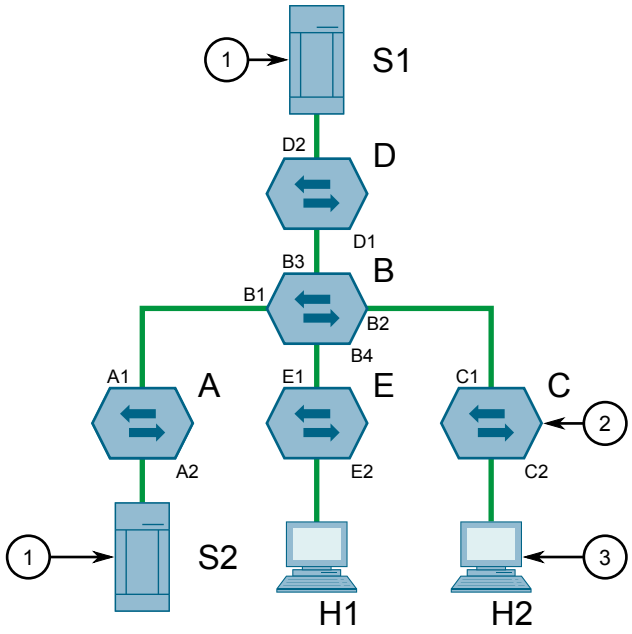
- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled on the RUGGEDCOM RX1500, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the RUGGEDCOM RX1500, 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » mcast-filtering*** and configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false GMRP Enable
`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 { leave-timer }`	**Synopsis:** An integer between 600 and 300000 **Default:** 4000 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.

3. Enable GMRP on one or more switched Ethernet ports. For more information, refer to "Configuring a Switched Ethernet Port" (Page 335).
4. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » mcast-filtering » igmp-snooping*** and configure the following parameter(s) as required:

Parameter	Description
`igmp-mode { igmp-mode }`	**Synopsis:** [active | passive] **Default:** passive Specifies the IGMP mode: • PASSIVE : The switch passively snoops IGMP traffic and never sends IGMP queries. • ACTIVE : The switch generates IGMP queries, if no queries from a better candidate for the querier are detected for a while.
`igmp-query-interval { igmp-query-interval }`	**Synopsis:** An integer between 10 and 3600 **Default:** 60 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.
`igmp-version { igmp-version }`	**Synopsis:** [v2 | v3] **Default:** v2 The version of IGMP. Options include: • v2: IGMP version 2. • v3: IGMP version 3. Backwards compatible with v2.
`router-forwarding { router-forwarding }`	**Synopsis:** [true | false] **Default:** true Whether or not multicast streams will always be forwarded to multicast routers.
`rstp-flooding`	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.

3. Assign one or more ports for IGMP to use when sending Membership Reports. For more information, refer to "Adding a Router Port" (Page 369).
4. Enable IGMP snooping for the required static VLAN(s). For more information, refer to "Adding a Static VLAN" (Page 386).
5. Type `commit` and press **Enter** to save the changes.

8.5.3.2 Viewing a List of Router Ports

To view a list of router ports used for IGMP snooping, type:

```
show running-config switch mcast-filtering igmp-snooping
router-ports
```

If router ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mcast-filtering igmp-snooping router-ports |
 tab
SLOT  PORT
------------
lm1   1

 !
!
```

If no router ports have been configured, add ports as needed. For more information, refer to "Adding a Router Port" (Page 369).

8.5.3.3 Adding a Router Port

To add a router port for IGMP snooping, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the router port by typing:

   ```
   switch mcast-filtering igmp-snooping router-ports { slot }
   { port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

8.5.3.4 Deleting a Router Port

To delete a router port for IGMP snooping, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the router port by typing:

   ```
   no switch mcast-filtering igmp-snooping router-ports
   { slot } { port }
   ```

   Where:

   - `{ slot }` is the name of the module location

- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config switch mcast-filtering static-mcast-table
```

If entries have been established, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mcast-filtering static-mcast-table
switch mcast-filtering
 static-mcast-table 10 01:00:00:01:01:01
 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Static Multicast Group Entry" (Page 370).

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. Make sure the CLI is in Configuration mode.
2. Add the table entry by typing:

Note

Letters in MAC addresses must be lowercase.

```
switch mcast-filtering static-mcast-table { id } { ad
dress }
```

Where:

- `{ id }` is the ID for the VLAN upon which the static multicast group operates
- `{ address }` is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx

3. Add one or more egress ports. For more information, refer to "Adding an Egress Port" (Page 372).
4. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Delete the table entry by typing:

   ```
   no switch mcast-filtering static-mcast-table { id } { ad
   dress }
   ```

   Where:

   - `{ id }` is the ID for the VLAN upon which the static multicast group operates
   - `{ address }` is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show switch mcast-filtering static-mcast-table { id } { ad
dress } egress-ports
```

Where:

- `{ id }` is the ID for the VLAN upon which the static multicast group operates
- `{ address }` is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx

If egress ports have been established, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mcast-filtering static-mcast-table 10
 01:00:00:01:01:01 egress-ports
switch mcast-filtering
 static-mcast-table 10 01:00:00:01:01:01
```

```
   egress-ports lm2 1
   !
  !
 !
```

If no egress ports have been configured, add egress ports as needed. For more information, refer to "Adding an Egress Port" (Page 372).

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. Make sure the CLI is in Configuration mode.
2. Add the egress port by typing:

   ```
   switch mcast-filtering static-mcast-table { id } { ad
   dress } egress-ports { slot } { port }
   ```

   Where:

   - `{ id }` is the ID for the VLAN upon which the static multicast group operates
   - `{ address }` is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

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. Make sure the CLI is in Configuration mode.
2. Delete the table entry by typing:

   ```
   no switch mcast-filtering static-mcast-table { id } { ad
   dress } egress-ports { slot } { port }
   ```

   Where:

   - `{ id }` is the ID for the VLAN upon which the static multicast group operates
   - `{ address }` is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
   - `{ slot }` is the name of the module location

- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

8.5.6 Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, type:

```
show switch mcast-filtering mcast-group-summary
```

If multicast groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show switch mcast-filtering mcast-group-summary
                        STATIC  STATIC  GMRP  GMRP
VID  MAC                SLOT    PORTS   SLOT  PORTS
-------------------------------------------------------
10   01:00:00:01:01:01
                        lm1     4
```

The following information is provided:

Parameter	Description
`vid`	**Synopsis:** An integer The VLAN Identifier of the VLAN upon which the multicast group operates.
`mac`	**Synopsis:** A string up to 17 characters long The multicast group MAC address.
`{ slot }`	**Synopsis:** [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.
`ports`	**Synopsis:** A string up to 128 characters long The selected ports on the module installed in the indicated slot.
`{ slot }`	**Synopsis:** [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.
`ports`	**Synopsis:** A string up to 128 characters long The selected ports on the module installed in the indicated slot.

8.5.7 Viewing a List of IP Multicast Groups

To view a list of all multicast groups, type:

```
show switch mcast-filtering ip-mcast-groups
```

If IP multicast groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show switch mcast-filtering ip-mcast-groups
     IP                              JOINED  JOINED  ROUTER  ROUTER
VID  ADDRESS    MAC                  SLOT    PORTS   SLOT    PORTS
-------------------------------------------------------------------
100  225.0.1.1  01:00:5e:00:01:01
                                     lm1     3
                                             lm1     1
200  225.0.1.2  01:00:5e:00:01:02
                                     lm1     4
                                             lm1     2
```

The following information is provided:

Parameter	Description
`{ vid }`	**Synopsis:** An integer The VLAN Identifier of the VLAN upon which the multicast group operates.
`{ ip-address }`	**Synopsis:** A string The multicast group IP address.
`mac`	**Synopsis:** A string up to 17 characters long The multicast MAC address corresponding to the group multicast IP address.
`Joined Slot`	The name of the module location provided on the silkscreen across the top of the device.
`Joined Ports`	**Synopsis:** An integer between 1 and 16 The selected ports on the module installed in the indicated slot.
`Router Slot`	The name of the module location provided on the silkscreen across the top of the device.
`Router Ports`	**Synopsis:** 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 385).
- **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 377)

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 376).

Port Type	VLANs Supported	PVID Format	Usage
Edge	1 (Native) Configured	Untagged	*VLAN Unaware Networks*: All frames are sent and received without the need for VLAN tags.
		Tagged	*VLAN Aware Networks*: VLAN traffic domains are enforced on a single VLAN.
Trunk	All Configured	Tagged or Untagged	*switch-to-Switch Connections*: VLANs must be manually created and administered, or can be dynamically learned through GVRP. *Multiple-VLAN End Devices*: Implement connections to end devices that support multiple VLANs at the same time.

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 383).

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 387).

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. VIDs 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 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)

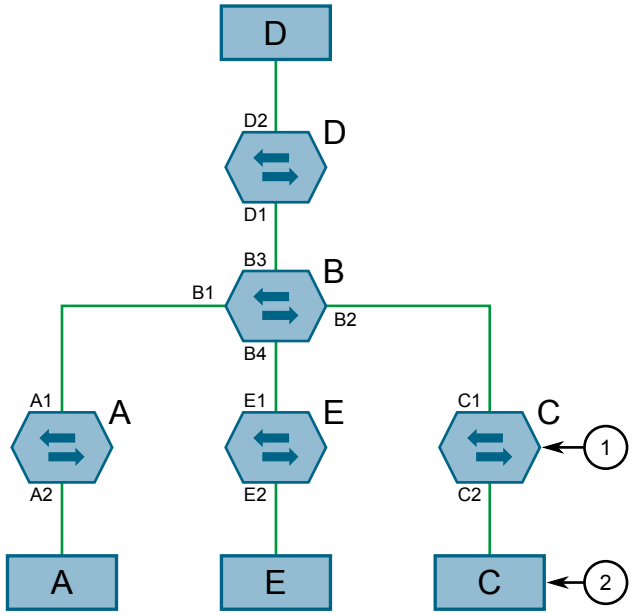
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere 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 D
- 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 177).

8.6.1.10 VLAN Advantages

The following are a few of the advantages offered by VLANs.

Traffic Domain Isolation

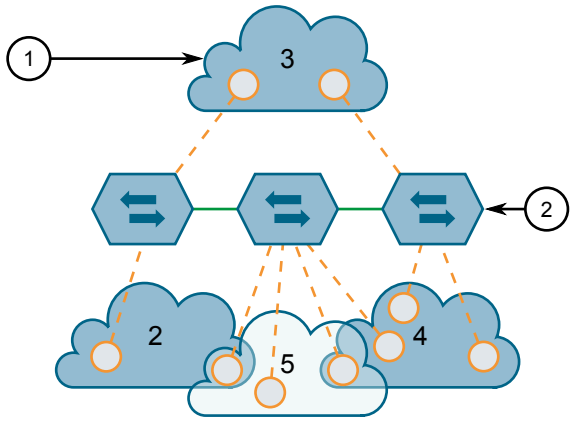
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

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

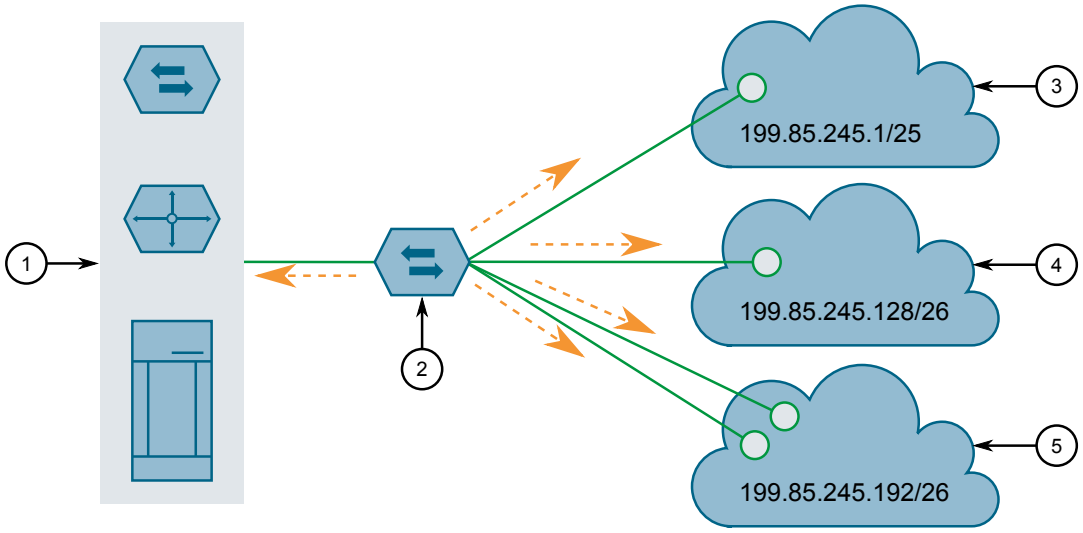
VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

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 `range-end` value repositions the matching serial VLAN. However, the matching serial VLAN is not affected when the `range-start` 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » switch-config*** and configure the following parameter(s) as required:

   Note

   Internal VLAN ranges are enabled by default whenever a serial module is detected, and are disabled otherwise.

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false Enables/disables the Internal VLAN Range settings.
`range-start { range-start }`	**Synopsis:** An integer between 2 and 4094 **Default:** 4094 Defines the lower end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.
`range-end { range-end }`	**Synopsis:** An integer between 2 and 4094 **Default:** 4094 Defines the higher end of a range of VLANs used for the device only.VLAN ID 1 is not permitted.

3. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.

2. Enable or disable ingress filtering by typing:

   Enabling Ingress Filtering

   ```
   switch vlans ingress-filtering enabled
   ```

   Disabling Ingress Filtering

   ```
   noswitch vlans ingress-filtering enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show switch vlans vlan-summary
```

A table similar to the following example appears:

```
ruggedcom# show switch vlans vlan-summary
     IGMP            UNTAGD  UNTAGD  TAGGED  TAGGED
VID  SNOOPING  MSTI  SLOT    PORTS   SLOT    PORTS   QOS  INGRESS  MARK
-------------------------------------------------------------------------
1    false     0
                    sm      none
                    lm1     1,2
                    lm2     none
                    lm3     none
                    lm4     none
                    lm5     none
                    lm6     none
                                    sm      none
                                    lm1     none
                                    lm2     none
                                    lm3     none
                                    lm4     none
                                    lm5     none
                                    lm6     none
                                                    0    0
                                                    1    0
                                                    2    0
                                                    3    0
                                                    4    0
.
.
.
```

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 335).

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. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » vlans » all-vlans » { id }***, where { id } is the ID of the VLAN and configure the following parameter(s) as needed:

Parameter	Description
`ip-address-src { ip-address-src }`	**Synopsis:** [static | dynamic] 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.
`ipv6-address-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** static Whether the IPv6 address is static or dynamically assigned via Dynamic Host Configuration Protocol (DHCP). This must be static for non-management interfaces.
`proxyarp`	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself.
`on-demand`	Brings up this interface on demand only.
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface). **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1500 bytes (jumbo frames) up to 9216 bytes when the VLAN is only associated with Gigabit Ethernet ports.

3. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to "Adding a QoS Map" (Page 919).
4. Type `commit` and press **Enter** to save 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, type:

```
show running-config switch vlans static-vlan
```

If static VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch vlans static-vlan | tab
     IGMP
VID  SNOOPING  MSTI  SLOT  PORT
---------------------------------
1    -         cst

!
```

If no static VLANs have been configured, add static VLANs as needed. For more information, refer to "Adding a Static VLAN" (Page 386).

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. Make sure the CLI is in Configuration mode.
2. Add the static VLAN by typing:

   ```
   switch vlans static-vlan { id }
   ```

   Where:

   - { id } is the VLAN identifier. The VLAN identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.
3. Configure the following parameter(s) as required:

Parameter	Description
`igmp-snooping`	Enables or disables IGMP Snooping on the VLAN.
`msti { msti }`	**Synopsis:** [cst] or An integer between 1 and 16 **Default:** cst 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.

4. If needed, configure a forbidden ports list. For more information, refer to "Adding a Forbidden Port" (Page 387).
5. Configure the VLAN for the port. For more information, refer to "Configuring VLANs for Switched Ethernet Ports" (Page 385).
6. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Delete the static VLAN by typing:

   ```
   no switch vlans static-vlan { id }
   ```

   Where:

   - `{ id }` is the ID of the VLAN
3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config switch vlans static-vlan forbidden-ports
```

If ports have been forbidden, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch vlans static-vlan forbidden-ports | tab
VID  SLOT  PORT
-----------------
50
     lm1   1
     lm1   2
60
     lm1   2
     lm1   3
     lm1   4
70
     lm1   5

!
```

If no ports have been forbidden, add forbidden ports as needed. For more information, refer to "Adding a Forbidden Port" (Page 387).

8.6.6.2 Adding a Forbidden Port

To add a forbidden port, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the forbidden port by typing:

   ```
   switch vlans static-vlan { name } forbidden-ports { slot }
   { port }
   ```

   Where:

   - `{ name }` is the name of the static VLAN
   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type `commit` and press **Enter** to save the changes.

8.6.6.3 Deleting a Forbidden Port

To delete a forbidden port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » vlans » static-vlan » { name } » forbidden-ports***, where { name } is the name of the static VLAN.
3. Configure the following parameter(s) as required:

   ```
   no switch vlans static-vlan { name } forbidden-ports
   { slot } { port }
   ```

   Where:

   - `{ name }` is the name of the static VLAN
   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

4. Type `commit` and press **Enter** to save 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 HDLC-ETH Connections" (Page 453)
- "Managing VLANs for Virtual Switches" (Page 498)
- "Managing VLANs for L2TPv3 Tunnels" (Page 518)
- "Managing VLANs for Routable Ethernet Ports" (Page 135)

9 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 581).

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 SM, the maximum number of Layer 3 switching rules is 1000.

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 235)

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 733)
- For static IPv4 routes, refer to "Adding an IPv4 Static Route" (Page 744)
- For static multicast groups, refer to "Adding a Static Multicast Group" (Page 751)

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 397).	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. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » layer3-switching***and configure the following parameter(s) as required:

Parameter	Description
`unicast-mode { unicast-mode }`	**Synopsis:** [disabled | auto | static] **Default:** auto • 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. • 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. • Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.
`multicast-mode { multicast-mode }`	**Synopsis:** [disabled | auto | static] **Default:** auto • 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. • 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. • Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.

`learn-mode { learn-mode }`	**Synopsis:** [flow-oriented | host-oriented]
	Default: flow-oriented
	Defines how dynamically learned traffic flows are identified:
	• Flow-oriented: Traffic flows are identified by a 5-tuple signature:
	`Src IP address`
	`Dst IP address`
	`Protocol`
	`Src TCP/UDP port`
	`Dst TCP/UDP port`
	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.

Parameter	Description

	• Host-oriented: Traffic flows are identified by a 2-tuple signature:
	`Src IP address`
	`Dst IP address`
	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.

`aging-time { aging-time }`	**Synopsis:** An integer between 16 and 600 **Default:** 32 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.

3. Type `commit` and press **Enter** to save 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. Make sure the CLI is in Configuration mode.
2. Enable or disable IPSec hardware acceleration by typing the following commands:

   Enable

   ```
   switch layer3-switching protocol-types ipsec
   ```

   Disable

   ```
   no switch layer3-switching protocol-types ipsec
   ```

3. Type `commit` and press **Enter** to save 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, type:

```
show switch layer3-switching arp-table
```

```
ruggedcom# show switch layer3-switching arp-table | tab
IP ADDRESS   MAC               VID
-----------------------------------------------------
192.11.0.2   00:11:94:11:00:01  4084
192.11.0.3   00:11:94:11:00:02  4084
192.11.0.4   00:11:94:11:00:03  4084
192.11.0.5   00:11:94:11:00:04  4084
192.11.0.6   00:11:94:11:00:05  4084
```

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 396).

9.4.2 Adding a Static ARP Table Entry

To add a static ARP table entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the table entry by typing:

   ```
   switch layer3-switching arp-table { address } mac { mac-address } vid { vlan-id }
   ```

   Where:

   - { address } is the IP address of the network device the entry describes
   - { mac-address } is the the MAC address of the network device specified by the IP address
   - { vlan-id } is the VLAN Identifier of the VLAN upon which the MAC address operates
3. Type `commit` and press **Enter** to save the changes.

9.4.3 Deleting a Static ARP Table Entry

To delete a static ARP table entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the key by typing:

   ```
   no switch layer3-switching arp-table { address }
   ```

   Where:

   - `{ address }` is the IP address for the network device the entry describes
3. Type `commit` and press **Enter** to save the changes.

9.5 Viewing a Static and Dynamic ARP Table Summary

To view a static and dynamic ARP table summary, type:

```
show switch layer3-switching arp-table-summary
```

If ARP table entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show switch layer3-switching arp-table-summary
IP ADDRESS   MAC               VID   STATIC  STATUS
-------------------------------------------------------
192.11.0.2   00:11:94:11:00:01  4084  false   resolved
192.11.0.3   00:11:94:11:00:02  4084  false   resolved
192.11.0.4   00:11:94:11:00:03  4084  false   resolved
192.11.0.5   00:11:94:11:00:04  4084  false   resolved
192.11.0.6   00:11:94:11:00:05  4084  false   resolved
```

The table or list provides the following information:

Parameter	Description
`{ ip-address }`	**Synopsis:** A string The IP address of the network device the entry describes.
`mac`	**Synopsis:** A string up to 17 characters long **Default:** 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
`vid`	**Synopsis:** An integer The VLAN Identifier of the VLAN upon which the MAC address operates.
`static`	**Synopsis:** [true | false] **Default:** 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`	**Synopsis:** [resolved | unresolved] **Default:** unresolved The Address Resolution Protocol (ARP) entry resolution status: • Resolved: MAC-IP address pair is resolved and operational. • Unresolved: the device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically.

9.6 Viewing Routing Rules

To view a list of routing rules, type:

```
show switch layer3-switching routing-rules-summary
```

A table or list similar to the following example appears:

```
ruggedcom# show switch layer3-switching routing-rules-summary
  PACKETS
RULE  RULE     IN    OUT                       SRC                DEST               PER
    ROUTING
ID    TYPE     VLAN  VLAN  PROTO  SOURCE       PORT  DESTINATION  PORT  GATEWAY       SECOND
 STATIC  ACTION   STATUS
-------------------------------------------------------------------------------------------
0     unicast  -     -     17     192.12.1.120  1024  192.11.1.120  1024  192.11.1.120  11
 false   forward  active
1     unicast  -     -     17     192.12.1.69   1024  192.11.1.69   1024  192.11.1.69   11
 false   forward  active
2     unicast  -     -     17     192.11.0.160  1024  192.12.0.160  1024  192.12.0.160  11
 false   forward  active
3     unicast  -     -     17     192.11.0.92   1024  192.12.0.92   1024  192.12.0.92   11
 false   forward  active
4     unicast  -     -     17     192.12.0.92   1024  192.11.0.92   1024  192.11.0.92   11
 false   forward  active
5     unicast  -     -     17     192.12.0.254  1024  192.11.0.254  1024  192.11.0.254  11
 false   forward  active
6     unicast  -     -     17     192.12.0.223  1024  192.11.0.223  1024  192.11.0.223  11
 false   forward  active
7     unicast  -     -     17     192.11.0.85   1024  192.12.0.85   1024  192.12.0.85   11
 false   forward  active
8     unicast  -     -     17     192.12.0.95   1024  192.11.0.95   1024  192.11.0.95   11
 false   forward  active
9     unicast  -     -     17     192.12.0.180  1024  192.11.0.180  1024  192.11.0.180  12
 false   forward  active
10    unicast  -     -     17     192.12.0.67   1024  192.11.0.67   1024  192.11.0.67   11
 false   forward  active
11    unicast  -     -     17     192.12.0.161  1024  192.11.0.161  1024  192.11.0.161  11
 false   forward  active
12    unicast  -     -     17     192.11.2.190  1024  192.12.2.190  1024  192.12.2.190  11
 false   forward  active
```

The table or list provides the following information:

Parameter	Description
`{ rule-id }`	**Synopsis:** 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`	**Synopsis:** [multicast | unicast | invalid | hidden] Identifies the type of the rule: unicast,multicast,invalid.
`in-vlan`	**Synopsis:** An integer Identifies the ingress VLAN. To match the rule, the packet's ingress VLAN must match the number.
`out-vlans`	**Synopsis:** An integer Identifies the egress VLAN. The matched multicast packet is sent to the identified VLAN.
`proto`	**Synopsis:** An integer The IP Encapsulated Protocol number. Unless zero is specified, the incoming packet's IP protocol must match this number.

Parameter	Description
source	**Synopsis:** 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.
src-port	**Synopsis:** An integer between 0 and 65535 The port associated with the source flow. A value of 0 means Not Applicable.
destination	**Synopsis:** 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.
dest-port	**Synopsis:** An integer between 0 and 65535 The port associated with the destination flow. A value of 0 means Not Applicable.
gateway	**Synopsis:** A string Defines the nexthop IP address. The matched unicast packet is sent to the identified gateway.
packets-per-second	**Synopsis:** An integer Displays the statistical throughput of all packets matching the rule, in packets per second.
static	**Synopsis:** [true | false] Whether the rule is static or dynamic. Static rules are configured as a result of management activity. Dynamic rules are automatically learned by the device and can be unlearned subject to aging time.
routing-action	**Synopsis:** [forward | exclude] The action applied to packets matching the rule: • Forward: Perform a hardware acceleration. • Exclude: Exclude from hardware acceleration and always pass matching packets to the CPU for software routing.
status	**Synopsis:** [active | resolving | pending | excluding] Whether the rule is currently operational or not: • Active: The rule is fully operational and can be applied, so hardware acceleration is performed. • Resolving: The rule is not operational yet due to some unresolved information, like the Address Resolution Protocol (ARP) or gateway's MAC address in the MAC Address Table. Hardware acceleration is not performed. • Pending: there are not enough hardware resources to setup the rule and all its dependencies. Hardware acceleration is not performed.

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 389).

To flush dynamic hardware routing rules, type:

```
switch layer3-switching flush-dynamic-rules
```

10 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 the "RUGGEDCOM Modules Catalog" [https://support.industry.siemens.com/cs/us/en/view/109747072] series.

10.1 Managing Serial Ports

This section describes how to configure, monitor and manage serial ports on the device.

10.1.1 Viewing a List of Serial Ports

To view a list of serial ports configured on the device, type:

```
show running-config interface serial
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial | tab
                            BAUD  DATA          STOP  FLOW     PORT
SLOT  PORT  ENABLED  ALIAS  RATE  BITS  PARITY  BITS  CONTROL  TYPE   PROTOCOL
------------------------------------------------------------------------------
lm3   1     true     -      9600  8     none    1     none     rs232
lm3   2     true     -      9600  8     none    1     none     rs232
lm3   3     true     -      9600  8     none    1     none     rs232
lm3   4     true     -      9600  8     none    1     none     rs232
lm3   5     true     -      9600  8     none    1     none     rs232
lm3   6     true     -      9600  8     none    1     none     rs232

!
```

10.1.2 Viewing Serial Port Statistics

To view statistics collected for a specific serial port, type:

```
show interfaces serial port
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces serial port | tab
                                TX      TX        RX      RX        PACKET   PARITY   FRAMING   OVERRUN
IFNAME    MEDIA   SPEED   PROTOCOL  CHARS   PACKETS   CHARS   PACKETS   ERRORS   ERRORS   ERRORS    ERRORS
-------------------------------------------------------------------------------------------------------
ser-3-1   RS232   9.6K    none      0       0         0       0         0        0        0         0
ser-3-2   RS232   9.6K    none      0       0         0       0         0        0        0         0
ser-3-3   RS232   9.6K    none      0       0         0       0         0        0        0         0
ser-3-4   RS232   9.6K    none      0       0         0       0         0        0        0         0
ser-3-5   RS232   9.6K    none      0       0         0       0         0        0        0         0
ser-3-6   RS232   9.6K    none      0       0         0       0         0        0        0         0
```

The following information is provided:

Parameter	Description
`{ ifname }`	**Synopsis:** A string between 1 and 10 characters long The name of the serial interface.
`media`	**Synopsis:** A string up to 31 characters long The type of port media { RS232 RS422 RS485 }.
`speed`	**Synopsis:** [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).
`protocol`	**Synopsis:** A string up to 31 characters long The serial protocol assigned to this port.
`tx-chars`	**Synopsis:** An integer The number of bytes transmitted over the serial port.
`tx-packets`	**Synopsis:** An integer The number of packets transmitted over the serial port.
`rx-chars`	**Synopsis:** An integer The number of bytes received by the serial port.
`rx-packets`	**Synopsis:** An integer The number of packets received by the serial port.
`packet-errors`	**Synopsis:** An integer The number of packet errors on this serial port.
`parity-errors`	**Synopsis:** An integer The number of parity errors on this serial port.
`framing-errors`	**Synopsis:** An integer The number of framing errors on this serial port.

Parameter	Description
`overrun-errors`	**Synopsis:** An integer The number of overrun errors on this serial port.

10.1.3 Viewing Transport Connection Statistics

To view the statistics collected for all transport connections, type:

```
show interfaces serial transport-connections
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces serial transport-connections | tab
                     REMOTE  LOCAL             RX       TX       TARGET
INDEX  REMOTE IP     PORT    PORT   TRANSPORT  PACKETS  PACKETS  PORT      STATUS
-------------------------------------------------------------------------------
1      10.200.22.199 15836   20000  TCP        177      0        ser-3-1,  Active
```

To view the statistics collected for a specific transport connection, type:

```
show interfaces serial transport-connections { index }
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces serial transport-connections 1 | tab
                     REMOTE  LOCAL             RX       TX       TARGET
INDEX  REMOTE IP     PORT    PORT   TRANSPORT  PACKETS  PACKETS  PORT    STATUS
-------------------------------------------------------------------------------
1      192.168.12.2  55677   502    TCP        3691     3691     ser-2,  Active
```

These tables or lists provide the following information:

Parameter	Description
`{ index }`	**Synopsis:** A string up to 32 characters long The transport connection index.
`remote-ip`	**Synopsis:** A string up to 32 characters long The IP address of the remote serial server.
`remote-port`	**Synopsis:** An integer The port of the remote serial server.
`local-port`	**Synopsis:** An integer The local port for the incoming connection.
`transport`	**Synopsis:** A string up to 8 characters long The transport protocol (UDP or TCP) for this serial port.
`rx-packets`	**Synopsis:** An integer The number of packets received from TCP/UDP.

Parameter	Description
tx-packets	**Synopsis:** An integer The number of packets transmitted to TCP/UDP.
target-port	**Synopsis:** A string up to 1024 characters long The target serial port.
status	**Synopsis:** A string up to 31 characters long The connection status of the serial port.

10.1.4 Viewing DNP Device Table Statistics

To view the statistics collected for DNP device tables, type:

```
show interfaces serial dnp-device-table
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces serial dnp-device-table | tab
DEVICE                  SERIAL
ADDRESS  REMOTE IP      PORT
---------------------------------
10       -              ser-3-1
20       10.200.22.199  -
```

The following information is provided:

Parameter	Description
{ device-address }	**Synopsis:** A string up to 32 characters long The DNP device address.
remote-ip	**Synopsis:** 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	**Synopsis:** A string up to 128 characters long The target serial port.

10.1.5 Clearing Serial Port Statistics

To clear the statistics collected for a specific serial port, type:

```
interfaces serial port { name } clear-port-stats
```

Where:

- `{ name }` is the name assigned to the port

10.1.6 Configuring a Serial Port

To configure a serial port, do the following:

⚠ NOTICE

Do not enable flow control when Modbus TCP protocol is enabled.

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » { port }***, where { port } is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true 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.
`alias { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface.
`baud-rate { baud-rate }`	**Synopsis:** [1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 | 230400 | 76800] **Default:** 9600 The baud rate selection of the serial port.
`data-bits { data-bits }`	**Synopsis:** An integer between 7 and 8 **Default:** 8 The number of data bits.
`parity { parity }`	**Synopsis:** [none | even | odd] **Default:** none The parity of the serial port.
`stop-bits { stop-bits }`	**Synopsis:** An integer between 1 and 2 **Default:** 1 The number of stop bits of the serial port.
`flow-control { flow-control }`	**Synopsis:** [none | xonxoff] **Default:** none The flow control of the serial port.
`port-type { port-type }`	**Synopsis:** [rs232 | rs422 | rs485] **Default:** rs232 The type of serial port.

4. Configure one or more serial protocols. For more information, refer to "Adding a Serial Port Protocol" (Page 412).

5. Type `commit` and press **Enter** to save the changes.

10.1.7 Restarting the Serial Server

To restart the serial server, type:

```
interfaces serial restart-serserver
```

10.1.8 Resetting a Serial Port

To reset a serial port, type:

```
interfaces serial port { name } reset
```

Where:

- `{ name }` is the name assigned to the port

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)
	Opinion Header Field
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 A1 67 0F 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
```

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 RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 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, type:

```
show interfaces serial port protocol
```

If protocols have been configured, a table or list similar to the following example appears:

```
ruggedcom# show interfaces serial port protocol
IFNAME   PROTOCOL
-------------------
ser-3-1  none
ser-3-2  none
ser-3-3  none
ser-3-4  none
ser-3-5  none
ser-3-6  none
```

If no serial port protocols have been configured, add protocols as needed. For more information, refer to "Adding a Serial Port Protocol" (Page 412).

10.2.3 Adding a Serial Port Protocol

To add a serial port protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the protocol by typing:

   ```
   interface serial { slot } { port } protocols { protocol }
   ```

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.

- `{ protocol }` is the protocol type. Options include **dnp**, **tcpmodbus**, **rawsocket**, **vmserial** and **microlok**.

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 413).
   - For information about configuring a Modbus TCP protocol, refer to "Configuring the Modbus TCP Protocol" (Page 414).
   - For information about configuring a raw socket protocol, refer to "Configuring the Raw Socket Protocol" (Page 415).
   - For information about configuring a MicroLok protocol, refer to "Configuring the MicroLok Protocol" (Page 416).
4. Type `commit` and press **Enter** to save the changes.

10.2.4 Configuring the DNP Protocol

To configure the DNP protocol for a serial port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » { interface } » protocols » dnp » setdnp***, where { interface } is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
`address-learning { address-learning }`	**Synopsis:** A string between 1 and 15 characters long The interface to learn the RTU address from.
`aging-timer { aging-timer }`	**Synopsis:** An integer between 60 and 10800 **Default:** 1000 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.
`max-connection { max-connection }`	**Synopsis:** An integer between 1 and 32 **Default:** 1 The maximum number of incoming DNP connections.

4. Add a Device Address table. For more information about adding Device Address tables, refer to "Adding a DNP Device Address Table" (Page 418).
5. Type `commit` and press **Enter** to save the changes.

10.2.5 Configuring the Modbus TCP Protocol

To configure the modbus TCP protocol for a serial port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » { interface } » protocols » tcpmodbus » settcpmodbus***, where { interface } is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
`response-timer { response-timer }`	**Synopsis:** An integer between 50 and 10000 **Default:** 100 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.
`pack-timer { pack-timer }`	**Synopsis:** An integer between 5 and 1000 **Default:** 1000 The maximum allowable time to wait for a response to a Modbus request to complete once it has started.
`turnaround { turnaround }`	**Synopsis:** An integer between 0 and 1000 **Default:** 0 The amount of delay (if any) to insert after the transmissions of Modbus broadcast messages out the serial port.
`retransmit { retransmit }`	**Synopsis:** An integer between 0 and 2 **Default:** 0 The number of times to retransmit the request to the RTU before giving up.
`max-connection { max-connection }`	**Synopsis:** An integer between 1 and 32 **Default:** 1 The maximum number of incoming connections.
`local-port { local-port }`	**Synopsis:** An integer **Default:** 502 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.
`rtu-list { rtu-list }`	**Synopsis:** A string 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.

4. Type `commit` and press **Enter** to save the changes.

10.2.6 Configuring the Raw Socket Protocol

To configure the raw socket protocol for a serial port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » { interface } » protocols » rawsocket***, where { interface } is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
`pack-char { pack-char }`	**Synopsis:** [off] or An integer between 0 and 255 **Default:** off The numeric value of the ASCII character which will force forwarding of accumulated data to the network.
`pack-timer { pack-timer }`	**Synopsis:** An integer between 5 and 1000 **Default:** 1000 The delay from the last received character until when data is forwarded.
`pack-size { pack-size }`	**Synopsis:** [max] or An integer between 16 and 1400 **Default:** max The maximum number of bytes received from the serial port to be forwarded.
`turnaround { turn around }`	**Synopsis:** An integer between 0 and 1000 **Default:** 0 The amount of delay (if any) to insert between the transmissions of individual messages out the serial port.
`call-direction { call-direction }`	**Synopsis:** [in | out | both] **Default:** out Whether to accept an incoming connection, place an outgoing connection or do both.
`max-connection { max-connection }`	**Synopsis:** An integer between 1 and 32 **Default:** 1 The maximum number of incoming connections to permit when the call direction is incoming.
`remote-ip { re mote-ip }`	**Synopsis:** 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.

Parameter	Description
`remote-port { remote-port }`	**Synopsis:** An integer between 1024 and 65535 The TCP destination port used in outgoing connections.
`local-ip { local-ip }`	**Synopsis:** 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 { local-port }`	**Synopsis:** An integer between 1024 and 65535 The local TCP/UDP port to use to accept incoming connections.
`transport { transport }`	**Synopsis:** [tcp | udp] **Default:** 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 432).
5. Type `commit` and press **Enter** to save the changes.

10.2.7 Configuring the MicroLok Protocol

To configure the MicroLok protocol for a serial port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » { interface } » protocols » microLok » setMicroLok***, where { interface } is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
`transport { transport }`	**Synopsis:** [tcp | udp] **Default:** udp The network transport used to transport protocol data over an IP network.
`local-port { local-port }`	**Synopsis:** An integer between 1024 and 65535 **Default:** 60000 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.

Parameter	Description
`dscp { dscp }`	**Synopsis:** An integer between 0 and 63 **Default:** 0 The DSCP value for Microlok traffic priority. Only egress traffic is supported.

4. Add a Device Address table. For more information about adding Device Address tables, refer to "Adding a MicroLok Device Address Table" (Page 420).
5. Type `commit` and press **Enter** to save the changes.

10.2.8 Deleting a Serial Port Protocol

To delete a serial port protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the serial port protocol by typing:

   ```
   no interface serial { slot } { port } protocols { proto
   col }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ protocol }` is the protocol type
3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config interface serial { interface } protocols
dnp setdnp device-table
```

Where:

- `{ interface }` is the slot name and port number of the serial port

If Device Address tables have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial protocols dnp setdnp device-table
interface
 serial lm3 1
  protocols dnp
   setdnp device-table 12
    remote-ip     172.30.130.2
    remote-device
   !
  !
 !
!
```

If no Device Address tables have been configured, add tables as needed. For more information, refer to "Adding a DNP Device Address Table" (Page 418).

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. Make sure the CLI is in Configuration mode.
2. `interface serial { slot } { port } protocols dnp setdnp device-table { address }`

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.
   - `{ address }` is 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.
3. Configure the following parameter(s) as required:

Parameter	Description
`remote-ip { remote-ip }`	**Synopsis:** 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.

4. Type `commit` and press **Enter** to save the changes.

10.3.3 Deleting a Device Address Table

To delete a Device Address table, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the Device Address Table by typing:

   ```
   no interface serial { slot } { port } protocols dnp setdnp
   device-table { address }
   ```

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.
   - `{ address }` is 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.
3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config interface serial { interface } protocols
microlok setmicrolok device-address-table
```

Where:

- `{ interface }` is the slot name and port number of the serial port

If Device Address tables have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial protocols microlok setmicrolok de
vice-address-table
interface
 serial lm3 1
  protocols microlok
   setmicrolok device-address-table 65535
   !
  !
 !
!
```

If no Device Address tables have been configured, add tables as needed. For more information, refer to "Adding a MicroLok Device Address Table" (Page 420).

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. Make sure the CLI is in Configuration mode.
2. `interface serial { slot } { port } protocols microlok set microlok device-address-table { address }`

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.
   - `{ address }` is the local or remote MicroLok device address. The address may be that of a MicroLok device connected to a local serial port or one available via the serial port of a remote IP host.
3. Configure the following parameter(s) as required:

Parameter	Description
`device-name { device-name }`	**Synopsis:** A string between 1 and 16 characters long The addressed Microlok device name
`device-type { device-type }`	**Synopsis:** [local | remote] **Default:** local 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'.
`remote-ip { remote-ip }`	**Synopsis:** A string between 7 and 15 characters long 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'.

4. Type `commit` and press **Enter** to save the changes.

10.4.3 Deleting a MicroLok Device Address Table

To delete a Device Address table, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the Device Address Table by typing:

   ```
   no interface serial { slot } { port } protocols microlok
   setmicrolok device-address-table { address }
   ```

   Where:

   - `{ slot }` is the name of the module location.
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.
   - `{ address }` is 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.

3. Type `commit` and press **Enter** to save the changes.

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. Add the rawsocket protocol. For more information, refer to "Adding a Serial Port Protocol" (Page 412).
2. Configure the Remote Host for the encapsulation of raw-socket serial over multicast with the destination Multicast IP, UDP port, and interface(s). For more information, refer to "Adding a Remote Host" (Page 432) and "Adding a Remote Host Interface" (Page 436).
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 434) and "Adding a Local Host Interface" (Page 437).

4. Verify that multicast traffic can be seen on the incoming and outgoing interface(s) by typing:

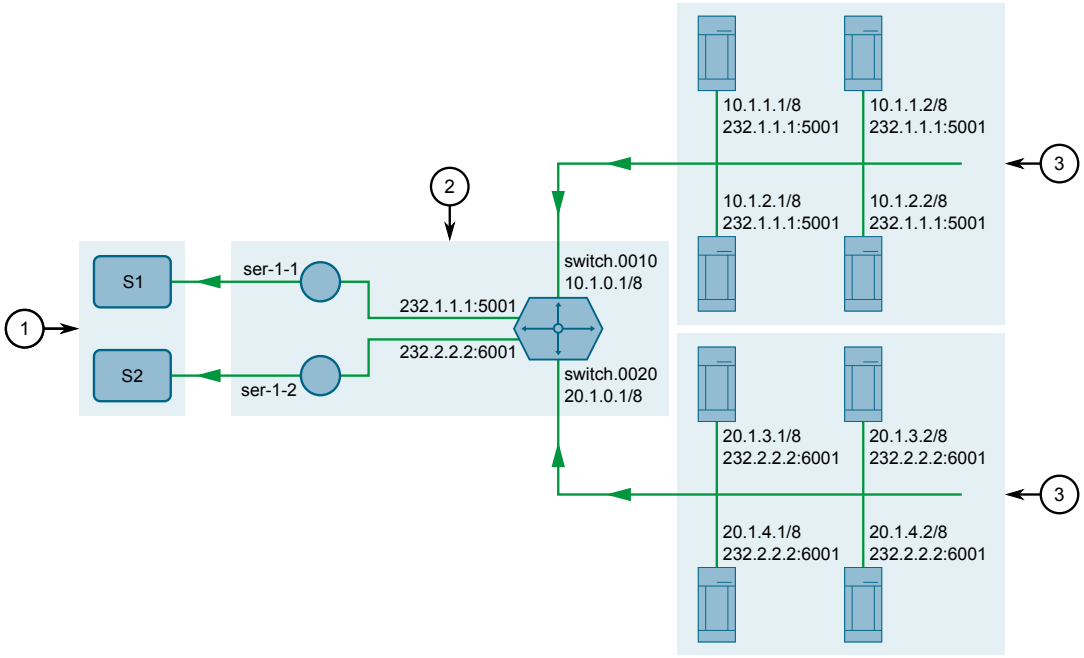
```
traceserial
```

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 RX1500)
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 269).

2. Create a rawsocket connection for ser-1-1:

   ```
   interface serial lm1 1 protocols rawsocket
   ```

   For more information, refer to "Adding a Serial Port Protocol" (Page 412).
3. Set the rawsocket of the local port to 5001:

   ```
   setrawsocket local-port 5001
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).
4. Set the transport method to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).
5. Set the multicast group for the local host to 232.1.1.1:

   ```
   setrawsocket local-host 232.1.1.1
   ```

   For more information, refer to "Adding a Local Host" (Page 434).
6. Set *switch.0010* as the interface for the local host:

   ```
   interface switch.0010
   ```

   For more information, refer to "Adding a Local Host Interface" (Page 437)
7. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

1. Create a raw socket connection for ser-1-2:

   ```
   interface serial lm1 2 protocols rawsocket
   ```

   For more information, refer to "Adding a Serial Port Protocol" (Page 412).
2. Set the local port for raw socket to 6001:

   ```
   setrawsocket local-port 6001
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).
3. Set the transport method for raw socket to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).
4. Set the multicast group for the local host to 232.2.2.2:

   ```
   setrawsocket local-host 232.2.2.2
   ```

   For more information, refer to "Adding a Local Host" (Page 434).

5. Set *switch.0020* as the interface for the local host:

   ```
   interface switch.0020
   ```

   For more information, refer to "Adding a Local Host Interface" (Page 437)
6. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.
7. Verify the configuration by typing the following:

   ```
   traceserial
   ```

Final Configuration Example

ser-1-1 Configuration

```
serial lm1 1
  no alias
  protocols rawsocket
   setrawsocket local-port 5001
   setrawsocket transport udp
   setrawsocket local-host 232.1.1.1
    interface switch.0010
```

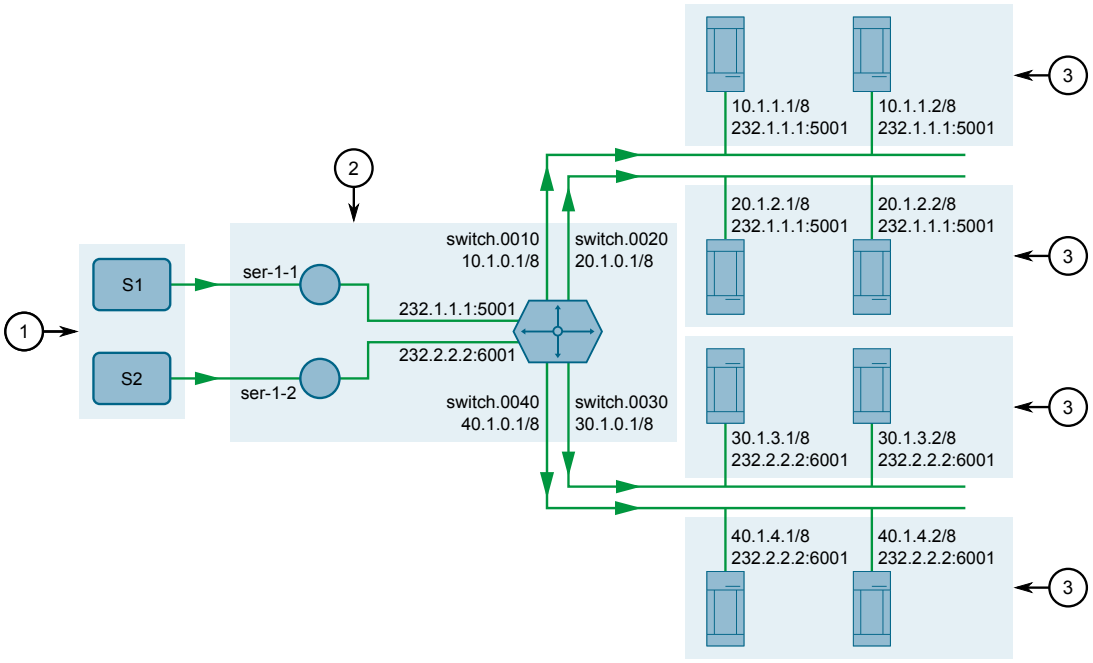
ser-1-2 Configuration

```
serial lm1 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 RX1500)
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 269).
2. Create a raw socket connection for ser-1-1:

   ```
   interface serial lm1 1 protocols rawsocket
   ```

   For more information, refer to "Adding a Serial Port Protocol" (Page 412).
3. Set the raw socket of the local port to 10001:

   ```
   setrawsocket local-port 10001
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).
4. Set the transport method to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).

5. Set the multicast group for the local host to 232.1.1.1 and the UDP destination port to 5001:

   ```
   setrawsocket remote-host 232.1.1.1 5001
   ```

   For more information, refer to "Adding a Remote Host" (Page 432).

6. Set *switch.0010* and *switch.0020* as the interfaces for the remote host:

   ```
   interface switch.0010
   interface switch.0020
   ```

   For more information, refer to "Adding a Remote Host Interface" (Page 436)

7. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

1. Create a raw socket connection for ser-1-2:

   ```
   interface serial lm1 2 protocols rawsocket
   ```

   For more information, refer to "Adding a Serial Port Protocol" (Page 412).

2. Set the rawsocket of the local port to 10002:

   ```
   setrawsocket local-port 10002
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).

3. Set the transport method to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).

4. Set the multicast group for the local host to 232.2.2.2 and the UDP destination port to 6001:

   ```
   setrawsocket local-host 232.2.2.2 6001
   ```

   For more information, refer to "Adding a Local Host" (Page 434).

5. Set *switch.0030* and *switch.0040* as the interfaces for the remote host:

   ```
   interface switch.0030
   interface switch.0040
   ```

   For more information, refer to "Adding a Remote Host Interface" (Page 436)

6. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

7. Verify the configuration by typing the following:

   ```
   traceserial
   ```

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

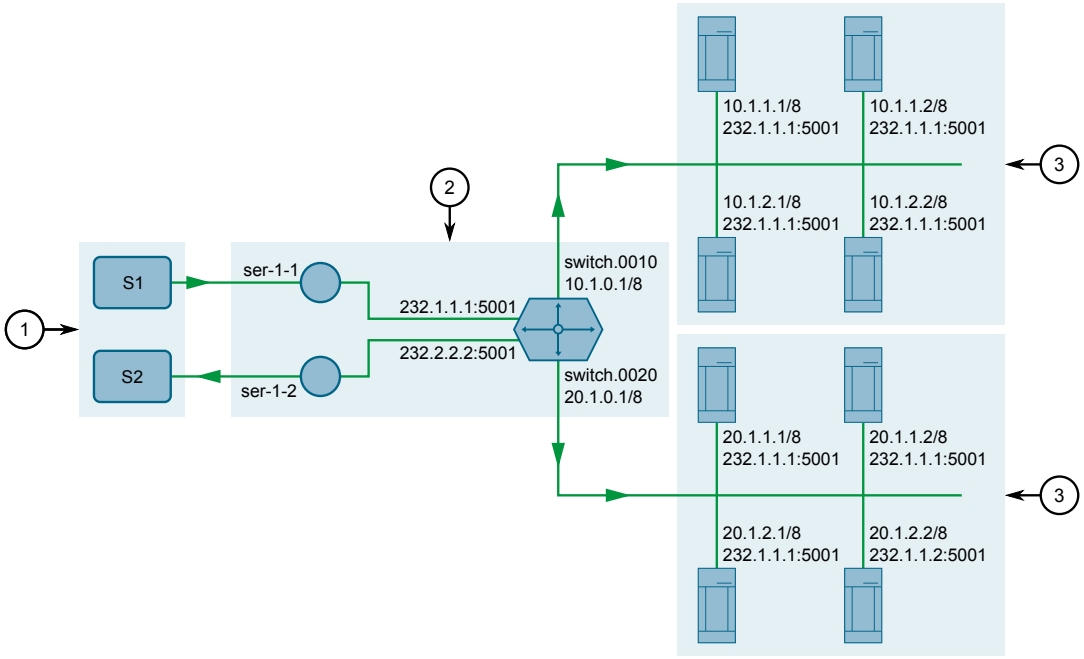
```
serial lm1 2
  no alias
  protocols rawsocket
   setrawsocket local-port 10002
   setrawsocket transport udp
   setrawsocket remote-host 232.2.2.2 6001
    interface switch.0030
    !
    interface switch.0040
```

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 RX1500)
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 269).
2. Create a raw socket connection for ser-1-1:

   ```
   interface serial lm1 1 protocols rawsocket
   ```

   For more information, refer to "Adding a Serial Port Protocol" (Page 412).
3. Set the raw socket of the local port to 10001:

   ```
   setrawsocket local-port 10001
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).
4. Set the transport method to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).

5. Set the multicast group for the remote host to 232.1.1.1 and the UDP destination port to 5001:

   ```
   setrawsocket remote-host 232.1.1.1 5001
   ```

   For more information, refer to "Adding a Remote Host" (Page 432).

6. Set *switch.0010* and *switch.0020* as the interfaces for the remote host:

   ```
   interface switch.0010
   interface switch.0020
   ```

   For more information, refer to "Adding a Remote Host Interface" (Page 436)

7. Enable remote host loopback:

   ```
   loopback true
   ```

   For more information, refer to "Adding a Local Host" (Page 434)

8. Create a raw socket connection for ser-1-2:

   ```
   interface serial lm1 2 protocols rawsocket
   ```

   For more information, refer to "Adding a Serial Port Protocol" (Page 412)

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:

   ```
   setrawsocket local-port 5001
   ```

   For more information, refer to "Adding a Local Host" (Page 434)

10. Set the transport method to *UDP*:

    ```
    setrawsocket transport udp
    ```

    For more information, refer to "Configuring the Raw Socket Protocol" (Page 415).

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.

    ```
    setrawsocket local-host 232.1.1.1
    ```

    For more information, refer to "Adding a Local Host" (Page 434)

12. Enable local host loopback:

    ```
    loopback true
    ```

    For more information, refer to "Adding a Local Host" (Page 434)

13. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

14. Verify the configuration by typing the following:

    ```
    traceserial
    ```

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
    loopback true
    interface switch.0010
    !
    interface switch.0020
```

Serial Port 2 Configuration

```
serial lm1 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, type:

```
show running-config interface serial protocols rawsocket se
trawsocket remote-host
```

If hosts have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial protocols rawsocket setrawsocket
 remote-host
interface
serial lm5 1
  no alias
  protocols rawsocket
   setrawsocket local-port 30001
   setrawsocket transport udp
   setrawsocket remote-host 1.1.1.2 60001
   !
   setrawsocket remote-host 232.1.1.1 60001
    interface switch.0010
    !
   !
  !
!
```

```
!
!
```

If no remote hosts have been configured, add hosts as needed. For more information, refer to "Adding a Remote Host" (Page 432).

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. Make sure the CLI is in Configuration mode.
2. Add the remote host by typing:

   ```
   interface serial { slot } { port } protocols rawsocket se
   trawsocket remote-host { address } { remote-port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ address }` is the IP address for the remote host or a multicast group IP address for which the interface is a source
   - `{ remote-port }` is the port number for the remote host
3. Configure the following parameter(s) as required:

Parameter	Description
`loopback { loopback }`	**Synopsis:** [true | false] **Default:** false Enables transmitting to the loopback interface with the destination multicast group IP address and remote port. Matching local hosts with loopback enabled will receive the transmitted data.

4. [Optional] Add a remote host interface. For more information, refer to "Adding a Remote Host Interface" (Page 436).
5. Type `commit` and press **Enter** to save the changes.

10.6.3 Deleting a Remote Host

To delete a remote host, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the remote host by typing:

   ```
   no interface serial { slot } { port } protocols rawsocket
   setrawsocket remote-host { address } { remote-port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ address }` is the IP address for the remote host
   - `{ remote-port }` is the port number for the remote host
3. Type `commit` and press **Enter** to save 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, type:

```
show running-config interface serial protocols rawsocket se
trawsocket local-host
```

If hosts have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial protocols rawsocket setrawsocket
 local-host
interface
 serial lm5 1
  protocols rawsocket
   setrawsocket local-host 224.1.2.1
    interface ge-4-4
    !
   !
  !
 !
!
```

If no local hosts have been configured, add hosts as needed. For more information, refer to "Adding a Local Host" (Page 434).

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. Make sure the CLI is in Configuration mode.
2. Add the local host by typing:

   ```
   interface serial { slot } { port } protocols rawsocket se
   trawsocket local-host { address }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ address }` is a multicast group IP address for which the interface is a sink

   Note

   When a local host is added, either loopback must be enabled or a local host interface must be added.

3. If a local host interface is required, proceed to step 4 (Page 434). 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.
4. [Optional] Add a local host interface. For more information, refer to "Adding a Local Host Interface" (Page 437).
5. Type `commit` and press **Enter** to save the changes.

10.7.3 Deleting a Local Host

To delete a local host, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the local host by typing:

   ```
   no interface serial { slot } { port } protocols rawsocket
   setrawsocket local-host { address } { local-port }
   ```

   Where:

   - `{ slot }` is the name of the module location

- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ address }` is the IP address for the local host
- `{ local-port }` is the port number for the local host

3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config interface serial { slot } { port } proto
cols rawsocket setrawsocket remote-host { remote-host } in
terface
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ remote-host }` is the remote host

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial lm5 1 protocols rawsocket setraw
socket remote-host 224.1.2.1 interface
interface
 serial lm5 1
  protocols rawsocket
   setrawsocket remote-host 224.1.2.1
    interface ge-4-4
    !
   !
  !
 !
!
```

If no remote host interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Remote Host Interface" (Page 436).

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 the CLI is in Configuration mode.
2. Navigate to:

   ```
   interface serial { slot } { port } protocols rawsocket se
   trawsocket remote-host { remote-host } interface
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ remote-host }` is the remote host
3. Configure the following parameter(s) as required:

Parameter	Description
`name { name }`	**Synopsis:** A string The transmitting interface's name for the destination multicast group IP address and remote port.

4. Type `commit` and press **Enter** to save the changes.

10.8.3 Deleting a Remote Host Interface

To delete a remote host interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the remote host by typing:

   ```
   no interface serial { slot } { port } protocols rawsocket
   setrawsocket remote-host { remote-host } interface { in
   terface name }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ remote-host }` is the remote host
   - `{ interface name }` is the name of the interface

3. Type `commit` and press **Enter** to save the changes.

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, type:

```
show running-config interface serial { slot } { port } proto
cols rawsocket setrawsocket local-host { local-host } inter
face
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ local-host }` is the local host

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial lm5 1 protocols rawsocket setraw
socket local-host 224.1.2.1 interface
interface
 serial lm5 1
  protocols rawsocket
   setrawsocket local-host 224.1.2.1
    interface ge-4-4
    !
   !
  !
 !
!
```

If no local host interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Local Host Interface" (Page 437).

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. Make sure the CLI is in Configuration mode.
2. Navigate to:

   ```
   interface serial { slot } { port } protocols rawsocket se
   trawsocket local-host { local-host } interface
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ local-host }` is the local host
3. Configure the following parameter(s) as required:

Parameter	Description
`name { name }`	**Synopsis:** A string The receiving interface's name for the source multicast group IP address and the local port number defined for the serial port.

4. Type `commit` and press **Enter** to save the changes.

10.9.3 Deleting a Local Host Interface

To delete a local host interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the local host by typing:

   ```
   no interface serial { slot } { port } protocols rawsocket
   setrawsocket local-host { local-host } interface { inter
   face name }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ local-host }` is the local host
   - `{ interface name }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

11 WAN and Wireless

This chapter describes how to configure and manage the various WAN and wireless interfaces available in RUGGEDCOM ROX II.

Note

Some features require the device to be equipped with a specific line module.

11.1 Connecting as a PPP Client

To connect or disconnect from a cellular network as a PPP client, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure the cellular modem interface has been configured. For more information, refer to "Configuring a Cellular Modem Interface" (Page 456).
3. Make sure an appropriate cellular modem profile has been configured. For more information, refer to either:
   - "Managing CDMA Profiles" (Page 464)
   - "Managing GSM Profiles" (Page 466)
4. Make sure an account has been activated with a service provider for the modem type (e.g. HSPA+, Edge or CDMA).
5. Make sure antennas are properly connected to the device before initiating the connection. For more information, refer to the "RUGGEDCOM RX1500 Installation Manual".
6. For HSPA+ and Edge modems, insert a SIM card into the cellular modem module.
7. For CDMA modems, activate the modem either manually or over-the-air. For more information, refer to "Activating a Cellular Modem Account" (Page 462).
8. Verify the network status for the appropriate cellular modem type. For more information, refer to:
   - "Viewing the HSPA Network Status for Cellular Modems" (Page 459)
   - "Viewing the CDMA Network Status for Cellular Modems" (Page 460)
9. Select the cellular modem profile to use when connecting to the wireless network by typing:

   ```
   interface cellmodem { slot } { port } [ hspa | edge | cd
   ma ] ppp-client connect-to { profile }
   ```

   Where:

- `{ slot }` is the name of the module location.
- `{ profile }` is the cellular modem profile.

10. Type `commit` and press **Enter** to save the changes.

11.2 Managing WAN Interfaces

This section describes how to configure an interface to a Wide Area Network (WAN).

Note

WAN interfaces are not supported by the RUGGEDCOM RX1524 or RX1536.

11.2.1 Viewing a List of WAN Interfaces

To view a list of WAN interfaces, type:

```
show running-config interface wan
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan
interface
 wan lm2 1
  enabled
  no alias
  t1 channel 2
   connection ppp nomagic
  !
 !
 wan lm2 2
  no alias
 !
!
```

11.2.2 Configuring a WAN Interface

To configure a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface }***, where { interface } is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false Enables this WAN port.

Parameter	Description
`link-alarms { link-alarms }`	**Synopsis:** [true | false] **Default:** 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.
`alias { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface

4. Configure a T1 or E1 line. For more information, refer to "Configuring a T1 Line" (Page 444) or "Configuring an E1 Line" (Page 444).
5. Type `commit` and press **Enter** to save the changes.

11.2.3 Viewing WAN Statistics

To view statistics for the WAN network, type:

```
show interfaces wan t1e1
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces wan t1e1
interfaces wan t1e1 te1-2-1
 slot        lm2
 port        1
 channelno   2
 state       up
 reliability 255/255
 receive-stats
  frames       227
  bytes        6306
  linkinactive 0
  load         1/255
 transmit-stats
  txframes    217
  txbytes     5733
  txrealigned 0
  load        1/255
 receive-error
  overrun       0
  crcerror      0
  abort         0
  corruption    0
  pcierror      0
  dmaerror      0
.
.
.
```

Note

Some statistics are only available for physical or logical interfaces.

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** [sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport] or A string Line module name of the slot.
port	**Synopsis:** An integer between 1 and 16 or A string Port number on the slot.
channelno	**Synopsis:** An integer between 1 and 32 or A string Channel number on the port.
state	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] Status of the interface.
local	**Synopsis:** A string Loacal IP address of the interface.
remote	**Synopsis:** A string Peer IP address.
mask	**Synopsis:** A string Netmask.
reliability	**Synopsis:** A string Reliability of the interface over 5 minutes. It is calculated as an exponential average of the fraction of the total received and transmitted errors and the total packets that are received and transmitted successfully.
create-time	**Synopsis:** A string The duration of time since interface is created.
last-status-change	**Synopsis:** A string The duration of time since last change of interface status.

For information about clearing the WAN statistics, refer to "Clearing WAN Statistics" (Page 442).

11.2.4 Clearing WAN Statistics

The following describes how to clear the statistics collected when WAN interfaces are enabled. Statistics for one or all interfaces can be cleared.

To clear statistics for all WAN interfaces, type:

```
interfaces wan clearstatistics all-interfaces
```

To clear statistics for a specific WAN interface, type:

```
interfaces wan clearstatistics [ ddsName | t1e1Name |
t3e3Name ] { interface }
```

Where:

- `{ interface }` is the WAN interface

11.2.5 Performing a Loopback Test

Loopback tests are a useful means of testing the T1/E1 hardware on the device and the T1/E1 connection with remote devices. Three types of tests are available:

- **Digital Loopback**
  RUGGEDCOM ROX II digitally sends frames and immediately returns them to the device. This test is used to isolate problems within the T1/E1 circuit.
- **Remote Loopback**
  RUGGEDCOM ROX II transmits frames to the Tx port and compares them with frames received on the Rx port. A loopback plug or cable must be installed on the T1/E1 port. This test is used to isolate problems within the WAN module.
- **Line Loopback**
  RUGGEDCOM ROX II transmits frames across the T1/E1 line to a remote Channel Service Unit/Data Service Unit (CSU/DSU). This test determines if a problem exists outside the device.

Regardless of the loopback type, a loopback test is successful if the frames received match those that were sent. Missing frames and frames that contain discrepancies indicate a potential problem in the T1/E1 hardware or line.

To perform a loopback test on a WAN interface, do the following:

⚠ NOTICE

Performing a loopback test on an active interface will immediately cause it to go down. However, the trunk will be automatically initialized after the test is complete.

1. Make sure a WAN interface has been configured. For more information, refer to "Configuring a WAN Interface" (Page 440).
2. Configure the following parameter(s) as required:

   ```
   interfaces wan loopback duration { time } nloops { loops }
   physical-name { interface } type [ digital | line | re
   mote ] duration { seconds }
   ```

   Where:

   - `{ time }` is the number of seconds required to run the test
   - `{ loops }` is the number of loops
   - `{ interface }` is the name of the physical interface

- `{ duration }` is the duration of the test in seconds

The results are displayed when the test is complete.

11.2.6 Configuring a T1 Line

To configure a T1 line for a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface } » t1***, where { interface } is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
`frame { frame }`	**Synopsis:** [esf] **Default:** esf The frame format.
`line-code { line-code }`	**Synopsis:** [b8zs] **Default:** b8zs The line encoding/decoding scheme.
`clock { clock }`	**Synopsis:** [normal | master] **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.
`lbo { lbo }`	**Synopsis:** [0db | 7.5db | 15db | 22.5db | 0-110ft | 110-220ft | 220-330ft | 330-440ft | 440-550ft | 550-660ft] **Default:** 0db Line Build Out: tunes the shape of the T1 pulses and adjusts their amplitude depending upon distances and the desired attenuation.

4. Type `commit` and press **Enter** to save the changes.

11.2.7 Configuring an E1 Line

To configure E1 parameters for a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface } » E1***, where { interface } is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
`frame { frame }`	**Synopsis:** [ncrc4 | crc4] **Default:** ncrc4 The frame format.
`line-code { line-code }`	**Synopsis:** [hdb3] **Default:** hdb3 A line encoding/decoding scheme.
`clock { clock }`	**Synopsis:** [normal | master] **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.

4. Type `commit` and press **Enter** to save the changes.

11.2.8 Configuring DDS

To configure DDS for a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface } » dds » ddsparams***, where { interface } is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
`mode { mode }`	**Synopsis:** [56k | 64k] **Default:** 56k DDS speed mode (kbps).
`clock { clock }`	**Synopsis:** [normal | master] **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.

4. Configure a PPP or frame relay connection. For more information, refer to "Configuring a PPP Connection" (Page 449) or "Configuring a Frame Relay Connection" (Page 450).
5. Type `commit` and press **Enter** to save the changes.

11.2.9 Managing Channels

This section describes how to create and manage channels for a T1/E1 WAN interface.

11.2.9.1 Viewing a List of Channels

To view a list of T1 or E1 lines, type:

```
show running-config interface wan { slot } { port } { proto
col } channel
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ protocol }` is either T1 or E1

If channels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan lm2 1 t1 channel
interface
 wan lm2 1
  t1 channel 2
   connection ppp nomagic
  !
 !
!
```

If no channels have been configured, add channels as needed. For more information, refer to "Adding a Channel" (Page 446).

11.2.9.2 Adding a Channel

To configure a channel for a T1/E1 physical interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the channel by typing:

   ```
   interface wan { slot } { port } { protocol } channel
   { number }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ protocol }` is either T1 or E1
   - `{ number }` is the channel number

3. Configure the following parameter(s) as required:

For T1 Lines

Parameter	Description
`{ channelnumber }`	**Synopsis:** An integer between 1 and 24 Channel Number.
`ts { ts }`	**Synopsis:** A string between 0 and 128 characters long **Default:** all Time slots for this channel. Format: the string 'all', or a comma-separated list of numbers in the range of 1 to 24. To specify a range of numbers, separate the start and end of the range with '..' or with a hyphen '-' Example 1: 1,2,3 and 1..3 both represent time slots 1 through 3. Example 2: 1,2,5..10,11 represents time slots 1, 2, 5, 6, 7, 8, 9, 10, and 11.

For E1 Lines

Parameter	Description
`{ channelnumber }`	**Synopsis:** An integer between 1 and 31 The channel number.
`ts { ts }`	**Synopsis:** A string between 0 and 128 characters long **Default:** all Time slots for this channel. Format: 'all' or number from 1-31, separated by ',' or '..' or with a hyphen '-' Ex1: 1,2,3 or 1..3 which represents time slot from 1 to 3. Ex2: 1,2,5..10,11 which represents time slot 1,2,5,6,7,8,9,10,11

4. If necessary, configure VLANs for an HDLC-ETH connection. For more information, refer to "Adding an HDLC-ETH VLAN" (Page 454).
5. If necessary, configure an MLPPP connection. For more information, refer to "Configuring a Multi Link PPP Connection" (Page 449).
6. If necessary, configure a PPP connection. For more information, refer to "Configuring a PPP Connection" (Page 449).
7. If necessary, configure a frame relay connection. For more information, refer to "Configuring a Frame Relay Connection" (Page 450).
8. Type `commit` and press **Enter** to save the changes.

11.2.9.3 Deleting a Channel

To delete a channel configured for a T1/E1 physical interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the channel by typing:

   ```
   no interface wan { slot } { port } { protocol } channel
   { number }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - `{ protocol }` is either T1 or E1
   - `{ number }` is the channel number

3. Type `commit` and press **Enter** to save the changes.

11.2.10 Configuring an HDLC-ETH Connection

HDLC-ETH refers to Ethernet over an HDLC (High-Level Data Link Control) connection on a T1/E1 line. This connection passes Layer2 and Layer 3 packets from a LAN through a T1/E1 line by creating a virtual switch containing one or more Ethernet interfaces and an HDLC-ETH interface. For more information about configuring a virtual switch, refer to "Adding a Virtual Switch" (Page 489).

A T1/E1 WAN interface configured for HDLC-ETH works like a routable Ethernet port, such as fe-cm-1 and switch.0001, which can be configured with an IP address and subnet mask. Since it acts the same as an Ethernet port, a peer IP address for an HDLC-ETH interface does not need to be configured.

Before configuring an HDLC-ETH connection, a T1/E1 line must be in place. For more information, refer to:

- "Configuring a T1 Line" (Page 444)
- "Configuring an E1 Line" (Page 444)

To configure an HLDC-ETH connection for a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface } » { protocol } » channel » { number } » connection » hdlc-eth***, where { interface } is the WAN interface, { parameter } is either T1 or E1, and { number } is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
`encoding { encoding }`	**Synopsis:** [nrz] **Default:** nrz HDLC encoding type

Parameter	Description
`parity { parity }`	**Synopsis:** [crc16_ccitt] **Default:** crc16_ccitt HDLC parity type
`on-demand`	This interface is up or down on demand of link fail over.
`mtu { mtu }`	**Synopsis:** An integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

4. Add one or more VLANs for the HDLC-ETH connection. For more information, refer to "Adding an HDLC-ETH VLAN" (Page 454).
5. Type `commit` and press **Enter** to save the changes.

11.2.11 Configuring a Multi Link PPP Connection

To configure a Multi Link Point-to-Point Protocol (MLPPP) connection for a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface } » { protocol } » channel » { number }***, where { interface } is the WAN interface, { parameter } is either T1 or E1, and { number } is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
`bundle { bundle }`	**Synopsis:** An integer between 1 and 50 **Default:** 1 The bundle number
`on-demand`	This interface is up or down on demand of link fail over.
`mtu { mtu }`	**Synopsis:** An integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

4. Type `commit` and press **Enter** to save the changes.

11.2.12 Configuring a PPP Connection

To configure a Point-to-Point Protocol (PPP) connection, do the following:

1. Make sure the CLI is in Configuration mode.

2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**
     interface » wan » { interface } » { protocol } » channel » { number } » connection, where { interface } is the WAN interface, { parameter } is either T1 or E1, and { number } is the channel number.
   - **For DDS**
     interface » wan » { interface } » dds » connection, where { interface } is the WAN interface, { parameter } is either T1 or E1, and { number } is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
`nomagic { nomagic }`	**Synopsis:** [true | false] **Default:** false Disables the Magic Number. (Valid on RX1000 only)
`on-demand`	This interface is up or down on demand of link fail over.
`mtu { mtu }`	**Synopsis:** An integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

4. Type `commit` and press **Enter** to save the changes.

11.2.13 Configuring a Frame Relay Connection

To configure a frame relay connection for a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**
     interface » wan » { interface } » { protocol } » channel » { number } » connection, where { interface } is the WAN interface, { parameter } is either T1 or E1, and { number } is the channel number.
   - **For DDS**
     interface » wan » { interface } » dds » connection, where { interface } is the WAN interface, { parameter } is either T1 or E1, and { number } is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
`station { station }`	**Synopsis:** [cpe | switch] **Default:** cpe The behavior of the frame relay connection, i.e. CPE (Customer Premises Equipment) or as a switch.
`signal { signal }`	**Synopsis:** [ansi | lmi | q933 | none] **Default:** ansi The frame relay link management protocol used.
`t391 { t391 }`	**Synopsis:** An integer between 5 and 30 **Default:** 10 (Link Integrity Verification polling) Indicates the number of seconds between transmission of in-channel signaling messages. Valid for cpe.
`t392 { t392 }`	**Synopsis:** An integer between 5 and 30 **Default:** 16 (Verification of polling cycle) Indicates the expected number of seconds between reception of in-channel signaling messages transmitted by cpe. Valid for Switch.
`n391 { n391 }`	**Synopsis:** An integer between 1 and 255 **Default:** 6 Defines the frequency of transmission of full status enquiry messages. Valid for CPE.
`n392 { n392 }`	**Synopsis:** An integer between 1 and 10 **Default:** 4 The number of error events (enumerated by n393) for which the channel is declared inactive; valid for either cpe or Switch.
`n393 { n393 }`	**Synopsis:** An integer between 1 and 10 **Default:** 4 The number of error events on the frame relay channel; valid for either cpe or switch.

4. Type `commit` and press **Enter** to save the changes.

11.2.14 Managing Data Links for Frame Relay Connections

Before data can be forwarded over a Frame Relay connection to a remote destination, links to link-local virtual circuits must be configured.

11.2.14.1 Viewing a List of Data Links

To view a list of data links configured for a frame relay connection, type:

```
show running-config interface wan { interface } { protocol }
channel { number } connection framerelay dlci
```

Where:

- `{ interface }` is the WAN interface
- `{ protocol }` is either T1 or E1
- `{ number }` is the channel number

If data links have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan lm2 1 t1 channel 1 connection
 framerelay dlci
interface
wan lm2 1
  t1 channel 1
   connection framerelay dlci 100
   !
  !
!
```

If no data links have been configured, add data links as needed. For more information, refer to "Adding a Data Link" (Page 452).

11.2.14.2 Adding a Data Link

To add a data link for a frame relay connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the data link by typing:

   ```
   interface wan { interface } { protocol } channel { num
   ber } connection framerelay dlci { id }
   ```

   Where:

   - `{ interface }` is the WAN interface
   - `{ protocol }` is either T1 or E1
   - `{ number }` is the channel number
   - `{ id }` is the ID of the data link
3. Configure the following parameter(s) as required:

Parameter	Description
`on-demand`	This interface is up or down on demand of link fail over.

Parameter	Description
`mtu { mtu }`	**Synopsis:** An integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

4. Type `commit` and press **Enter** to save the changes.

11.2.14.3 Deleting a Data Link

To delete a data link for a frame relay connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the data link by typing:

   ```
   no interface wan { interface } { protocol } channel { num
   ber } connection framerelay dlci { id }
   ```

   Where:

   - `{ interface }` is the WAN interface
   - `{ protocol }` is either T1 or E1
   - `{ number }` is the channel number
   - `{ id }` is the ID of the data link
3. Type `commit` and press **Enter** to save the changes.

11.2.15 Managing VLANs for HDLC-ETH Connections

VLANs can be used to create logical separations between multiple HDLC-ETH connections within a T1 or E1 channel.

Note

Frames egressed through this logical interface will not be tagged with the VLAN configured for the HDLC-ETH connection.

11.2.15.1 Viewing a List of HDLC-ETH VLANs

To view a list of VLANs configured for an HDLC-ETH connection, type:

```
show running-config interface wan { interface } { protocol }
channel connection hdlc-eth vlan { id }
```

Where:

- `{ interface }` is the WAN interface

- `{ protocol }` is either T1 or E1
- `{ id }` is the ID of the VLAN

If VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan lm4 1 t1 channel connection hdlc-eth
 vlan | tab
                                IP
                    ON          ADDRESS
CHANNELNUMBER  VID  DEMAND  MTU   SRC      QOS  INGRESS  MARK
-----------------------------------------------------------------
1
               100  -       1500  static
               200  -       1500  static

 !
!
```

If no VLANs have been configured, add VLANs as needed. For more information, refer to "Adding an HDLC-ETH VLAN" (Page 454).

11.2.15.2 Adding an HDLC-ETH VLAN

To add a VLAN to an HDLC-ETH connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the VLAN by typing:

   ```
   interface wan { interface } { protocol } channel { num
   ber } connection hdlc-eth vlan { id }
   ```

   Where:

   - `{ interface }` is the WAN interface
   - `{ protocol }` is either T1 or E1
   - `{ number }` is the channel number
   - `{ id }` is the ID of the VLAN
3. Configure the following parameter(s) as required:

Parameter	Description
`on-demand`	This interface is up or down on demand of link fail over.
`mtu { mtu }`	**Synopsis:** An integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
`ip-address-src { ip-address-src }`	**Synopsis:** [static | dynamic] **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a

Parameter	Description
	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

4. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to "Adding a QoS Map" (Page 919).
5. Type `commit` and press **Enter** to save the changes.

11.2.15.3 Deleting an HDLC-ETH VLAN

To delete a VLAN for an HDLC-ETH connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the VLAN by typing:

   ```
   no interface wan { interface } { protocol } channel { num
   ber } connection hdlc-eth vlan { id }
   ```

   Where:

   - `{ interface }` is the WAN interface
   - `{ protocol }` is either T1 or E1
   - `{ number }` is the channel number
   - `{ id }` is the ID of the VLAN
3. Type `commit` and press **Enter** to save the changes.

11.3 Managing Cellular Modem Interfaces

This section describes how to configure an interface to a cellular network. Depending on the cellular modem module installed, the device can access a 3G or 4G LTE network. Some modules also feature GPS capabilities.

Note

Cellular modems with support for EDVO network technology are backwards compatible with CDMA 2G and CDMA 1x RTT networks.

Cellular modems with support for HSPA+ network technology are backwards compatible with GSM, GPRS, EDGE, UMTS, HSDPA/HSUPA networks.

11.3.1 Enabling/Disabling Cellular Modem Interfaces

To enable or disable a cellular modem interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***interface » wan » { interface }***, where { interface } is the cellular modem interface.
3. Enable or disable the desired cellular modem interface by typing:

   Enable

   ```
   interface cellmodem { interface } enabled
   ```

   Where { interface } is the cellular modem interface.

   Disable

   ```
   no interface cellmodem { interface } enabled
   ```

   Where { interface } is the cellular modem interface.
4. If the interface is enabled, further configure the interface as required. For more information, refer to "Configuring a Cellular Modem Interface" (Page 456).
5. Type `commit` and press **Enter** to save the changes.

11.3.2 Configuring a Cellular Modem Interface

To configure a cellular modem interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » { interface }***, where { interface } is the cellular modem interface.
3. Configure the following parameter(s) as required:

Parameter	Description
`link-alarms { link-alarms }`	**Synopsis:** [true | false] **Default:** 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.
`alias { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface

4. [Optional] Enable the interface. For more information, refer to "Enabling/ Disabling Cellular Modem Interfaces" (Page 455).
5. [Optional] Enable and configure LTE on the interface. For more information, refer to "Managing the LTE Modem" (Page 469).
6. Type `commit` and press **Enter** to save the changes.

11.3.3 Activating Dual SIM Cards

The RUGGEDCOM RX1500-series supports dual micro-SIM cards for the LTE modem to provide a fail-over mechanism should one of the SIM cards lose connectivity with the network.

To activate both micro-SIM cards, do the following:

1. Make sure both micro-SIM cards are installed. For more information, refer to the "Modules Catalog" for the RUGGEDCOM RX1500-series.
2. Configure a GSM profile for each micro-SIM card, making sure the fail-over profile for each is the other card. For more information, refer to "Adding a GSM Profile" (Page 466).
3. Configure the cellular modem interface to connect to the cellular network via the primary profile. For more information, refer to "Connecting as a PPP Client" (Page 439).

11.3.4 Viewing a List of Cellular Modem Interfaces

To view a list of cellular modem interfaces, type:

```
show running-config interface cellmodem
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface cellmodem
interface
 cellmodem lm4 1
  enabled
  no alias
  cdma ppp-client
 !
!
```

11.3.5 Viewing the Status of a Cellular Modem Interface

To view the status of a cellular modem interface, type:

```
show interfaces cellmodem cel-{ slot }-{ port } | select
state | select admin-state | select media
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

A table or list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem cel-4-1 | select state | select admin-state |
 select media
                                ADMIN
```

```
IFNAME   TYPE  STATE  MEDIA      STATE
---------------------------------------
cel-4-1  lte   down   LTE modem  up
```

The following information is displayed:

Parameter	Description
state	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] The port's link status.
media	**Synopsis:** A string up to 31 characters long The wireless data communication technology that modem is compatible with{ GSM/HSPA, CDMA/EVDO, LTE }.
admin-state	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] The port's administrative status.

11.3.6 Viewing PPP Interface Statistics

To view the statistics for the PPP interface, type:

```
show interfaces cellmodem ppp-connections
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem ppp-connections
               CONNECTION    LOCAL  REMOTE  TX     RX
IFNAME   TYPE  STATUS        IP     IP      BYTES  BYTES  MTU
-------------------------------------------------------------
cel-4-1  cdma  Disconnected                0      0      0
```

The following information is displayed:

Parameter	Description
connection-status	**Synopsis:** A string up to 128 characters long PPP connection status
local-ip	**Synopsis:** A string up to 32 characters long The IP address assigned to the modem by the remote server
remote-ip	**Synopsis:** A string up to 32 characters long The IP address of the remote server
apn	**Synopsis:** A string The name of the wireless network access point.

Parameter	Description
username	**Synopsis:** A string **Default:** N/A The user ID to connect to the remote server.
tx-bytes	**Synopsis:** An integer The bytes transmitted over the modem
rx-bytes	**Synopsis:** An integer The bytes received by the modem
mtu	**Synopsis:** An integer MTU (Maximum Transmission Unit) value on the ppp interface

11.3.7 Viewing the HSPA Network Status for Cellular Modems

To view the status of the HSPA GSM network for a cellular modem, type:

```
show interfaces cellmodem { interface } { profile } { pro
file }
```

Where:

- `{ interface }` is the slot name and port number for the cellular modem
- `{ profile }` is the profile (e.g. hspa or hspaplus)

A list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem cel-1-1 hspaplus hspaplus
hspaplus
 network supported GSM,GPRS,EDGE,UMTS,HSDPA/HSUPA,HSPA+
 imei              353567043273375
 radio             on
 rssi indicator    -61
 network operator  TELUS
 network in use    HSDPA/HSUPA
 network status    "Registered to Home network"
 sim               89122301001691886 69F
 active profile    none
 ber               99
 imsi              302220034620366
 msisdn            14373412539
 mcc               302
 mnc               220
```

This list provides the following information:

Parameter	Description
network-supported	**Synopsis:** A string up to 128 characters long Wireless technologies supported by the modem

Parameter	Description
imei	**Synopsis:** A string up to 128 characters long International Mobile Equipment Indentity
radio	**Synopsis:** A string up to 128 characters long The current RF status of cellmodem
rssi-indicator	**Synopsis:** An integer The Received Signal Strength Indicator in dBm
network-operator	**Synopsis:** A string up to 128 characters long The wireless network operator currently in use
network-in-use	**Synopsis:** A string up to 128 characters long The network technology currently in use by the modem
network-status	**Synopsis:** A string up to 128 characters long The registration status of the modem with the wireless network
sim	**Synopsis:** A string up to 128 characters long The Subscriber Indentity Module number
active-profile	**Synopsis:** A string up to 128 characters long The active profile of cellular connection
ber	**Synopsis:** A string up to 128 characters long The percentage at which errors occur in the transmission of digital data.
imsi	**Synopsis:** A string up to 128 characters long The unique identifier of a cellular network user.
msisdn	**Synopsis:** A string up to 128 characters long The identity of a mobile phone number, internationally.
mcc	**Synopsis:** A string up to 128 characters long The country to which a mobile subscriber belongs.
mnc	**Synopsis:** A string up to 128 characters long A two or three digit number used to uniquely identify a given network from within a specified country.

11.3.8 Viewing the CDMA Network Status for Cellular Modems

To view the status of the CDMA network for a cellular modem, type:

```
show interfaces cellmodem cdma
```

A list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem cdma
interfaces cellmodem cel-4-1 cdma
 cdma
  network supported "CDMA 1xRTT/EV-DO"
  esn               0x60E58148
  ecio              0
  rssi indicator    -113
  network operator  Verizon
  network in use    NO
  network status    "Modem is not activated"
  phone number      0000003576
  ber               99
  imsi              Unknown
  msisdn            ""
  mcc               Unknown
  mnc               Unknown
```

The following information is displayed:

Parameter	Description
network-supported	**Synopsis:** A string up to 128 characters long Wireless technologies supported by the modem
esn	**Synopsis:** A string up to 128 characters long The Electronic Serial Number of the modem. ESN is only avaible for the CDMA modem.
ecio	**Synopsis:** An integer The total energy per chip per power density value in dBm
rssi-indicator	**Synopsis:** An integer The Received Signal Strength Indicator in dBm
network-operator	**Synopsis:** A string up to 128 characters long The wireless network operator currently in use
network-in-use	**Synopsis:** A string up to 128 characters long The network technology currently in use by the modem
network-status	**Synopsis:** A string up to 128 characters long The registration status of the modem with the wireless network
phone-number	**Synopsis:** A string up to 128 characters long The subscriber phone number of the CDMA modem
ber	**Synopsis:** A string up to 128 characters long The percentage at which errors occur in the transmission of digital data.
imsi	**Synopsis:** A string up to 128 characters long The unique identifier of a cellular network user.

Parameter	Description
msisdn	**Synopsis:** A string up to 128 characters long The identity of a mobile phone number, internationally.
mcc	**Synopsis:** A string up to 128 characters long The country to which a mobile subscriber belongs.
mnc	**Synopsis:** A string up to 128 characters long A two or three digit number used to uniquely identify a given network from within a specified country.

11.3.9 Activating a Cellular Modem Account

Before using the cellular modem, a cellular account must be activated on a service provider's network. Once the account is activated, the modem will be able to connect to the cellular network without further intervention. There are two account activation methods used by RUGGEDCOM ROX II: OTA (Over-the-Air) and Manual.

11.3.9.1 Activating a Cellular Modem Account Over-the-Air

RUGGEDCOM ROX II supports the OTASP (Over-the-Air Service Provisioning) mechanism offered by most CDMA cellular service providers for provisioning cellular end stations for use on their networks. Using this method, the service provider (or carrier) supplies an OTASP dial string which RUGGEDCOM ROX II can use to activate the cellular account. During this OTASP call, the carrier authorizes and configures the modem for use on its network.

Note

The service provider may issue a second OTASP dial string for accessing the cellular network if a string other than the default is required. This string must be configured when adding a CDMA profile for the cellular modem interface. For more information about adding a CDMA profile, refer to "Adding a CDMA Profile" (Page 464).

Note

A typical OTASP dial string begins with **228*.

To configure the OTASP dial string, type:

1. Make sure the CLI is in Configuration mode.
2. Configure the activation data string by typing:

```
interfaces cellmodem { slot } { port } { profile } activa
tion activation-dial-string { string }
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ profile }` is the profile configured for the module
- `{ string }` is the activation data string

3. Type `commit` and press **Enter** to save the changes.

11.3.9.2 Activating a Cellular Modem Account Manually

If the service provider does not support Over the Air Service Provisioning (OTASP), the account must be activated manually.

To manually activate a cellular modem account, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interfaces » cellmodem » { slot/port/profile } » activation***, where { slot/port/profile } is the slot name, port number and profile configured for the cellular modem.
3. Configure the following parameter(s) as required:

Parameter	Description
`activation-code`	**Synopsis:** A string up to 128 characters long The Master Subsidy Lock code provided by the wireless service carrier
`phone-number`	**Synopsis:** A string up to 32 characters long The Mobile Directory Number provided by the wireless service carrier
`mobile-id-number`	**Synopsis:** A string up to 32 characters long The Mobile Indentification Number provided by the wireless service carrier
`system-id`	**Synopsis:** A string up to 32 characters long System Identification Number provided by wireless service carrier
`network-id`	**Synopsis:** A string up to 32 characters long The Wireless Network ID provided by the wireless service carrier

4. Type `commit` and press **Enter** to save the changes.

11.4 Running AT Commands

To issue AT (Hayes) commands to the cellular modem, type:

```
interfaces cellmodem { interface } { profile } at command
{ command }
```

Where:

- `{ interface }` is the cellular modem interface
- `{ profile }` is the cellular profile
- `{ command }` is the AT command

11.5 Managing Cellular Modem Profiles

The following describes how to configure cellular modem profiles.

11.5.1 Managing CDMA Profiles

CDMA (Code Division Multiple Access) profiles must be configured before 3G EVDO CDMA data is available. For more information about viewing 3G EVDO CDMA data, refer to "Viewing the CDMA Network Status for Cellular Modems" (Page 460).

11.5.1.1 Viewing a List of CDMA Profiles

To view a list of CDMA profiles, type:

```
show running-config global cellular profiles cdma
```

If profiles have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config global cellular profiles cdma | tab
                  USE                        DIAL    DISCONNECT  FAILOVER
           DIAL   PEER                       ON      IDLE        ON
NAME       STRING DNS   USERNAME  PASSWORD  DEMAND  TIMEOUT     DEMAND    MTU
-------------------------------------------------------------------------------
gsm-cdma   #777   -     N/A       N/A       -       0           -         1500

!
```

If no CDMA profiles have been configured, add profiles as needed. For more information, refer to "Adding a CDMA Profile" (Page 464).

11.5.1.2 Adding a CDMA Profile

To add a CDMA profile for the cellular modem interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the restriction by typing:

   ```
   global cellular profiles cdma { name }
   ```

   Where:

   - `{ name }` is the name of the profile

3. Configure the cellular network by typing the following commands:

Parameter	Description
`dial-string { dial-string }`	**Synopsis:** A string up to 32 characters long **Default:** #777 The dial string to connect to the wireless provider.

4. Configure the CDMA PPP settings by typing the following commands:

Parameter	Description
`use-peer-dns`	Enables the DNS server entries that the PPP server recommends. Enables this option unless you provide your own name servers.
`username { username }`	**Synopsis:** A string **Default:** N/A The user ID to connect to the remote server.
`password { password }`	**Synopsis:** A string The password to be authenticated by the remote server. Must not begin with 4.
`dial-on-demand`	Activates dial-on-demand for this connection. The establishment of the PPP connection is postponed until there is data to be transmitted via the interface. If dial-on-demand is configured, Failover on Demand cannot be configured.
`disconnect-idle-timeout { disconnect-idle-timeout }`	**Synopsis:** An integer **Default:** 0 The time in seconds to wait before disconnecting PPP when there is no traffic on the link. This option is only valid when dial-on-demand is enabled.
`failover-on-demand`	Activates link failover on-demand on this device. PPP link establishment on this device is controlled by link failover. If Failover on Demand is configured, Dial on Demand cannot be configured.
`mtu { mtu }`	**Synopsis:** An integer between 128 and 1500 **Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP interface.

5. Type `commit` and press **Enter** to save the changes.

11.5.1.3 Deleting a CDMA Profile

To delete a CDMA Profile, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen key by typing:

   ```
   no global cellular profiles cdma { name }
   ```

   Where:

   - `{ name }` is the name of the profile
3. Type `commit` and press **Enter** to save the changes.

11.5.2 Managing GSM Profiles

GSM (Global System for Mobile Communications) profiles must be configured before HSPA data is available. For more information about viewing the status of the HSPA networks, refer to "Viewing the HSPA Network Status for Cellular Modems" (Page 459).

11.5.2.1 Viewing a List of GSM Profiles

To view a list of GSM profiles, type:

```
show running-config global cellular profiles gsm
```

If profiles have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config global cellular profiles gsm | tab
                                              USE                        DIAL    DISCONNECT
 FAILOVER
                     APN   DIAL                    PEER                       ON      IDLE        ON
NAME  APN           TYPE  STRING    SIM  PROFILE  DNS   USERNAME  PASSWORD  DEMAND  TIMEOUT     DE
MAND    MTU
-------------------------------------------------------------------------------------------
gsm1  apn.gsm1.net  ipv4  *99***1#  1    -        -     N/A       N/A       -       0           -
     1500

!
```

If no GSM profiles have been configured, add profiles as needed. For more information, refer to "Adding a GSM Profile" (Page 466).

11.5.2.2 Adding a GSM Profile

To add a GSM profile for the cellular modem interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the restriction by typing:

   ```
   global cellular profiles gsm { name }
   ```

   Where:

   - `{ name }` is the name of the profile

3. Configure the cellular network by typing the following commands:

   Note

   The Access Point Name (APN) is necessary only on GPRS networks (Edge or HSPA). It is the name of the cellular network access point that provides a gateway to the Internet. This information is provided by the wireless network when a data service account is registered.

   Each APN is specific to the location where the modem will operate. A new APN is required if the modem is moved to another location.

   Note

   The dial string is a special command to be sent by the cellular modem to the cellular network to establish a data connection. For example, a typical dial string for GSM/GPRS networks is **99***1#*. This command will depend on the wireless network. Contact the service provided for the correct dial string command for data service. A regular telephone number is usually not required to connect to a GSM/GPRS network.

Parameter	Description
`apn { apn }`	**Synopsis:** A string **Default:** none The name of the wireless network access point.
`apn-type { apn-type }`	**Synopsis:** [ipv4 | ipv6 | ipv4v6] **Default:** ipv4 Specify APN type used to attach to PDN
`dial-string { dial-string }`	**Synopsis:** A string **Default:** *99***1# The dial string given by the wireless provider to connect to the access point name.
`sim { sim }`	**Synopsis:** An integer between 1 and 2 **Default:** 1 Specify SIM index to be used by this profile
`peer { peer }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The peer address to override the one from carrier.

4. Select the failover profile to use by typing the following command:

Parameter	Description
`profile { profile }`	**Synopsis:** A string up to 32 characters long Specify the cellular connection profile

5. Configure the GSM PPP settings by typing the following commands:

Parameter	Description
`use-peer-dns`	Enables the DNS server entries that the PPP server recommends. Enables this option unless you provide your own name servers.
`username { username }`	**Synopsis:** A string **Default:** N/A The user ID to connect to the remote server.
`password { password }`	**Synopsis:** A string The password to be authenticated by the remote server. Must not begin with 4.
`dial-on-demand`	Activates dial-on-demand for this connection. The establishment of the PPP connection is postponed until there is data to be transmitted via the interface. If dial-on-demand is configured, Failover on Demand cannot be configured.
`disconnect-idle-timeout { disconnect-idle-timeout }`	**Synopsis:** An integer **Default:** 0 The time in seconds to wait before disconnecting PPP when there is no traffic on the link. This option is only valid when dial-on-demand is enabled.
`failover-on-demand`	Activates link failover on-demand on this device. PPP link establishment on this device is controlled by link failover. If Failover on Demand is configured, Dial on Demand cannot be configured.
`mtu { mtu }`	**Synopsis:** An integer between 128 and 1500 **Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP interface.
`authentication { authentication }`	**Synopsis:** [none | chap | pap] **Default:** none The authentication protocol used to establish a cellular data link

6. Type `commit` and press **Enter** to save the changes.

11.5.2.3 Deleting a GSM Profile

To delete a GSM Profile, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the chosen key by typing:

   ```
   no global cellular profiles gsm { name }
   ```

   Where:

   - `{ name }` is the name of the profile

3. Type `commit` and press **Enter** to save the changes.

11.6 Managing the LTE Modem

This section describes how to manage the LTE modem.

11.6.1 Viewing LTE Cellular Modem Information

To view information about an LTE cellular modem, type the following:

```
show interfaces cellmodem { interface } lte
```

A list similar to the following appears:

```
interfaces cellmodem cel-4-1 lte
 state       down
 media       "LTE modem"
 admin state up
 lte
  network supported "UMTS, LTE"
  imei              354328090290500
  radio             on
  rssi indicator    -59
  network operator  TELUS
  network in use    "E-UTRAN (LTE)"
  network status    "Registered to Home network"
  sim               8912230100169188669(Sim1)
  active profile    none
  ber               4
  imsi              302220034620366
  msisdn            14373412539
  mcc               302
  mnc               220
  gps
   mode standalone
```

The following information is displayed:

Parameter	Description
`network-supported`	**Synopsis:** A string up to 128 characters long Wireless technologies supported by the modem
`imei`	**Synopsis:** A string up to 128 characters long International Mobile Equipment Indentity

Parameter	Description
radio	**Synopsis:** A string up to 128 characters long The current RF status of cellmodem
rssi-indicator	**Synopsis:** An integer The Received Signal Strength Indicator in dBm
network-operator	**Synopsis:** A string up to 128 characters long The wireless network operator currently in use
network-in-use	**Synopsis:** A string up to 128 characters long The network technology currently in use by the modem
network-status	**Synopsis:** A string up to 128 characters long The registration status of the modem with the wireless network
sim	**Synopsis:** A string up to 128 characters long The Subscriber Indentity Module number
active-profile	**Synopsis:** A string up to 128 characters long The active profile of cellular connection
ber	**Synopsis:** A string up to 128 characters long The percentage at which errors occur in the transmission of digital data.
imsi	**Synopsis:** A string up to 128 characters long The unique identifier of a cellular network user.
msisdn	**Synopsis:** A string up to 128 characters long The identity of a mobile phone number, internationally.
mcc	**Synopsis:** A string up to 128 characters long The country to which a mobile subscriber belongs.
mnc	**Synopsis:** A string up to 128 characters long A two or three digit number used to uniquely identify a given network from within a specified country.

11.6.2 Configuring an LTE Modem

To configure an LTE modem, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable the LTE modem. For more information, refer to "Enabling/Disabling the LTE Modem" (Page 472).

3. Navigate to ***interface » cellmodem » { interface } » lte*** , where { interface } is the slot name and port number of the cellular modem port.
4. Configure the following parameter(s) as required:

Note

For more information about enabling or disabling a hard reset of the LTE modem, refer to "Enabling/Disabling a Hard Reset" (Page 474).

Parameter	Description
`failure-recovery-mode { failure-recovery-mode }`	**Synopsis:** [sim-failover | cellular-reset] **Default:** sim-failover The cellular failure recovery mode to be invoked when a cellular network error is detected. • sim-failover: The cellular modem will failover to the secondary SIM card. • cellular-reset: The existing cellular modem connection will be reset by resetting the cellular modem.
`max-try { max-try }`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 Specify the maximum number of SIM card failover retries. 0 means re-try forever
`force-hard-reset { force-hard-reset }`	**Synopsis:** [true | false] **Default:** false Perform a hard reset on the celluar modem when all soft reset attempts have been exhausted. A hard reset will perform a power cycle on the cellular modem.
`soft-reset-attempts { soft-reset-attempts }`	**Synopsis:** An integer between 0 and 65535 **Default:** 5 The number of soft resets to attempt before performing a hard reset.
`failure-detect-mode { failure-detect-mode }`	**Synopsis:** [cellular-failure | ip-polling] **Default:** cellular-failure The cellular failure detection mode to determine when a cellular network error exists. • cellular-failure: Detect cell modem (signal loss), SIM card or cellular Access Point faults. • ip-polling: Use pings to poll a remote host to test connectivity.
`failover-timer { failover-timer }`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The time in minutes before initiating SIM card failover.

Parameter	Description
`ipv4-address { ipv4-address }`	**Synopsis:** A string between 7 and 15 characters long The IPv4 address used for sending pings to test connectivity.
`ip-polling-interval { ip-polling-interval }`	**Synopsis:** An integer between 5 and 65535 **Default:** 60 The time in seconds between each ping message sent to the remote host.
`ip-polling-resp-timeout { ip-polling-resp-timeout }`	**Synopsis:** An integer between 1 and 65535 **Default:** 3 The time in seconds to wait for a response from the IP ping poll request.
`ip-polling-retry-delay { ip-polling-retry-delay }`	**Synopsis:** An integer between 15 and 65535 **Default:** 15 The time in seconds to wait before issuing a ping retry to a remote host address.
`max-ip-poll-failures { max-ip-poll-failures }`	**Synopsis:** An integer between 1 and 65535 **Default:** 3 The number of allowed IP polling response failures before initiating SIM failover.
`ip-polling-startup-delay { ip-polling-startup-delay }`	**Synopsis:** An integer between 1 and 65535 **Default:** 3 The time in seconds to wait after system startup before issuing IP ping polls.

5. Type `commit` and press **Enter** to save the changes
6. [Optional] Enable GPS. For more information, refer to "Enabling/Disabling GPS" (Page 474).

11.6.3 Enabling/Disabling the LTE Modem

To enable or disable the LTE modem for a cellular modem interface, do the following:

Note

The operational state of the LTE modem is determined by the associated cellular modem interface. For more information about enabling or disabling the cellular modem interface, refer to "Enabling/Disabling Cellular Modem Interfaces" (Page 455).

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the LTE modem by typing:

   Enable

```
interface cellmodem { slot } { port } enabled
```

Where:

- `{ slot }` is the name of the module location.
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.

Disable

```
no interface cellmodem { slot } { port } enabled
```

Where:

- `{ slot }` is the name of the module location.
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module.

3. Type `commit` and press **Enter** to save the changes.

11.6.4 Resetting the Cellular Modem

When a cellular connection failure is detected, RUGGEDCOM ROX II automatically performs a soft reset of the cellular modem to recover the connection. A manual soft reset option is also available, as well as a hard reset in cases where a soft reset fails to restore connectivity.

This section describes how to manually reset the modem and how to enable and disable an automatic hard reset.

11.6.4.1 Performing a Manual Soft Reset

During a soft reset, the cellular modem driver sends AT (Hayes) commands to the cellular modem to re-initialize itself. Power to the cellular modem is maintained throughout the process.

To manually soft-reset the cellular modem, type:

Note

A soft reset requires approximately 30 seconds, during which the cellular link will be terminated.

```
interfaces cellmodem { slot } { port } lte reset
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

11.6.4.2 Enabling/Disabling a Hard Reset

RUGGEDCOM ROX II allows users to configure an automatic hard reset of the cellular modem when a connection fails in cases where a soft reset does not restore cellular connectivity. Both cellular failure and IP polling failure detection methods are supported.

Users can configure the number of soft resets to be attempted before performing a hard reset.

During a hard reset, the cellular modem is powered down and powered back up again. The cellular modem is then re-initialized.

To enable or disable a hard reset of the cellular modem, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable the LTE modem. For more information, refer to "Enabling/Disabling the LTE Modem" (Page 472).
3. Navigate to ***interface » cellmodem » { interface } » lte*** , where { interface } is the slot name and port number of the cellular modem port.
4. Enable or disable a hard reset by typing:

   Enable

   ```
   interface cellmodem { slot } { port } lte force-hard-reset
   ```

   Disable

   ```
   no cellmodem { slot } { port } lte force-hard-reset
   ```

5. Configure the number of soft reset attempts by typing:

   ```
   interface cellmodem { slot } { port } lte soft-reset-at
   tempts { integer }
   ```

   Where { integer } is the desired number of soft resets that should be attempted before the hard reset is performed. The number can be between 0 and 65535, with 0 meaning that no soft reset attempts will be made.

   The default value is 5.

6. Configure the related LTE modem parameters as desired. For more information, refer to "Configuring an LTE Modem" (Page 470)
7. Type `commit` and press **Enter** to save the changes.

11.6.5 Enabling/Disabling GPS

When GPS is enabled, users can look up the current location of the device. If configured, RUGGEDCOM ROX II can also send an NMEA GPS data streams via TCP to a server that hosts a GPS application.

To enable or disable GPS on the cellular modem, do the following:

1. Make sure the CLI is in Configuration mode.

2. Enable or disable GPS by typing:

   Enabling GPS

   ```
   interface cellmodem celport { slot } { port } lte gps en
   abled
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

   Disabling GPS

   ```
   no interface cellmodem celport { slot } { port } lte gps
   enabled
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. [Optional] Enable or disable NMEA GPS data streams. For more information, refer to "Enabling and Configuring GPS NMEA Data Streams" (Page 475).
4. Type `commit` and press **Enter** to save the changes

11.6.6 Viewing the Configured GPS Mode

To view the configured GPS mode for the interface, type the following:

```
show interfaces cellmodem lte gps
```

A list similar to the following appears:

```
IFNAME   TYPE  MODE
--------------------------
cel-4-1  lte   standalone
```

The following information is displayed:

Parameter	Description
`mode`	**Synopsis:** A string up to 64 characters long Shows configured GPS mode

11.6.7 Enabling and Configuring GPS NMEA Data Streams

When GPS and NMEA are enabled, RUGGEDCOM ROX II can receive NMEA data from the cellular modem and relay it to a remote host upon request. This feature can be enabled or disabled independent of the LTE modem configuration.

To enable and configure GPS NMEA data streams, do the following:

1. Make sure the CLI is in Configuration mode.
2. Type the following:

   ```
   interface cellmodem { interface } lte gps nmea
   ```

   Where:

   - `{ interface }` is the cellular modem interface
3. Configure the following parameters as required:

Parameter	Description
`enabled`	Enables NMEA stream
`listen-ip { listen-ip }`	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address that device will listen on for remote host request
`local-port { local-port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 10110 The port that device will listen on for remote host request
`extra-ip-ports { extra-ip-ports }`	**Synopsis:** A string The device will also listen on these IP Addresses. For port values, add ':#' to set the 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.
`max-sessions { max-sessions }`	**Synopsis:** An integer between 1 and 32 **Default:** 10 The maximum number of concurrent tcp/ip sessions.

4. Type `commit` and press **Enter** to save the changes.

11.6.8 Managing Firmware Updates

Firmware for the LTE modem can be upgraded either directly via USB flash drive or wirelessly via a remote HTTP/HTTPS server.

Note

The SIM card must be installed during the firmware update.

During wireless upgrades, RUGGEDCOM ROX II initiates the connection to the remote server, then pulls and updates the firmware. Firmware can be updated either on-demand or automatically, as defined by the user.

RUGGEDCOM ROX II performs the following actions when updating the firmware:

1. Connects to the USB flash drive or remote server and verifies the firmware version
2. Downloads the new firmware
3. Validates the new firmware to make sure it is valid for the modem
4. Flashes the new firmware to the modem
5. Logs all firmware update events and actions to the system log (Syslog)
6. Brings the modem back to normal operation

11.6.8.1 Viewing the Firmware Update Status

To view the status of the firmware update, type:

```
show interfaces cellmodem { interface } firmware-update
```

Where:

- `{ interface }` is the cellular modem interface

This table displays the following information:

Parameter	Description
`current-version`	**Synopsis:** A string up to 64 characters long The current firmware revision
`status-message`	**Synopsis:** A string up to 128 characters long Additional details on the status of the update.
`last-update-attempt`	**Synopsis:** A string up to 64 characters long The date and time of the completion of the last update attempt.
`last-update-result`	**Synopsis:** [N/A | Successful | Failed] Indicates whether or not the last firmware update was completed successfully

11.6.8.2 Configuring the Firmware Update Mode and Source

The method in which RUGGEDCOM ROX II discovers and downloads firmware updates is user configurable. The source can also be configured to point to a remote upgrade server or a local USB flash drive.

To upgrade the firmware update mode and source, do the following:

1. If the firmware will be distributed via a remote upgrade server, make sure the upgrade server is configured and the latest firmware version has been added. For more information, refer to "Managing Upgrade Servers" (Page 110).

2. Make sure a cellular modem interface is enabled. For more information, refer to "Configuring a Cellular Modem Interface" (Page 456).
3. Make sure the CLI is in Configuration mode.
4. Navigate to ***interface » wan » { interface } » lte » firmware-upgrade***, where { interface } is the cellular modem interface.
5. Configure the following parameter(s) as required:

Parameter	Description
`repository-url { repository-url }`	**Synopsis:** A string up to 256 characters long The URL of the firmware to download. Supported URIs are HTTP, HTTPS, USB and SD. To update 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 the storage medium and either navigate "chassis", "storage", "removable" (Web UI) or type "show chassis". For all other protocols, the format is "protocol://host:port/path-to-file". When using the default port for the protocol, omit ":port".
`username { username }`	**Synopsis:** A string up to 64 characters long The user name required to connect with the upgrade server.
`password { password }`	**Synopsis:** A string up to 1024 characters long The password associated with the username
`mode { mode }`	**Synopsis:** [manual-check-and-update | auto-check-manual-update | auto-check-and-update] **Default:** manual-check-and-update The update mode. Options include: * manual-check-and-update - FOTA checks and installs the firmware when initiated by the user * auto-check-manual-update - FOTA checks for new firmware automatically and installs updates when initiated by the user * auto-check-and-update - FOTA checks for and installs new firmware automatically
`interval { interval }`	**Synopsis:** An integer between 1 and 365 **Default:** 90 The number of days to wait before automatically checking for new firmware.

6. Type `commit` and press **Enter** to save the changes.

11.6.8.3 Launching a Firmware Update

To launch a firmware update, do the following:

⚠ NOTICE

Before launching a firmware upgrade, note the following:

- An active cellular connection is not required during the firmware update.
- If power is interrupted during the upgrade, the device will become unrecoverable. If this occurs, contact Siemens Customer Support.
- Changes to the LTE modem configuration are not permitted until the upgrade is complete.
- If the upgrade fails, refer to "Firmware Updates" (Page 972).

1. Make sure the firmware update mode has been configured. For more information, refer to "Configuring the Firmware Update Mode and Source" (Page 477).
2. Make sure the firmware file is available to the device.
   - If using a USB flash drive, insert the drive in the device. For more information, refer to the "Installation Manual" for the RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536.
   - If using a remote upgrade server, make sure the firmware has been added to the upgrade server. For more information about configuring an upgrade server, refer to "Configuring the Upgrade Server" (Page 111).
3. Make sure the cellular modem interface is enabled. For more information, refer to "Enabling/Disabling Cellular Modem Interfaces" (Page 455).
4. Launch the firmware update by typing:

   ```
   interfaces cellmodem { interface } firmware-update launch-update
   ```

   Where:

   - { interface } is the cellular modem interface.
5. [Optional] Verify the firmware update. For more information, refer to "Viewing the Firmware Update Status" (Page 477).
6. Reset the cellular modem. For more information, refer to "Resetting the Cellular Modem" (Page 473).
7. [Optional] Verify the firmware version installed after the operation is complete.

   If a RUGGEDCOM W41, W51, W61, or W91 module is installed, run the following AT command:

   ```
   at#swpkgv
   ```

   If a RUGGEDCOM W71 module is installed, run the following AT command:

```
at#firmware
```

For more information, refer to "Running AT Commands" (Page 463).

11.7 Managing PPPoE

The Point-to-Point over Ethernet (PPPoE) is a network protocol that encapsulates Point-to-Point (PPP) protocol frames within Ethernet frames. It allows multiple hosts on the same network to connect to the WAN via a services router (or client), which connects to an access concentrator (or server) via Ethernet.

PPPoE combines Ethernet and PPP protocols to provide a method for authenticating, encrypting, and compressing PPPoE traffic sent by hosts before it is forwarded by the client.

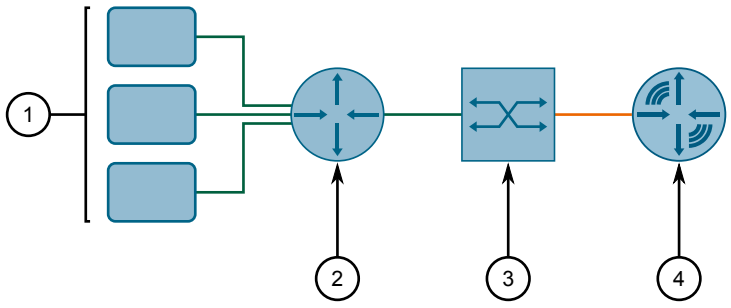
⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

PPPoE communications use protocols that are susceptible to known security issues. Make sure all underlying protocols use strong authentication/encryption to provide security and, where possible, make sure to only use PPPoE in a secure network environment.

11.7.1 Understanding PPPoE

RUGGEDCOM ROX II devices can be configured to act as a services router (or client) for other hosts on the network. The client is connected to a modem that has a Digital Subscriber Line (DSL) connection to an ISP's access concentrator (or server). Upon successfully authenticating the PPPoE connection, the ISP grants access to either MPLS or Internet services.



① Hosts
② PPPoE Client (Services Router)
③ DSL Modem
④ PPPoE Server (Access Concentrator)

Figure 11.1 PPPoE Network

PPPoE Stages

When initialized, PPPoE establishes a connection between the client and server in two stages:

- **Discovery Stage**
  The client finds an available server and establishes a session ID by doing the following:
  - The client broadcasts a PPPoE Active Discovery Initiation (PADI) packet requesting a service.
  - Server's on the LAN that can provide the service reply with a PPPoE Active Discovery Offer (PADO) packet. The PADO includes the server's name, the unicast address of the client, and the service that was requested.
  - Based on the PADO's received, the client selects a server and sends it a PPPoE Active Discovery Request (PADR).
  - The server returns a PPPoE Active Discovery Session-Confirmation (PADS) packet. The packet will include a session ID if the session request is accepted. Otherwise, the packet will include a service name error.
- **Session Stage**
  The server authenticates the client and then negotiates a PPP connection using information collected in the discovery stage.

Once the connection is created an a session is established, all PPPoE packets are encapsulated in the PPPoE and PPP headers.

Authentication Modes

RUGGEDCOM ROX II supports the following authentication modes:

- **PAP** – Password Authentication Protocol
- **CHAP** – Challenge Handshake Authentication Protocol
- **MS-CHAP** – Microsoft Challenge Handshake Authentication Protocol Version 1
- **MS-CHAP2** – Microsoft Challenge Handshake Authentication Protocol Version 2

11.7.2 Managing PPPoE Profiles

A PPPoE profile defines the characteristics of a PPPoE session. This includes defining the maximum packet size, the authentication mode, credentials, and more.

Each PPPoE interface must be mapped to a PPPoE profile.

Multiple PPPoE profiles can be defined, allowing for a variety of different configurations. One such profile could be created to act as a default profile.

11.7.2.1 Viewing a List of PPPoE Profiles

To view a list of PPPoE profiles, type:

```
show running-config global pppoe profiles
```

If profiles have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config global pppoe profiles | tab
                          USE             LCP
                  DEFAULT  PEER  LCP ECHO  ECHO     AUTH
NAME        MTU   ROUTE    DNS   INTERVAL  FAILURE  MODE  USERNAME                PASSWORD
-------------------------------------------------------------------------------------------
pppoe-serv  1452  true     true  4         2        pap   3390006311@company.com  $4$oe5WCLM68FR
whYYI0d4IDw==

!
```

If no PPPoE profiles have been configured, add profiles as needed. For more information, refer to "Adding PPPoE Profile" (Page 482).

11.7.2.2 Adding PPPoE Profile

To add a PPPoE profile, do the following:

1. Obtain a username and password from the ISP for the PPPoE service.
2. Make sure the CLI is in Configuration mode.
3. Create the PPPoE profile by typing:

   ```
   global pppoe profiles { profile }
   ```

   Where:

   - { profile } is the name of the profile
4. Configure the following parameters as required:

Parameter	Description
`mtu { mtu }`	**Synopsis:** An integer between 16 and 1492 **Default:** 1452 The MTU value for the PPPoE interface.
`default-route { default-route }`	**Synopsis:** [true | false] **Default:** false Enables the default route using this interface whenever it connects.
`use-peer-dns { use-peer-dns }`	**Synopsis:** [true | false] **Default:** false Enables the DNS server entries that the PPPoE server recommends. Enables this option unless you provide your own name servers.

Parameter	Description
`lcp-echo-interval { lcp-echo-interval }`	**Synopsis:** An integer **Default:** 4 The interval in seconds to send an LCP echo-request frame.
`lcp-echo-failure { lcp-echo-failure }`	**Synopsis:** An integer **Default:** 2 The number of times LCP echo-requests are sent without a valid response. If the number of failures are exceeded, the PPPoE connection will be terminated.
`auth-mode { auth-mode }`	**Synopsis:** [pap | chap | ms-chap | ms-chapv2] **Default:** ms-chapv2 The authentication method used for the PPPoE connection.
`username { username }`	**Synopsis:** A string **Default:** N/A The user ID to connect to the remote server.
`password { password }`	**Synopsis:** A string up to 255 characters long The password to be authenticated by the remote server.

5. Type `commit` and press **Enter** to save the changes.

11.7.2.3 Deleting a PPPoE Profile

To delete a PPPoE profile, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen key by typing:

   ```
   no global pppoe profiles { name }
   ```

   Where:

   - `{ name }` is the name of the profile
3. Type `commit` and press **Enter** to save the changes.

11.7.3 Managing PPPoE Interfaces

PPPoE interfaces are created automatically whenever PPPoE is enabled for a routable Ethernet port. The interface is created under ***interfaces » pppoe*** and given a name based on the associated Ethernet port. For example, the interface pppoe-1-1 is associated with port lm1/1.

A maximum of four PPPoE interfaces are supported.

Note

PPPoE interfaces can only be established on switched Ethernet ports that are not in switchport mode. For more information, refer to "Configuring a Switched Ethernet Port" (Page 335).

11.7.3.1 Configuring a PPPoE Interface

To configure a PPPoE interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Create the PPPoE interface by typing:

   ```
   interface switch { slot } { port } pppoe profile { pro
   file } enabled
   ```

   Where:

   - { slot } is the name of the module location
   - { port } is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - { profile } is the PPPoE profile
3. Type `commit` and press **Enter** to save the changes.

11.7.3.2 Viewing PPPoE Statistics

To view statistics collected for each PPPoE interface, type:

```
show interfaces pppoe
```

```
ruggedcom# show interfaces pppoe
           CONNECTION
IFNAME     STATUS      LOCAL IP        REMOTE IP     TXBYTES  RXBYTES
-------------------------------------------------------------------------
pppoe-4-2  up          198.251.59.210  198.251.52.3  960      884
```

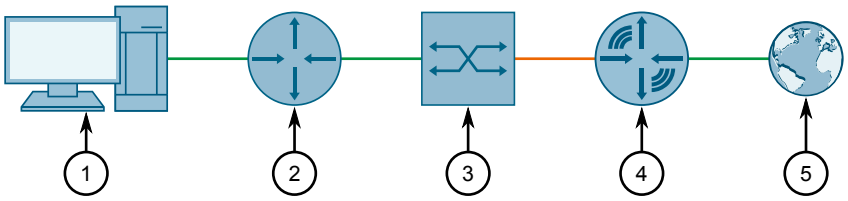
The following information is displayed:

Parameter	Description
`{ ifname }`	**Synopsis:** A string between 1 and 15 characters long The name of the PPP over Ethernet interface.
`connection-status`	**Synopsis:** [up | down] The status of the connection. Possible values include: • **up** – the PPPoE interface is up and ready to forward packets • **down** – the PPPoE interface is down

Parameter	Description
`localIp`	**Synopsis:** A string The local IP address assigned by the remote server.
`remoteIp`	**Synopsis:** A string The IP address of the remote server.
`txbytes`	**Synopsis:** An integer The bytes transmitted over the PPPoE link.
`rxbytes`	**Synopsis:** An integer The bytes received over the PPPoE link.

11.7.4 Example: Configuring a PPPoE Connection with an ISP

The following demonstrates how to establish a PPPoE connection with an ISP and provide Internet access to a host.



① Host
② PPPoE Client (Services Router)
③ DSL Modem
④ PPPoE Server (Access Concentrator)
⑤ Internet

Figure 11.2 PPPoE Connection with an ISP

To configure the device, do the following:

1. Add a PPPoE profile with the following settings:

default-route	true
use-peer-dns	true
auth-mode	{ Determined by ISP }
username	{ Provided by ISP }
password	{ Provided by ISP }

   For more information about adding a PPPoE profile, refer to "Adding PPPoE Profile" (Page 482).

2. Enable internal VLANs. For more information, refer to "Configuring the Internal VLAN Range" (Page 382).

3. Commit the changes.
4. Configure a switched Ethernet port as a PPPoE interface. The port must be enabled and not in switchport mode. For more information, refer to "Configuring a PPPoE Interface" (Page 484).
5. Commit the changes.
6. Verify the PPPoE connection over the PPPoE interface. For more information, refer to "Viewing PPPoE Statistics" (Page 484).
7. Since the PPPoE profile was configured to use the default route, verify the default route is installed. For more information, refer to "Viewing the Status of IPv4 Routes" (Page 581).
8. Ping a public IP address to verify access to the Internet. For more information, refer to "Using Network Utilities" (Page 26).
9. Send/receive traffic over the PPPoE connection and then verify the number of bytes sent (TX) and received (RX). For more information, refer to "Viewing PPPoE Statistics" (Page 484).
10. Assign a static IPv4 address to a switched Ethernet port other than the one configured as the PPPoE interface.

    If the port is in switchport mode, the IPv4 address must be assigned to the VLAN interface (e.g. switch.0001). Otherwise, the IPv4 address is assigned to the routing interface (e.g. fe-1-1).

    For more information, refer to "Adding an IPv4 Address" (Page 269).
11. Ping the local host to verify the connection. For more information, refer to "Using Network Utilities" (Page 26).
12. [Optional] Configure and enable a 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. The firewall should also enable NAT masquerading. For more information, refer to "Managing Firewalls" (Page 235).
13. Commit the changes.
14. Ping the device from the local host to the public Internet address, and verify the traffic received on the PPPoE interface using Tcpdump. For more information, refer to "Using Network Utilities" (Page 26).

12 Tunneling and VPNs

This chapter describes how to configure various tunnels and Virtual Private Networks (VPNs).

12.1 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 HLDC-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 245).

12.1.1 Viewing a List of Virtual Switches

To view a list of virtual switches, type:

```
show running-config interface virtualswitch
```

If virtual switches have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface virtualswitch
interface
 virtualswitch vs1
  retain-ip
  no alias
  no proxyarp
  interface fe-cm-1
  !
 !
!
```

If no virtual switches have been configured, add virtual switches as needed. For more information, refer to "Adding a Virtual Switch" (Page 489).

12.1.2 Adding a Virtual Switch

To add a virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the virtual switch by typing:

   ```
   interface virtualswitch { name }
   ```

   Where:

   - `{ name }` is the name assigned to the virtual switch
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables this interface.
`retain-ip { retain-ip }`	**Synopsis:** [true | false] **Default:** false Retain IP on bridge device.
`forward-delay { forward-delay }`	**Synopsis:** An integer **Default:** 15 Delay (in seconds) of the listening and learning state before goes to forwarding state.
`alias { alias }`	**Synopsis:** A string up to 64 characters long The SNMP alias name of the interface
`ip-address-src { ip-address-src }`	**Synopsis:** [static | dynamic] **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
`ipv6-address-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** static Whether the IPv6 address is static or dynamically assigned via DHCPv6.
`proxyarp`	Enables/Disables whether the port will respond to ARP requests for hosts other than itself

4. Add one or more interfaces for the virtual switch. For more information, refer to "Adding a Virtual Switch Interface" (Page 491).
5. [Optional] **ip-address-src** or **ipv6-address-src** 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 269) or "Adding an IPv6 Address" (Page 270).

6. [Optional] Assign one or more VLANs to the virtual switch. For more information, refer to "Adding a Virtual Switch VLAN" (Page 499).
7. Type `commit` and press **Enter** to save the changes.

12.1.3 Deleting a Virtual Switch

To delete a virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen virtual switch by typing:

   ```
   no interface virtualswitch { name }
   ```

   Where:

   - `{ name }` is the name assigned to the virtual switch
3. Type `commit` and press **Enter** to save the changes.

12.1.4 Managing Virtual Switch Interfaces

This section describes how to configure and manage interfaces for virtual switches.

12.1.4.1 Viewing a List of Virtual Switch Interfaces

To view a list of virtual switch interfaces, type:

```
show running-config interface virtualswitch { name } inter
face
```

Where:

- `{ name }` is the name assigned to the virtual switch

If virtual switch interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface virtualswitch vs1 interface | tab
NAME
-----------------
switch.0100
te1-4-1c01.0100

 !
!
```

If no virtual switch interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Virtual Switch Interface" (Page 491).

12.1.4.2 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 the 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. Make sure the CLI is in Configuration mode.
2. Add an interface to the virtual switch by typing:

   ```
   interface virtualswitch { name } interface { interface }
   ```

   Where:

   - `{ name }` is the name assigned to the virtual switch
   - `{ interface }` is the name assigned to the interface

   The new interface is now accessible by typing:

   ```
   ip vsw-{ name }
   ```

   The new virtual switch is now visible under the **ip** menu with the prefix *vsw-* (i.e. vsw-vs1, vsw-vs2, etc.).
3. Assign an IPv4 or IPv6 address to the interface. For more information, refer to "Adding an IPv4 Address" (Page 269) or "Adding an IPv6 Address" (Page 270).
4. If necessary, add one or more VLANs to the virtual switch interface. For more information, refer to "Adding a Virtual Switch VLAN" (Page 499).
5. Type `commit` and press **Enter** to save the changes.

12.1.4.3 Deleting a Virtual Switch Interface

To delete a virtual switch interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen virtual switch interface by typing:

   ```
   no interface virtualswitch { name } interface { inter
   face }
   ```

Where:

- `{ name }` is the name assigned to the virtual switch
- `{ interface }` is the name assigned to the interface

3. Type `commit` and press **Enter** to save the changes.

12.1.5 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.

12.1.5.1 Enabling/Disabling Virtual Switch Filtering

To enable or disable virtual switch filtering, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable virtual switch filtering by typing:

   Enabling Virtual Switch Filtering

   ```
   security virtualswitch-filter enabled
   ```

   Disabling Virtual Switch Filtering

   ```
   no security virtualswitch-filter enabled
   ```

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 489).

4. Type `commit` and press **Enter** to save the changes.

12.1.5.2 Viewing a List of Virtual Switch Filters

To view a list of virtual switch filters, type:

```
show running-config security virtualswitch-filter virtual
switch
```

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security virtualswitch-filter virtualswitch | tab
IF
NAME  NAME   ROUTE  NAME         NAME
-------------------------------------------
vs1
      arp    X
      ipv4   X
      ipv6   -
                    switch.0010
                                 switch.0020
      iso    -
                    switch.0010
                                 switch.0020
      goose  -
                    switch.0010
                                 switch.0020

 !
!
```

If no virtual switch filters have been configured, add filters as needed. For more information, refer to "Adding a Virtual Switch Filter" (Page 493).

12.1.5.3 Adding a Virtual Switch Filter

To add a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure one or more virtual switches are configured. For more information, refer to "Adding a Virtual Switch" (Page 489).
3. Add the virtual switch filter by typing:

   ```
   security virtualswitch-filter virtualswitch { interface }
   ```

   Where:

   - `{ interface }` is a virtual switch interface
4. Configure one or more rules to be used when filtering. For more information, refer to "Adding a Rule" (Page 495).
5. Add the desired rules to the virtual switch filter. For more information, refer to "Adding a Rule to a Virtual Switch Filter" (Page 496).
6. Type `commit` and press **Enter** to save the changes.

12.1.5.4 Deleting a Virtual Switch Filter

To delete a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the virtual switch filter by typing:

   ```
   no security virtualswitch-filter virtualswitch { name }
   ```

   Where:

   - `{ name }` is the name of the virtual switch filter
3. Type `commit` and press **Enter** to save the changes.

12.1.6 Managing Filtering Rules

A virtual switch filter can apply one or more rules to traffic traversing a virtual switch.

12.1.6.1 Viewing a List of Rules

To view a list of rules that can be used by a virtual switch filter, type:

```
show running-config security virtualswitch-filter rules
```

If rules have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security virtualswitch-filter rules | tab
NAME   ACTION  SRCMAC             DSTMAC             PROTO
-------------------------------------------------------------
arp    accept  -                  -                  arp
goose  accept  00:00:00:00:11:11  01:0c:cd:01:00:33  0x88b8
ipv4   accept  00:00:00:00:00:01  00:00:00:00:00:02  ipv4
ipv6   accept  -                  -                  ipv6
iso    accept  -                  -                  iso

 !
!
```

If no rules have been configured, add rules as needed. For more information, refer to "Adding a Rule" (Page 495).

12.1.6.2 Viewing a List of Rules Assigned to a Virtual Switch Filter

To view a list of rules assigned to a virtual switch filter, type:

```
show running-config security virtualswitch-filter virtual
switch { name } rule
```

Where:

- `{ name }` is the name of the virtual switch filter

If rules have been assigned, a table or list similar to the following example appears:

```
ruggedcom# show running-config security virtualswitch-filter virtualswitch vs1
 rule | tab
NAME   ROUTE  NAME         NAME
----------------------------------------
arp    X
ipv4   X
ipv6   -
               switch.0010
                            switch.0020
iso    -
               switch.0010
                            switch.0020
goose  -
               switch.0010
                            switch.0020

  !
 !
!
```

If no rules have been assigned, assign them as needed. For more information, refer to "Adding a Rule to a Virtual Switch Filter" (Page 496).

12.1.6.3 Adding a Rule

To add a rule that can be used by a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure one or more virtual switches are configured. For more information, refer to "Adding a Virtual Switch" (Page 489).
3. Add the virtual switch filter by typing:

   ```
   security virtualswitch-filter rules { rule }
   ```

   Where:

   - `{ rule }` is the name of the rule
4. Configure the following parameter(s) as required:

Parameter	Description
`action { action }`	**Synopsis:** [accept | drop] **Default:** accept The action taken when an incoming frame meets the criteria.
`srcmac { srcmac }`	**Synopsis:** A string up to 17 characters long The required source MAC address for incoming frames.
`dstmac { dstmac }`	**Synopsis:** A string up to 17 characters long The required destination MAC address for incoming frames.
`proto { proto }`	**Synopsis:** A string or [iso | arp | ipv4 | ipv6 | goose] The pre-defined protocol or hex-string (i.e. 0x88A2) used to create the frames.

Parameter	Description
`goose-ied-name { goose-ied-name }`	**Synopsis:** A string up to 32 characters long The name of the IED device. Only applicable to the GOOSE protocol.

5. Type `commit` and press **Enter** to save the changes.
6. Add the rule to a virtual switch filter. For more information, refer to "Adding a Rule to a Virtual Switch Filter" (Page 496).

12.1.6.4 Adding a Rule to a Virtual Switch Filter

To add a rule to a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the rule by typing:

   ```
   security virtualswitch-filter virtualswitch { name } rule
   { rule }
   ```

   Where:

   - `{ name }` is the name of the virtual switch filter
   - `{ rule }` is the name of the rule
3. Configure the in/out interfaces for the rule. For more information, refer to "Adding an In/Out Interface" (Page 498).
4. Type `commit` and press **Enter** to save the changes.

12.1.6.5 Deleting a Rule

To delete a rule used to filter virtual switch traffic, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the rule by typing:

   ```
   no security virtualswitch-filter rules { rule }
   ```

   Where:

   - `{ rule }` is the name of the rule
3. Type `commit` and press **Enter** to save the changes.

12.1.6.6 Deleting a Rule from a Virtual Switch Filter

To delete a rule from a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the filter by typing:

   ```
   no security virtualswitch-filter virtualswitch { name }
   rule { rule }
   ```

   Where:

   - `{ name }` is the name of the virtual switch filter
   - `{ rule }` is the name of the rule

3. Type `commit` and press **Enter** to save the changes.

12.1.7 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.

12.1.7.1 Viewing a List of In/Out Interfaces

To view a list of in/out interfaces that can be used by a virtual switch filter, type:

```
show running-config security virtualswitch-filter virtual
switch { name } rule { rule } [ in-interface | out-inter
face ]
```

Where:

- `{ name }` is the name of the virtual switch filter
- `{ rule }` is the name of the rule

If in/out interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security virtualswitch-filter virtualswitch vs1
 rule in-interface | tab
NAME   NAME
--------------------
ipv6
       switch.0010
iso
       switch.0010
goose
       switch.0010

  !
 !
!
```

If no in/out interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an In/Out Interface" (Page 498).

12.1.7.2 Adding an In/Out Interface

To add an in/out interface that can be used by a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the in/out interface by typing:

   ```
   security virtualswitch-filter virtualswitch { name } rule
   { rule } [ in-interface | out-interface ] { interface }
   ```

   Where:

   - `{ name }` is the name of the virtual switch filter
   - `{ rule }` is the name of the rule
   - `{ interface }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

12.1.7.3 Deleting an In/Out Interface

To delete an in/out interface that can be used by a virtual switch filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the interface by typing:

   ```
   no security virtualswitch-filter virtualswitch { name }
   rule { rule } [ in-interface | out-interface ] { inter
   face }
   ```

   Where:

   - `{ name }` is the name of the virtual switch filter
   - `{ rule }` is the name of the rule
   - `{ interface }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

12.1.8 Managing VLANs for Virtual Switches

This section describes how to configure and manage VLANs for virtual switches.

12.1.8.1 Viewing a List of Virtual Switch VLANs

To view a list of virtual switch VLANs, type:

```
show running-config interface virtualswitch { id } vlan
```

Where:

- `{ id }` is the ID assigned to the virtual switch

If VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface virtualswitch 1 vlan | tab
     IP
     ADDRESS
VID  SRC      QOS  INGRESS  MARK
---------------------------------
100  static

 !
!
```

If no virtual switch VLANs have been configured, add VLANs as needed. For more information, refer to "Adding a Virtual Switch VLAN" (Page 499).

12.1.8.2 Adding a Virtual Switch VLAN

To add virtual switch VLAN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the VLAN by typing:

   ```
   interface virtualswitch { id } vlan { vlan-id }
   ```

   Where:

   - `{ id }` is the ID assigned to the virtual switch
   - `{ vlan-id }` is the ID assigned to the VLAN
3. Configure the following parameter(s) as required:

Parameter	Description
`ip-address-src { ip-address-src }`	**Synopsis:** [static | dynamic] **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
`ipv6-address-src { ipv6-address-src }`	**Synopsis:** [static | dynamic] **Default:** static Whether the IPv6 address is static or dynamically assigned via DHCPv6

4. [Optional] Add a QoS map. For more information, refer to "Adding a QoS Map" (Page 919).
5. Type `commit` and press **Enter** to save the changes.

12.1.8.3 Deleting a Virtual Switch VLAN

To delete a virtual switch VLAN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen VLAN by typing:

   ```
   no interface virtualswitch { id } vlan { vlan-id }
   ```

   Where:

   - `{ id }` is the ID assigned to the virtual switch
   - `{ vlan-id }` is the ID assigned to the VLAN
3. Type `commit` and press **Enter** to save the changes.

12.2 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.

12.2.1 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, type:

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 530).

```
show tunnel l2tunneld status round-trip-time
```

A table or list similar to the following example appears:

```
ruggedcom# show tunnel l2tunneld status round-trip-time
                                    MINIMUM   AVERAGE   MAXIMUM
REMOTE IP    TRANSMITTED  RECEIVED  RTT       RTT       RTT       DEVIATION
-------------------------------------------------------------------------------
192.168.5.1  45           42        0.277000  0.917000  3.735000  0.556000
```

This table or list provides the following information:

Parameter	Description
`transmitted`	**Synopsis:** An integer The number of beacon frames transmitted through the tunnel.
`received`	**Synopsis:** An integer The number of beacon frames received through the tunnel.
`minimum-rtt`	**Synopsis:** A string up to 32 characters long The Minimum Beacon Round-Trip-Time.
`average-rtt`	**Synopsis:** A string up to 32 characters long The Average Beacon Round-Trip-Time.
`maximum-rtt`	**Synopsis:** A string up to 32 characters long The Maximum Beacon Round-Trip-Time.
`deviation`	**Synopsis:** A string up to 32 characters long The standard deviation.

12.2.2 Configuring the Layer 2 Tunnel Daemon

To configure the Layer 2 tunnel daemon, do the following:

⚠ NOTICE

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.

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » l2tunneld*** and configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables the Layer 2 protocols server.
`udp-port { udp-port }`	**Synopsis:** An integer between 1 and 65535 **Default:** 1311 The UDP port to communicate with the other daemon.
`beacon-interval { beacon-interval }`	**Synopsis:** An integer between 10 and 3600 or [off] **Default:** 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 524) or "Adding a Generic Tunnel" (Page 529).
4. Type `commit` and press **Enter** to save the changes.

12.3 Managing 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.

12.3.1 Configuring L2TP Tunnels

To configure L2TP tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » l2tp*** and configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables L2TP.
`local-ip { local-ip }`	**Synopsis:** 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 { first-ip }`	**Synopsis:** 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.
`max-connection { max-connection }`	**Synopsis:** An integer between 1 and 10 The maximum number of connections.

Parameter	Description
`closing-wait-timeout { closing-wait-time out }`	**Synopsis:** An integer between 5 and 120 **Default:** 60 The number of seconds to wait before the tunnel is cleaned up after the tunnel moves to closing-wait state.

3. Configure Domain Name System (DNS) or Windows Internet Name Service (WINS) servers. For more information, refer to either "Configuring DNS Servers" (Page 503) or "Configuring WINS Servers" (Page 504).
4. Configure L2TP tunnels to carry Point-to-Point Protocol (PPP) sessions. For more information, refer to "Configuring PPP Options" (Page 503).
5. Type `commit` and press **Enter** to save the changes.

12.3.2 Configuring DNS Servers

To configure redundant Domain Name System (DNS) servers for L2TP tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the primary and secondary DNS servers by typing:

   ```
   tunnel l2tp dns-server primary { primary-ip } secondary
   { secondary-ip }
   ```

   Where:

   - { primary-ip } is the IP address of the primary DNS server
   - { secondary-ip } is the IP address of the secondary DNS server
3. Type `commit` and press **Enter** to save the changes.

12.3.3 Configuring PPP Options

To configure L2TP tunnels to carry Point-to-Point Protocol (PPP) sessions, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » l2tp » ppp*** and 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 187).

Parameter	Description
`auth-local`	Authorizes locally instead of using radius server.
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1410 Maximum transmission unit (largest packet size allowed for this interface). **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1410 bytes (jumbo frames) up to 9216 bytes on Gigabit Ethernet ports only.
`mru { mru }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1410 The Maximum Receive Unit (MRU) or maximum packet size passed when received. **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1410 bytes (jumbo frames) up to 9216 bytes when the L2TP tunnel is established over Gigabit Ethernet ports.

3. Type `commit` and press **Enter** to save the changes.

12.3.4 Configuring WINS Servers

To configure redundant Domain Name System (WINS) servers for L2TP tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the primary and secondary WINS servers by typing:

   ```
   tunnel l2tp WINS-server primary { primary-ip } secondary
   { secondary-ip }
   ```

   Where:

   - { primary-ip } is the IP address of the primary WINS server
   - { secondary-ip } is the IP address of the secondary WINS server
3. Type `commit` and press **Enter** to save the changes.

12.4 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 LTPv3 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.

12.4.1 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.

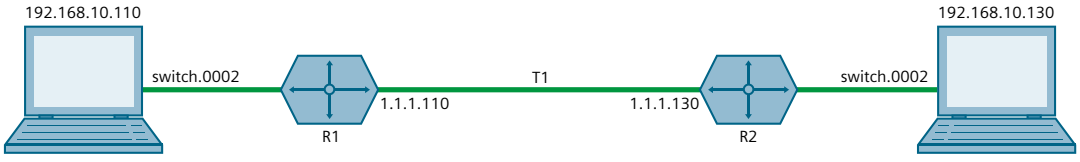


Figure 12.1 Basic L2TPv3 Tunnel

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 l2t-1-1 tunnel. Traffic sent via virtual switch switch.0003 traverses the l2t-1-2 tunnel.

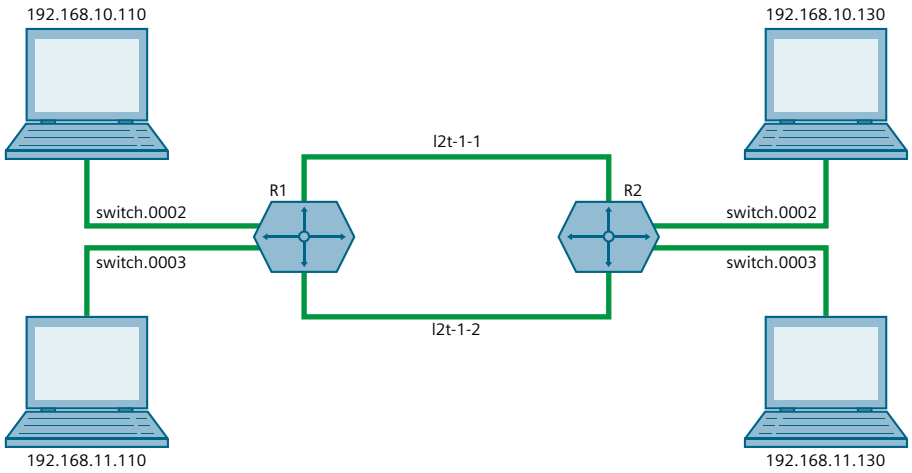


Figure 12.2 Multiple LAN Extensions Over a Single L2TPv3 Tunnel

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 l2t-1-1 bridge, and vice versa.

Traffic sent from 192.158.10.110 to 192.168.11.110 traverses the l2t-2-1 bridge, and vice versa.

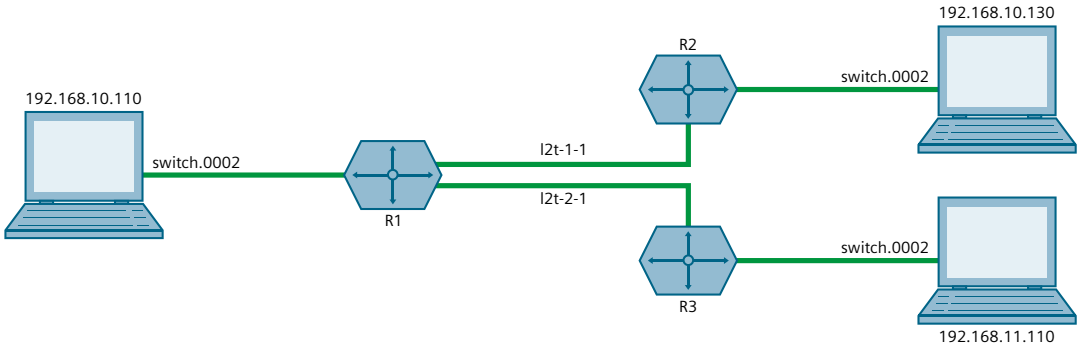


Figure 12.3 Multiple LAN Extensions Over Multiple L2TPv3 Tunnels

12.4.2 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 508) or "Adding a Dynamic L2TPv3 Tunnel" (Page 511).

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 491).

   For information about assigning an IP address to the L2TPv3 tunnel interface, refer to either "Managing IPv4 Addresses" (Page 269) or "Managing IPv6 Addresses" (Page 270).

12.4.3 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*.

12.4.3.1 Enabling/Disabling Static L2TPv3 Tunnels

To enable or disable static L2TPv3 tunnels, do the following:

1. Make sure the CLI is in Configuration mode.

2. Enable or disable static L2TPv3 tunnels by typing:

   Enabling Tunnels

   ```
   tunnel l2tpv3 static enabled
   ```

   Disabling Tunnels

   ```
   no tunnel l2tpv3 static enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

12.4.3.2 Viewing a List of Static L2TPv3 Tunnels

To view a list of static L2TPv3 tunnels, type:

```
show running-config tunnel l2tpv3 static tunnel
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tpv3 static tunnel
tunnel
 l2tpv3 static tunnel 1
  tunnel-id        1
  remote-tunnel-id 2
  transport-encap  udp
  local-ip         192.168.0.10
  local-port       1024
  remote-ip        192.168.0.11
  remote-port      1025
  session 1
   local-session-id       10
   remote-session-id      20
   l2tp-specific-sublayer default
   vlan 4
   !
  !
  session 2
   local-session-id       30
   remote-session-id      40
   l2tp-specific-sublayer default
  !
 !
!
```

If no tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Static L2TPv3 Tunnel" (Page 508).

12.4.3.3 Adding a Static L2TPv3 Tunnel

To add a static L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.

Note

The tunnel name must consist of one to three numeric and/or lowercase alphanumeric characters.

2. Add the tunnel by typing:

```
tunnel l2tpv3 static tunnel { name }
```

Where { name } is the name of the tunnel.

3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/Disables the tunnel
`tunnel-id { tunnel-id }`	**Synopsis:** An integer between 1 and 65535 The local tunnel-id
`remote-tunnel-id { remote-tunnel-id }`	**Synopsis:** An integer between 1 and 65535 Tunnel-id of remote tunnel endpoint
`transport-encap { transport-encap }`	**Synopsis:** [udp | ip] **Default:** udp The transport protocol (UDP or IP) to encapsulate the tunnel messages
`local-ip { local-ip }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long Ip address of local interface
`local-port { local-port }`	**Synopsis:** An integer between 1024 and 65535 Local listening transport port for tunnel service
`remote-ip { remote-ip }`	**Synopsis:** 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 { remote-port }`	**Synopsis:** An integer between 1024 and 65535 The listening transport port of remote device for tunnel service

4. Add one or more sessions to the tunnel configuration. For more information, refer to either:
   - "Adding a Session for a Static L2TPv3 Tunnel" (Page 514)
   - "Adding a Session for a Dynamic L2TPv3 Tunnel" (Page 515)
5. Enter `enable` to enable the tunnel.

6. Type `commit` and press **Enter** to save the changes.

12.4.3.4 Deleting a Static L2TPv3 Tunnel

To delete a static L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tunnel by typing:

   ```
   no tunnel l2tpv3 static tunnel { name }
   ```

   Where { name } is the name of the tunnel.
3. Type `commit` and press **Enter** to save the changes.

12.4.4 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.

12.4.4.1 Enabling and Configuring Dynamic L2TPv3 Tunnels

To enable and configure dynamic L2TPv3 tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable dynamic L2TPv3 tunnels by typing:

   ```
   tunnel l2tpv3 dynamic enabled
   ```

3. Configure the following parameters as required:

Parameter	Description
`mode { mode }`	**Synopsis:** [lac | lns] **Default:** lns The l2tp operational mode
`log-level { log-level }`	**Synopsis:** [none | error | warning | notice | info | all] **Default:** none Logging message level
`log-message { log-message }`	**Synopsis:** [none | protocol | fsm | api | transport | data | ppp | avp | func | system | all] **Default:** none Logging message category

4. Type `commit` and press **Enter** to save the changes.

12.4.4.2 Viewing a List of Dynamic L2TPv3 Tunnels

To view a list of dynamic L2TPv3 tunnels, type:

```
show running-config tunnel l2tpv3 dynamic tunnel
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tpv3 dynamic tunnel
tunnel
 l2tpv3 dynamic tunnel 1
  hostname       ruggedcom
  authentication none
  digest         md5
  interop        0
 !
!
```

If no tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Dynamic L2TPv3 Tunnel" (Page 511).

12.4.4.3 Adding a Dynamic L2TPv3 Tunnel

To add a dynamic L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.

   Note

   The tunnel name must consist of one to three numeric and/or lowercase alphanumeric characters.

2. Add the tunnel by typing:

   ```
   tunnel l2tpv3 dynamic tunnel { name }
   ```

   Where { name } is the name of the tunnel.

3. Configure the following parameter(s) to define the new tunnel:

   Note

   Transport encapsulation is only configurable when Dynamic L2TPv3 is in **lac** mode.

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/Disables the tunnel

Parameter	Description
`remote-ip { re mote-ip }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long Ip address of remote tunnel endpoint
`hostname { hostname }`	**Synopsis:** A string between 1 and 63 characters long Hostname used in AVP
`local-ip { local-ip }`	**Synopsis:** 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 { transport-encap }`	**Synopsis:** [udp | ip] **Default:** udp The transport protocol (UDP or IP) to encapsulate the tunnel messages
`authentication { au thentication }`	**Synopsis:** [none | challenge] **Default:** none The authentication of tunnel
`secret { secret }`	**Synopsis:** A string between 1 and 63 characters long The password of tunnel negotiation
`digest { digest }`	**Synopsis:** [md5 | sha1] **Default:** md5 Message digest AVP encryption
`interop { interop }`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 Specify a bitmask of flags to control non-standard behaviour for interopability with other L2TPv3 implementation
`persist-pend-timeout { persist-pend-time out }`	**Synopsis:** An integer between 10 and 6000 **Default:** 60 The time (in seconds) that a persisting tunnel will wait in RETRY state before trying to establish itself again
`hello { hello }`	**Synopsis:** An integer between 5 and 1000 **Default:** 60 timeout used for periodic L2TP Hello messages (in seconds)
`hidden { hidden }`	**Synopsis:** [true | false] **Default:** false Enables/Disabled AVP hidden

Parameter	Description
`receive-windows { receive-windows }`	**Synopsis:** An integer between 5 and 512 **Default:** 10 Received windows size
`established-timeout { established-timeout }`	**Synopsis:** An integer between 30 and 1000 **Default:** 120 The time (in seconds) that a tunnel will wait for the peer to complete the tunnel setup message exchange
`log { log }`	**Synopsis:** [true | false] **Default:** false Enables/Disables logging tunnel control messages

4. Configure the retransmit settings as required:

Parameter	Description
`max-retries { max-retries }`	**Synopsis:** An integer between 1 and 1000 **Default:** 5 The maximum number of retransmits of unacknowledged control frames
`retry-timeout { retry-timeout }`	**Synopsis:** An integer between 1 and 8 **Default:** 1 The delay (in seconds) before sending the first retry of unacknowledged control frames

5. Add one or more sessions to the tunnel configuration. For more information, refer to either:
   - "Adding a Session for a Static L2TPv3 Tunnel" (Page 514)
   - "Adding a Session for a Dynamic L2TPv3 Tunnel" (Page 515)
6. Type `commit` and press **Enter** to save the changes.

12.4.4.4 Deleting a Dynamic L2TPv3 Tunnel

To delete a dynamic L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tunnel by typing:

   ```
   no tunnel l2tpv3 dynamic tunnel { name }
   ```

   Where { name } is the name of the tunnel.
3. Type `commit` and press **Enter** to save the changes.

12.4.5 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.

12.4.5.1 Viewing a List of Sessions

To view a list of sessions defined for an L2TPv3 tunnel, type:

```
show running-config tunnel l2tpv3 [ static | dynamic ] tunnel
{ tunnel-name } session
```

Where { tunnel-name } is the name of the tunnel.

If sessions have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tpv3 static tunnel 1 session
tunnel
 l2tpv3 static tunnel 1
  session 1
   local-session-id       10
   remote-session-id      20
   l2tp-specific-sublayer default
   vlan 4
   !
  !
  session 2
   local-session-id       30
   remote-session-id      40
   l2tp-specific-sublayer default
  !
 !
!
```

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 514)
- "Adding a Session for a Dynamic L2TPv3 Tunnel" (Page 515)

12.4.5.2 Adding a Session for a Static L2TPv3 Tunnel

To add a session to a static L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the session by typing:

   ```
   tunnel l2tpv3 static tunnel { tunnel-name } session { tun
   nel-session }
   ```

   Where:

   - { tunnel-name } is the name of the tunnel
   - { tunnel-session } is the name of the tunnel session

3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/Disables the session
`local-session-id { local-session-id }`	**Synopsis:** An integer between 1 and 65535 The local session-id provides the necessary context for all further packet processing
`remote-session-id { remote-session-id }`	**Synopsis:** 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 { l2tp-specific-sublayer }`	**Synopsis:** [default | none] **Default:** default L2TP specific sublayer processing type
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1488 Maximum transmission unit (largest packet size allowed for this interface). **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1488 bytes (jumbo frames) up to 9216 bytes on Gigabit Ethernet ports only.

4. Configure local and remote cookies. For more information, refer to "Configuring Local and Remote Cookies" (Page 516).
5. Type `commit` and press **Enter** to save the changes.

12.4.5.3 Adding a Session for a Dynamic L2TPv3 Tunnel

To add a session to a dynamic L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the session by typing:

```
tunnel l2tpv3 dynamic tunnel { tunnel-name } session
{ tunnel-session }
```

Where:

- { tunnel-name } is the name of the tunnel
- { tunnel-session } is the name of the tunnel session

3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/Disables the session
`remote-end-id { remote-end-id }`	**Synopsis:** An integer between 1 and 65535 Remote endpoint ID to identify session with remote system
`l2tp-specific-sublayer { l2tp-specific-sublayer }`	**Synopsis:** [default | none] **Default:** default L2TP specific sublayer processing type
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1488 Maximum transmission unit (largest packet size allowed for this interface). **Note** RUGGEDCOM RX1500, RX1501, RX1510, RX1511, and RX1512 devices support packet sizes over 1488 bytes (jumbo frames) up to 9216 bytes on Gigabit Ethernet ports only.
`log { log }`	**Synopsis:** [true | false] **Default:** false Enables/Disables logging session control messages

4. Configure local and remote cookies. For more information, refer to "Configuring Local and Remote Cookies" (Page 516).
5. Type `commit` and press **Enter** to save the changes.

12.4.5.4 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.

1. Make sure the CLI is in Configuration mode.

2. Select an L2TPv3 tunnel and session by typing:

   ```
   tunnel l2tpv3 [ static | dynamic ] tunnel { tunnel-name }
   session { tunnel-session }
   ```

   Where:

   - { tunnel-name } is the name of the tunnel
   - { tunnel-session } is the name of the tunnel session

3. Type `local-cookie` and then configure the following parameters as required:

Parameter	Description
`size { size }`	**Synopsis:** [4 | 8] Cookie size in byte.
`low-value { low-value }`	**Synopsis:** An integer Lower value of cookie. This value must match with low-value of other endpoint's remote cookie
`high-value { high-value }`	**Synopsis:** 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

4. Type `remote-cookie` and then configure the following parameters as required:

Parameter	Description
`size { size }`	**Synopsis:** [4 | 8] Cookie size in byte
`low-value { low-value }`	**Synopsis:** An integer Lower value of cookie. This value must match with low-value of other endpoint's local cookie
`high-value { high-value }`	**Synopsis:** An integer Higher value of cookie if its size is 8. This value must match with high-value of other endpoint's local cookie

5. Type `commit` and press **Enter** to save the changes.

12.4.5.5 Deleting a Session

To delete a session for a static or dynamic L2TPv3 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the tunnel by typing:

   ```
   no tunnel l2tpv3 [ static | dynamic ] tunnel { tun
   nel-name } session { tunnel-session }
   ```

   Where:

   - { tunnel-name } is the name of the tunnel
   - { tunnel-session } is the name of the tunnel session

3. Type `commit` and press **Enter** to save the changes.

12.4.6 Managing VLANs for L2TPv3 Tunnels

This section describes how to manage VLANs for L2TPv3 tunnel sessions. Each session supports up to 128 VLAN memberships.

12.4.6.1 Viewing a List of VLANs

To view a list of the VLANs configured for a static or dynamic L2TPv3 tunnel session, type:

```
show running-config tunnel l2tpv3 [ static | dynamic ] tunnel
{ tunnel-name } session { tunnel-session } vlan
```

Where:

- { tunnel-name } is the name of the tunnel
- { tunnel-session } is the name of the tunnel session

A table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tpv3 static tunnel 1 session vlan
tunnel
 l2tpv3 static tunnel 1
  session 1
   vlan 4
   !
  !
 !
!
```

If no VLANs have been configured, add VLANs as needed. For more information, refer to "Adding a VLAN" (Page 518).

12.4.6.2 Adding a VLAN

To add a VLAN to a static or dynamic L2TPv3 tunnel session, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the session by typing:

```
tunnel l2tpv3 [ static | dynamic ] tunnel { tunnel-name }
session { tunnel-session } vlan { vid }
```

Where:

- { tunnel-name } is the name of the tunnel.
- { tunnel-session } is the name of the tunnel session.
- { vid } is the VLAN ID for the routable logical interface. the value must be between 1 and 4094.

3. Type `commit` and press **Enter** to save the changes.

12.4.6.3 Deleting a VLAN

To delete a VLAN for a static or dynamic L2TPv3 tunnel session, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tunnel by typing:

```
no tunnel l2tpv3 [ static | dynamic ] tunnel { tun
nel-name } session { tunnel-session } vlan { vid }
```

Where:

- { tunnel-name } is the name of the tunnel
- { tunnel-session } is the name of the tunnel session
- { vid } is the VLAN ID for the routable logical interface

3. Type `commit` and press **Enter** to save the changes.

12.4.7 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.

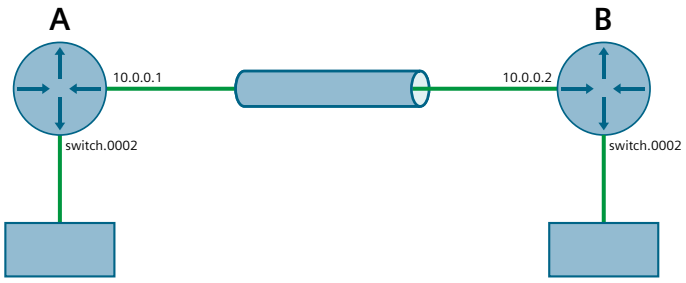


Figure 12.4 L2TPv3 Tunnel Between Routers

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 335).

     When switch port mode is disabled, an interface labeled fe-{ slot }-{ port } (e.g. fe-1-1) 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 269).

  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 385).

  4. Add a static L2TPv3 tunnel with the following settings:

name	tunnel1
tunnel-id	1
remote-tunnel-id	1
local-ip	10.0.0.1
local-port	5000
remote-ip	10.0.0.2
remote-port	5001

     For more information about adding a static L2TPv3 tunnel, refer to "Adding a Static L2TPv3 Tunnel" (Page 508).

  5. Add a session to the new static tunnel with the following settings:

name	session1
local-session-id	1
remote-session-id	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 514).

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 335).
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 269).
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 385).
4. Add a static L2TPv3 tunnel with the following settings:

name	tunnel1
tunnel-id	1
remote-tunnel-id	1
local-ip	10.0.0.2
local-port	5001
remote-ip	10.0.0.1
remote-port	5000

   For more information about adding a static L2TPv3 tunnel, refer to "Adding a Static L2TPv3 Tunnel" (Page 508).
5. Add a session to the new static tunnel with the following settings:

name	session1
local-session-id	1
remote-session-id	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 514).
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`.

12.5 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

12.5.1 Viewing the GOOSE Tunnel Statistics

To view the GOOSE tunnel statistics, type:

```
show tunnel l2tunneld status goose
```

A table or list similar to the following example appears:

```
ruggedcom# show tunnel l2tunneld status goose
l2tunneld status goose test
 ifname    switch.0100
 mac       01:0c:cd:01:00:33
 rx frames 2
 tx frames 0
 rx chars  114
 tx chars  0
 errors    0
 connections
             RX       TX       RX     TX
REMOTE IP    PACKETS  PACKETS  BYTES  BYTES  ERRORS
-------------------------------------------------------
192.168.2.2  2        0        122    0      0
```

This table or list provides the following information:

Parameter	Description
`ifname`	**Synopsis:** A string between 1 and 15 characters long The name of the VLAN interface.
`mac`	**Synopsis:** A string up to 17 characters long The Multicast Destination MAC Address of the Goose message.
`rx-frames`	**Synopsis:** An integer The number of frames received through the tunnel.
`tx-frames`	**Synopsis:** An integer The number of frames transmitted through the tunnel.
`rx-chars`	**Synopsis:** An integer The number of bytes received through the tunnel.
`tx-chars`	**Synopsis:** An integer The number of bytes transmitted through the tunnel.
`errors`	**Synopsis:** An integer The number of errors through the tunnel.

12.5.2 Viewing a List of GOOSE Tunnels

To view a list of GOOSE tunnels, type:

```
show running-config tunnel l2tunneld goose
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld goose tunnel | tab
                                      IP
NAME  INTERFACE    MULTICAST MAC      ADDRESS
-----------------------------------------------
1     switch.0001  01:0c:cd:01:01:01

!
```

If no GOOSE tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a GOOSE Tunnel" (Page 524).

12.5.3 Adding a GOOSE Tunnel

To configure a GOOSE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tunnel by typing:

   ```
   tunnel l2tunneld goose tunnel { name }
   ```

   Where:

   - `{ name }` is the name of the GOOSE tunnel
3. Configure the following parameter(s) as required:

Parameter	Description
`interface { interface }`	**Synopsis:** A string The interface to listen on for GOOSE frames.
`multicast-mac { multicast-mac }`	**Synopsis:** A string up to 17 characters long The multicast MAC address to listen for.

4. If necessary, configure one or more remote daemons for the tunnel. For more information, refer to "Adding a Remote Daemon" (Page 525).
5. Type `commit` and press **Enter** to save the changes.

12.5.4 Deleting a GOOSE Tunnel

To delete a GOOSE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the GOOSE tunnel by typing:

   ```
   no tunnel l2tunneld goose tunnel { name }
   ```

   Where:

- `{ name }` is the name of the GOOSE tunnel

3. Type `commit` and press **Enter** to save the changes.

12.5.5 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.

12.5.5.1 Viewing a List of Remote Daemons

To view a list of remote daemons configured for a GOOSE tunnel, type:

```
show running-config tunnel l2tunneld goose tunnel { name }
remote-daemon
```

Where:

- `{ name }` is the name of the GOOSE tunnel

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld goose tunnel 1 remote-daemon
tunnel
 l2tunneld goose tunnel 1
  remote-daemon 192.168.10.2
  !
 !
!
```

If no remote daemons have been configured, add daemons as needed. For more information, refer to "Adding a Remote Daemon" (Page 525).

12.5.5.2 Adding a Remote Daemon

To configure a remote daemon for a GOOSE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the remote daemon by typing:

   ```
   tunnel l2tunneld goose tunnel remote-daemon { address }
   ```

   Where:

   - `{ address }` is the IP address of the remote daemon

3. Type `commit` and press **Enter** to save the changes.

12.5.5.3 Deleting a Remote Daemon

To delete a remote daemon, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the remote daemon typing:

   ```
   no tunnel l2tunneld goose tunnel { name } remote-daemon
   { address }
   ```

   Where:

   - `{ name }` is the name of the GOOSE tunnel
   - `{ address }` is the IP address of the remote daemon
3. Type `commit` and press **Enter** to save the changes.

12.5.6 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.

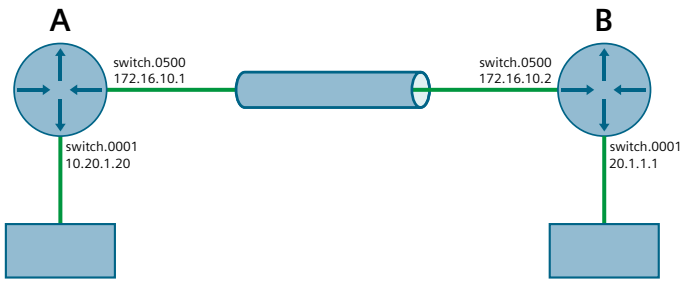


Figure 12.5 GOOSE Tunnel Between Routers

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:

name	incoming-traffic
interface	switch.0001
multicast-mac	01:0c:cd:01:00:44

     For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 524).
  2. Add a GOOSE tunnel for outgoing traffic to router B with the following settings:

name	outgoing-traffic
interface	switch.0500

multicast-mac	01:0c:cd:01:00:41

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 524).

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 501).

- **Configuring Router B**

1. Add a GOOSE tunnel for incoming traffic from the publisher/describer with the following settings:

name	incoming-traffic
interface	switch.0001
multicast-mac	01:0c:cd:01:00:41

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 524).

2. Add a GOOSE tunnel for outgoing traffic to router A with the following settings:

name	outgoing-traffic
interface	switch.0500
multicast-mac	01:0c:cd:01:00:44

For more information about adding a GOOSE tunnel, refer to "Adding a GOOSE Tunnel" (Page 524).

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 501).

12.6 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)

12.6.1 Viewing the Generic Tunnel Statistics

To view the generic tunnel statistics, type:

```
show tunnel l2tunneld status generic
```

A table or list similar to the following example appears:

```
ruggedcom# show tunnel l2tunneld status generic
TUNNEL               RX      TX      RX     TX                          RX
 TX       RX     TX
NAME    IFNAME       FRAMES  FRAMES  CHARS  CHARS  ERRORS  REMOTE IP    PACKETS
 PACKETS  BYTES  BYTES  ERRORS
-------------------------------------------------------------------------------
iso     switch.0002  5       6       300    360    0
                                                          192.168.5.1  11       0
        704    0      0
```

This table or list provides the following information:

Parameter	Description
`{ tunnel-name }`	**Synopsis:** A string up to 32 characters long The generic tunnel name.
`ifname`	**Synopsis:** A string between 1 and 15 characters long The name of the ingress interface.
`rx-frames`	**Synopsis:** An integer The number of frames received through the tunnel.
`tx-frames`	**Synopsis:** An integer The number of frames transmitted through the tunnel.
`rx-chars`	**Synopsis:** An integer The number of bytes received through the tunnel.
`tx-chars`	**Synopsis:** An integer The number of bytes transmitted through the tunnel.
`errors`	**Synopsis:** An integer The number of errors received through the tunnel.
`rx-packets`	**Synopsis:** An integer The number of frames received through the tunnel.
`tx-packets`	**Synopsis:** An integer The number of frames transmitted through the tunnel.
`rx-bytes`	**Synopsis:** An integer The number of bytes received through the tunnel.

Parameter	Description
`tx-bytes`	**Synopsis:** An integer The number of bytes transmitted through the tunnel.
`errors`	**Synopsis:** An integer The number of errors received through the tunnel.

12.6.2 Viewing a List of Generic Tunnels

To view a list of generic tunnels, type:

```
show running-config tunnel l2tunneld generic tunnel
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel | tab
                   REPLACE        EGRESS  IP
NAME  INGRESS IF   MAC      TYPE  IF      ADDRESS
-------------------------------------------------
1     switch.0001  -
                           iso

!
```

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Generic Tunnel" (Page 529).

12.6.3 Adding a Generic Tunnel

To configure a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tunnel by typing:

   ```
   tunnel l2tunneld generic tunnel { name }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
3. Configure the following parameter(s) as required:

Parameter	Description
`ingress-if { ingress-if }`	**Synopsis:** A string The interface to listen on for Ethernet type frames.
`replace-mac`	Replaces the sender's MAC with the out-interface's MAC.

4. If necessary, configure one or more remote daemon IP addresses for the tunnel. For more information, refer to "Adding an IP Address" (Page 531).
5. If necessary, define one or more Ethernet types to be forwarded. For more information, refer to "Adding an Ethernet Type" (Page 533).
6. Type `commit` and press **Enter** to save the changes.

12.6.4 Deleting a Generic Tunnel

To delete a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the generic tunnel by typing:

   ```
   no tunnel l2tunneld generic tunnel { name }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
3. Type `commit` and press **Enter** to save the changes.

12.6.5 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).

12.6.5.1 Viewing a List of IP Addresses

To view a list of remote Layer 2 protocol server IP addresses for a generic tunnel configuration, type:

```
show running-config tunnel l2tunneld generic tunnel re
mote-daemon
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel remote-daemon ip-
address | tab
NAME  IP ADDRESS
--------------------
1
```

```
      172.112.10.1

!
```

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a Generic Tunnel" (Page 529).

12.6.5.2 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. Make sure the CLI is in Configuration mode.
2. Add the IP address by typing:

   ```
   tunnel l2tunneld generic tunnel { name } remote-daemon ip-address { address }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
   - `{ address }` is the IP address of the remote Layer 2 protocols server
3. Type `commit` and press **Enter** to save the changes.

12.6.5.3 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. Make sure the CLI is in Configuration mode.
2. Delete the IP address by typing:

   ```
   no tunnel l2tunneld generic tunnel { name } remote-daemon ip-address { address }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
   - `{ address }` is the IP address of the remote Layer 2 protocols server
3. Type `commit` and press **Enter** to save the changes.

12.6.6 Managing Remote Daemon Egress Interfaces for Generic Tunnels

This section describes how to create and manage remote daemon egress interfaces for generic tunnels.

12.6.6.1 Viewing a List of Egress Interfaces

To view a list of egress interfaces configured for a generic tunnel, type:

```
show running-config tunnel l2tunneld generic tunnel re
mote-daemon egress-if
```

If egress interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel remote-daemon
 egress-if | tab
NAME  EGRESS IF
------------------
1
      switch.0001

!
```

If no egress interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an Egress Interface" (Page 532).

12.6.6.2 Adding an Egress Interface

To add an egress interface for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the egress interface by typing:

   ```
   tunnel l2tunneld generic tunnel { name } remote-daemon
   egress-if { interface }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
   - `{ interface }` is the egress interface for Ethernet type frames
3. Type `commit` and press **Enter** to save the changes.

12.6.6.3 Deleting an Egress Interface

To delete an egress interface for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the egress interface by typing:

   ```
   no tunnel l2tunneld generic tunnel { name } remote-daemon
   egress-if { interface }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
   - `{ interface }` is the egress interface for Ethernet type frames

3. Type `commit` and press **Enter** to save the changes.

12.6.7 Managing Ethernet Types for Generic Tunnels

This section describes how to define the types of Ethernet protocols that can be forwarded by generic tunnels.

12.6.7.1 Viewing a List of Ethernet Types

To view a list of Ethernet types configured for a generic tunnel, type:

```
show running-config tunnel l2tunneld generic tunnel ether
net-type
```

If Ethernet types have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel ethernet-type | tab
NAME  TYPE
------------
1
      iso

!
```

If no Ethernet types have been configured, add types as needed. For more information, refer to "Adding an Ethernet Type" (Page 533).

12.6.7.2 Adding an Ethernet Type

To add an Ethernet type for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the Ethernet type by typing:

   ```
   tunnel l2tunneld generic tunnel { name } ethernet-type
   { type }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
   - `{ type }` is the Ethernet type to be forwarded (i.e. 0xFEFE)
3. Type `commit` and press **Enter** to save the changes.

12.6.7.3 Deleting an Ethernet Type

To delete an Ethernet type for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the Ethernet type by typing:

   ```
   no tunnel l2tunneld generic tunnel { name } ethernet-type
   { type }
   ```

   Where:

   - `{ name }` is the name of the generic tunnel
   - `{ type }` is the Ethernet type (i.e. 0xFEFE)
3. Type `commit` and press **Enter** to save the changes.

12.7 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 12.6 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.

12.7.1 Viewing Statistics for GRE Tunnels

To view the statistics collected for GRE tunnels, type:

```
show interfaces gre
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces gre
                TUNNEL  RX       RX      RX     TX       TX      TX
IFNAME  STATUS  STATUS  PACKETS  ERRORS  DROPS  PACKETS  ERRORS  DROPS
-------------------------------------------------------------------------
g1      Active  Up    52         0       0      855      51      0
g2      Active  Up    0           0       0      0           791    0
```

This table or list provides the following information:

Parameter	Description
`{ ifname }`	**Synopsis:** A string between 1 and 10 characters long The name of the GRE tunnel.
`status`	**Synopsis:** A string between 1 and 20 characters long The status of the GRE tunnel interface, possible values include: • **Active** - GRE tunnel interface is up; • **Inactive** - GRE tunnel interface is down
`tunnel-status`	**Synopsis:** A string The status of the GRE tunnel: • **Up** - GRE tunnel is up and running; • **Down** - GRE tunnel interface is inactive or tunnel remote endpoint is not reachable; • **Keepalives Disabled** - Keepalive messages have been disabled, not able to know if the tunnel remote endpoint is reachable or not
`rx-packets`	**Synopsis:** An integer The number of packets received through the tunnel.
`rx-errors`	**Synopsis:** An integer The error packets received through the tunnel.
`rx-drops`	**Synopsis:** An integer The number of packets dropped by the tunnel.
`tx-packets`	**Synopsis:** An integer The number of packets transmitted through the tunnel.

Parameter	Description
`tx-errors`	**Synopsis:** An integer The number of error packets transmitted through the tunnel.
`tx-drops`	**Synopsis:** An integer The number of packets dropped by the tunnel.

12.7.2 Viewing a List of GRE Tunnels

To view a list of GRE tunnels, type:

```
show running-config tunnel gre
```

If GRE tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel gre | tab
IF
NAME  LOCAL IP      REMOTE IP     REMOTE NET      MTU   MULTICAST  COST
-------------------------------------------------------------------------
gre   172.16.17.18  172.19.20.21  192.168.2.0/24  1476  -          0
```

If no GRE tunnels have been configured, add tunnels as needed. For more information, refer to "Adding a GRE Tunnel" (Page 536).

12.7.3 Adding a GRE Tunnel

To add a GRE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the GRE tunnel by typing:

   ```
   tunnel gre { name }
   ```

   Where:

   - `{ name }` is the interface name of the GRE tunnel network. 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.
3. Configure the following parameter(s) as required:

Parameter	Description
`local-ip { local-ip }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The IP address of the local end of the tunnel.

Parameter	Description
`remote-ip { remote-ip }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The IP address of the remote end of the tunnel.
`remote-net { remote-net }`	**Synopsis:** A string between 9 and 18 characters long or A string between 4 and 43 characters long The target network of remote end of the tunnel.
`mtu { mtu }`	**Synopsis:** An integer between 68 and 9216 **Default:** 1476 The MTU of the GRE interface.
`multicast`	Enables multicast traffic on the tunnel interface.
`cost { cost }`	**Synopsis:** An integer between 1 and 255 **Default:** 1 The routing cost associated with networking routing that directs traffic through the tunnel.
`key { key }`	**Synopsis:** [none | input | output | both] **Default:** none The key for tunneled packets
`key-id { key-id }`	**Synopsis:** An integer between 0 and 4294967295 **Default:** 0 The key ID for tunneled packets
`checksum { checksum }`	**Synopsis:** [none | input | output | both] **Default:** none The checksum for tunneled packets
`sequence { sequence }`	**Synopsis:** [none | input | output | both] **Default:** none The sequence number for tunneled packets
`alarms { alarms }`	**Synopsis:** [true | false] **Default:** false 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 **admin > alarm-cfg**.

4. [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 538).
5. [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 538).

Note

An interface in the form of *gre-{ tunnel }* (e.g. gre-t1) is added automatically to the **ip** menu.

6. Assign an IP address to the tunnel. For more information, refer to either "Adding an IPv4 Address" (Page 269) or "Adding an IPv6 Address" (Page 270).
7. Type `commit` and press **Enter** to save the changes.

12.7.4 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 the configure how DSCP marks are assigned for a specific GRE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » gre » { tunnel } » mark-choice***, where { tunnel } is the name of the GRE tunnel.
3. Configure the DSCP marking by typing:

```
tunnel gre { name } mark-choice dscpmarking dscp-type
[ mark | forward ]
```

Where { name } is name of the GRE tunnel.

Options include:

- **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, select a DSCP mark to assign by typing:

```
dscp-mark [ AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31
| AF32 | AF33 | AF41 | AF42 | AF43 | BE | CS1 | CS2 | CS3
| CS4 | CS5 | CS6 | CS7 | EF ]
```

5. Type `commit` and press **Enter** to save the changes.

12.7.5 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. Make sure the CLI is in Configuration mode.
2. Enable or disable keepalive messages by typing:

   Enable

   ```
   tunnel gre { name } gre-keepalives enabled
   ```

   Disable

   ```
   no tunnel gre { name } gre-keepalives enabled
   ```

   Where { name } is the interface name of the GRE tunnel network. 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.
3. If keepalive messages are enabled, configure the following parameters:

Parameter	Description
`interval { interval }`	**Synopsis:** An integer between 1 and 32767 **Default:** 10 The interval in second(s) at which keepalive messages are sent to the remote endpoint.
`retries { retries }`	**Synopsis:** An integer between 1 and 255 **Default:** 3 The number of keepalive message the remote endpoint can ignore before it is considered unreachable.
`failover { failover }`	**Synopsis:** [true | false] **Default:** false Enable this tunnel to support failover.

4. Type `commit` and press **Enter** to save the changes.

12.7.6 Deleting a GRE Tunnel

To delete a GRE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the GRE tunnel by typing:

   ```
   no tunnel gre { name }
   ```

   Where:

   - `{ name }` is the name of the GRE tunnel
3. Type `commit` and press **Enter** to save the changes.

12.7.7 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 546).

⚠ NOTICE

To ensure IPsec connections are independently managed when configuring GRE/IPsec, the following conditions must be met:

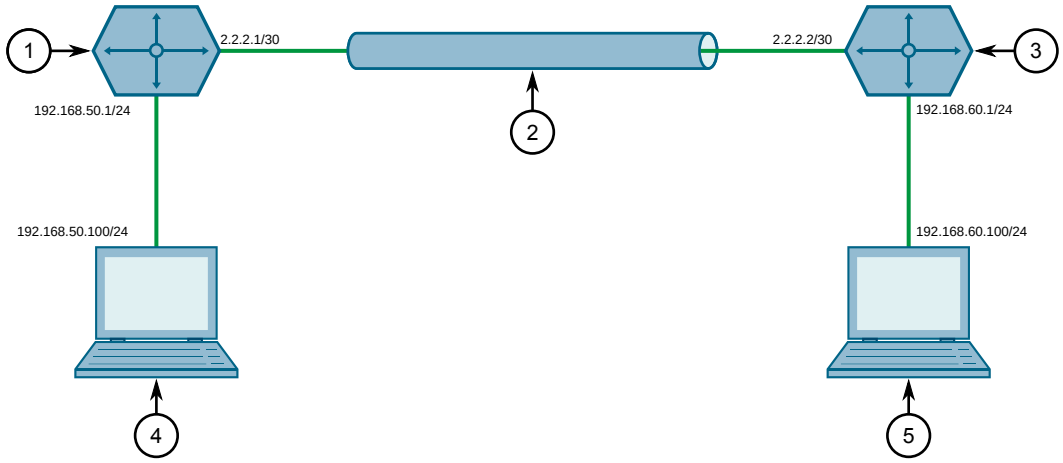
- The IPsec connection name must match the GRE tunnel interface name.
- Remote subnets defined under IPsec left/right sections are aware of each other only through the GRE tunnel. As the default value of the nexthop under left/right sections is *right side public-ip*, the nexthop value to the GRE tunnel 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/rightpublic 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 12.7 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 139).
   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 536).
   c. Enable Keepalive messages for GRE tunnel. For more information, refer to "Enabling/Disabling Keepalive Messages" (Page 538).
   d. Assign IP address *172.16.1.1/24* to the gre tunnel interface. For more information, refer to "Adding an IPv4 Address" (Page 269).
   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 553).

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 555).

g. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 560).

h. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 562).

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 563).

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 563).

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 567).

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 563).

m. Configure the right connection end for the IPsec tunnel with the following nexthop address parameters:

Parameter	Value
Type	address

Parameter	Value
Value	172.16.1.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 563).

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 567).

2. Configure Device B:

a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 139).

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 536).

c. Enable Keepalive messages for GRE tunnel. For more information, refer to "Enabling/Disabling Keepalive Messages" (Page 538).

d. Assign IP address *172.16.1.2/24* to the gre tunnel interface. For more information, refer to "Adding an IPv4 Address" (Page 269).

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 553).

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 555).

g. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 560).

h. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 562).

i. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address

Parameter	Value
Value	2.2.2.1

For more information about configuring connection ends, refer to "Managing Connection Ends" (Page 563).

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 563).

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 567).

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 563).

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 563).

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 567).

3. Enable the IPsec tunnel. For more information, refer to "Configuring IPsec Tunnels" (Page 549).
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 551).

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
  !
!
```

12.8 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 547).

⚠ 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 948).

12.8.1 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.

12.8.1.1 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.

12.8.1.2 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.

12.8.1.3 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 552).

12.8.1.4 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.

12.8.1.5 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 549).

12.8.1.6 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 241).

12.8.1.7 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 554).

12.8.2 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 235).

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec*** and configure the following parameter(s) as required:

Parameter	Description
`enabled`	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 { keep-alive }`	**Synopsis:** An integer between 1 and 86400 **Default:** 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 553).
4. Configure one or more encrypted connections. For more information, refer to "Adding a Connection" (Page 555).
5. Type `commit` and press **Enter** to save the changes.

12.8.3 Configuring Certificates and Keys

To configure certificates and keys for IPsec Tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a CA certificate and Certificate Revocation List (CRL). For more information, refer to "Adding a CA Certificate and CRL" (Page 218).
3. Add a private key. For more information, refer to "Adding a Private Key" (Page 220).
4. Add a certificate. For more information, refer to "Adding a Certificate" (Page 225).
5. Add a public key. For more information, refer to "Adding a Public Key" (Page 222).

6. Navigate to ***tunnel » ipsec » connection » { connection } » { end }***, where { connection } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end.
7. Configure the system public key by typing:

   ```
   tunnel ipsec connection { connection } [ left | right ]
   key type certificate
   ```

   Where:

   - `{ connection }` is the name of the connection
8. Configure the system identifier by typing:

   ```
   tunnel ipsec connection { connection } [ left | right ]
   identifier type from-certificate
   ```

   Where:

   - `{ connection }` is the name of the connection
9. Type `commit` and press **Enter** to save the changes.

12.8.4 Viewing the IPsec Tunnel Status

To view the status of the IPsec tunnel, type:

1. Make sure the CLI is in Configuration mode.
2. Display the status by typing:

   ```
   show tunnel ipsec status
   ```

   A table or list similar to the following example appears:

```
status
============================================================
000 using kernel interface: netkey
000 interface lo/lo :1
000 interface lo/lo 127.0.0.1
000 interface vrf_gw0/vrf_gw0 169.254.0.1
000 interface switch.0001/switch.0001 192.168.0.2
000 interface switch.1000/switch.1000 172.30.151.38
000 %myid = (none)
000 debug none
000
000 virtual_private (%priv):
000 - allowed 0 subnets:
000 - disallowed 0 subnets:
000 WARNING: Either virtual_private= is not specified, or there is a syntax
000          error in that line. 'left/rightsubnet=vhost:%priv' will not work!
000 WARNING: Disallowed subnets in virtual_private= is empty. If you have
000          private address space in internal use, it should be excluded!
000
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=8, keysizemin=64, key
sizemax=64
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=8, keysizemin=192, key
sizemax=192
000 algorithm ESP encrypt: id=11, name=ESP_NULL, ivlen=0, keysizemin=0, key
sizemax=0
```

```
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=8, keysizemin=128, key
sizemax=256
000 algorithm ESP encrypt: id=14, name=ESP_AES_CCM_A, ivlen=8, keysizemin=128,
 keysizemax=256
000 algorithm ESP encrypt: id=15, name=ESP_AES_CCM_B, ivlen=8, keysizemin=128,
 keysizemax=256
000 algorithm ESP encrypt: id=252, name=ESP_SERPENT, ivlen=8, keysizemin=128,
 keysizemax=256
000 algorithm ESP encrypt: id=253, name=ESP_TWOFISH, ivlen=8, keysizemin=128,
 keysizemax=256
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, key
sizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, key
sizemin=160, keysizemax=160
000 algorithm ESP auth attr: id=251, name=(null), keysizemin=0, keysizemax=0
000
000 algorithm IKE encrypt: id=0, name=(null), blocksize=16, keydeflen=131
000 algorithm IKE encrypt: id=3, name=OAKLEY_BLOWFISH_CBC, blocksize=8, keyde
flen=128
000 algorithm IKE encrypt: id=65289, name=OAKLEY_TWOFISH_CBC_SSH, block
size=16, keydeflen=128
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20
000 algorithm IKE hash: id=4, name=OAKLEY_SHA2_256, hashsize=32
000 algorithm IKE hash: id=6, name=OAKLEY_SHA2_512, hashsize=64
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
000
000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0}
 attrs={0,0,0}
000
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=RuggedCom,
 CN=router1, E=router1@example.com,+S=C]===192.168.11.0/24; erouted; eroute
 owner: #2
000 "ipsec-12":     myip=unset; hisip=unset; myup=ipsec _updown --route yes;
 hisup=ipsec _updown --route yes; mycert=router2;
000 "ipsec-12":   CAs: 'C=CA, ST=Ontario, O=RuggedCom, CN=CA, E=ca@exam
ple.com'...'%any'
000 "ipsec-12":   ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s;
 rekey_fuzz: 100%; keyingtries: 0
000 "ipsec-12":   policy: RSASIG+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+lKOD+rKOD;
 prio: 24,24; interface: switch.0012;
000 "ipsec-12":   newest ISAKMP SA: #4; newest IPsec SA: #2;
000 "ipsec-12":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048
000
000 #4: "ipsec-12":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE
 in 106s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin ini
tiate
000 #2: "ipsec-12":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVEN
T_SA_REPLACE in 19349s; newest IPSEC; eroute owner; isakmp#1; idle; import:ad
min initiate
000 #2: "ipsec-12" esp.edfbc8f8@192.168.12.1 esp.53ffca14@192.168.12.2
 tun.0@192.168.12.1 tun.0@192.168.12.2 ref=0 refhim=4294901761
000
```

12.8.5 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 548).

12.8.5.1 Viewing a List of Pre-Shared Keys

To view a list of pre-shared keys, type:

```
show running-config tunnel ipsec preshared-key
```

If pre-shared keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel ipsec preshared-key
tunnel
 ipsec
  preshared-key 192.168.12.1 192.168.12.2
   key $8$9YslfOBfkyYV8c1tqN4IDw==
  !
 !
!
```

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 553).

12.8.5.2 Adding a Pre-Shared Key

To add a pre-shared key, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the pre-shared key by typing:

   ```
   tunnel ipsec preshared-key [ { remote-address } | { lo
   cal-address } ] key { key }
   ```

   Where:

   - `{ remote-address }` is the remote IP address
   - `{ local-address }` is the local IP address
   - `{ key }` is the is the content of the pre-shared key
3. Configure the following parameter(s) as required:

Parameter	Description
`key { key }`	**Synopsis:** A string between 1 and 8192 characters long The pre-shared key.

4. Type `commit` and press **Enter** to save the changes.

12.8.5.3 Deleting a Pre-Shared Key

To delete a pre-shared key, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the pre-shared key by typing:

   ```
   no tunnel ipsec preshared-key [ { remote-address } | { lo
   cal-address } ] key { key }
   ```

   Where:

   - `{ remote-address }` is the remote IP address
   - `{ local-address }` is the local IP address
   - `{ key }` is the is the content of the pre-shared key

3. Type `commit` and press **Enter** to save the changes.

12.8.6 Managing Connections

An IPsec connection is an encrypted connection between two devices who share the same pre-authorized authentication key.

12.8.6.1 Viewing a List of Connections

To view a list of connections configured for a VPN, type:

```
show tunnel ipsec connection
```

If connections have been configured, a table similar to the following example appears:

```
ruggedcom# show running-config tunnel ipsec connection
tunnel
 ipsec
  connection ipsec-12
   no l2tp
   ike algorithm 3des md5 modp8192
   !
   esp algorithm aes128 sha1
   !
   left
    public-ip type default-route
    public-ip value 192.168.11.0/24
   !
   right
    public-ip type any
   !
  !
 !
!
```

If no connections have been configured, add connections as needed. For more information, refer to "Adding a Connection" (Page 555).

12.8.6.2 Adding a Connection

To add a new connection for a VPN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the connection by typing:

   ```
   tunnel ipsec connection { name }
   ```

   Where:

   - `{ name }` is the connection name. If the name is *default*, this makes it the default setting for all connections.
3. Configure the following parameter(s) as required:

Parameter	Description
`startup { startup }`	**Synopsis:** [ignore | add | start | route | default] **Default:** default The action to take when IPsec is initialized. The default value is 'ignore' unless overwritten by the default connection setting.
`authenticate { authenticate }`	**Synopsis:** [default | rsasig | secret] **Default:** default The authentication method. The default value is 'rsasig' unless overwritten by the default connection setting.
`connection-type { connection-type }`	**Synopsis:** [tunnel | transport | passthrough | default] **Default:** default The connection type/mode. Options include: • 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. • transport: Encrypts traffic on a host-to-host tunnel. • passthrough: Traffic is not encrypted.
`address-family { address-family }`	**Synopsis:** [ipv4 | ipv6] **Default:** ipv4 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.
`ike-version { ike-version }`	**Synopsis:** [v1 | v2] **Default:** v2 Option to determine which Internet Key Exchange (IKE) version to use. Options include: • v1: Use IKEv1. • v2: Use IKEv2.

4. If **authenticate** is set to **rsasig**, configure the following parameters:

Parameter	Description
`pfs { pfs }`	**Synopsis:** [default | yes | no] **Default:** default 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.
`keylife { keylife }`	**Synopsis:** [default] or An integer between 1081 and 86400 **Default:** default 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.
`ike-lifetime { ike-lifetime }`	**Synopsis:** [default] or An integer between 60 and 86400 **Default:** default 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.
`keyingtries { key ingtries }`	**Synopsis:** [default] or An integer equal to or greater than 1 **Default:** default 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.
`l2tp`	Enables/disables L2TP for this connection.
`connection-alarms { connection-alarms }`	**Synopsis:** [true | false] **Default:** false 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 **admin > alarm-cfg**.
`monitor-interface { monitor-interface }`	**Synopsis:** A string The interface to monitor. If the selected interface goes down and then up, this connection will be restarted.

5. If required, enable and configure dead peer detection. For more information, refer to "Configuring Dead Peer Detection" (Page 557).
6. 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 560).
7. If required, configure Encapsulated Security Payload (ESP) encryption for the connection. For more information, refer to "Managing the Encapsulated Security Payload (ESP) Protocol" (Page 561).
8. If required, configure the left (local router) and right (remote router) ends of the connection. For more information, refer to "Managing Connection Ends" (Page 563).
9. If required, configure L2TP tunnels. For more information, refer to "Configuring L2TP Tunnels" (Page 502).
10. If certificates and keys are required, make sure they are configured on the device. For more information, refer to "Configuring Certificates and Keys" (Page 550).
11. Type `commit` and press **Enter** to save the changes.

12.8.6.3 Configuring Dead Peer Detection

Dead Peer Detection (DPD), as defined in RFC 3706 [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. Make sure the CLI is in Configuration mode.
2. Enable dead peer detection by typing:

   ```
   tunnel ipsec connection { name } dead-peer-detect enabled
   [ true | false ]
   ```

   Where:

   - `{ name }` is the connection name.
3. Configure the following parameter(s) as required:

Note

The timeout period must be two minutes longer than the interval period.

Parameter	Description
`interval { interval }`	**Synopsis:** An integer between 1 and 3600 **Default:** 30 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.
`timeout { timeout }`	**Synopsis:** An integer between 1 and 28800 **Default:** 120 The time in seconds to wait before a peer is declared dead.
`action { action }`	**Synopsis:** [hold | clear | restart | restart-all-sa] **Default:** restart The action to be taken when a DPD enabled peer is declared dead. Options include: • hold: The route will be put on hold status. • clear: The route and Security Association (SA) will both be cleared • restart: The SA will immediately be renegotiated • restart-all-sa: All SA's to the dead peer will be renegotiated

4. Type `commit` and press **Enter** to save the changes.

12.8.6.4 Deleting a Connection

To delete a connection for a VPN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the connection by typing:

   ```
   no tunnel ipsec connection { name }
   ```

   Where:

   - `{ name }` is the name of the connection
3. Type `commit` and press **Enter** to save the changes.

12.8.6.5 Viewing the Status of a Connection

To view the status of an IPsec connection, type:

```
show tunnel ipsec connection { name } connection-status
```

Where { name } is the name of the connection. For example:

```
ruggedcom# show tunnel ipsec connection ipsec-12 connection-status
connection status "dead peer detect disabled"
```

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.

12.8.7 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.

12.8.7.1 Viewing a List of IKE Algorithms

To view a list of algorithms for the Internet Key Exchange (IKE) protocol, type:

```
show running-config tunnel ipsec connection { connection }
ike algorithm
```

Where:

- `{ connection }` is the name of the connection

If If algorithms have been configured, a table or list similar to the following example appears:

```
tunnel
 ipsec
  connection ipsec-12
   ike algorithm 3des md5 modp8192
   !
  !
 !
!
```

If no algorithms have been configured, add algorithms as needed. For more information, refer to "Adding an IKE Algorithm" (Page 560).

12.8.7.2 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. Make sure the CLI is in Configuration mode.
2. Add the algorithm by typing:

   ```
   tunnel ipsec connection { connection } ike algorithm { ci
   pher } { method } { modpgroup }
   ```

   Where:

   - `{ connection }` is the name of the connection.
   - `{ cipher }` is the cipher algorithm. Options include **3des**, **aes**, **aes128**, **aes192**, **aes256** and **any**.

     The default is **aes**.

     The option **any** selects the default.
   - `{ method }` is the hash method. Options include **any**, **md5**, **sha1** and **sha2**.

     The default is **sha2**.

     The option **any** selects the default.
   - `{ modpgroup }` is the value of the Modular Exponential (MODP) group. Options include **any**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144** and **modp8192**.

     The default is **modp2048**.

     The option **any** selects the default.
3. Type `commit` and press **Enter** to save the changes.

12.8.7.3 Deleting an IKE Algorithm

To delete an algorithm for the Internet Key Exchange (IKE) protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the algorithm by typing:

   ```
   no tunnel ipsec connection { connection } ike algorithm
   { cipher } { method } { modpgroup }
   ```

   Where:

- `{ connection }` is the name of the connection.
- `{ cipher }` is the cipher algorithm. Options include **3des**, **aes**, **aes128**, **aes192**, **aes256** and **any**.
- `{ method }` is the hash method. Options include **any**, **md5**, **sha1** and **sha2**.
- `{ modpgroup }` is the value of the Modular Exponential (MODP) group. Options include **any**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144**, **modp8192**, **dh19**, **dh20**, and **dh21**.

3. Type `commit` and press **Enter** to save the changes.

12.8.8 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.

12.8.8.1 Configuring ESP Encryption

To configure the encryption algorithm for the Encapsulate Security Payload (ESP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection » { connection } » esp***, where { connection } is the name of the connection.
3. Configure the encryption algorithm by typing:

```
tunnel ipsec connection { connection } esp modpgroup
{ modpgroup }
```

Where:

- `{ connection }` is the name of the connection.
- `{ modpgroup }` is the Modular Exponential (MODP) group. Options include **any**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144** and **modp8192**. The default is **modp2048** depending on the default connection setting. The option **any** selects the default.

4. If required, add additional cipher algorithms. For more information on how to add algorithms, refer to "Adding an ESP Algorithm" (Page 562).
5. Type `commit` and press **Enter** to save the changes.

12.8.8.2 Viewing a List of ESP Algorithms

To view a list of algorithms for the Encapsulate Security Payload (ESP) protocol, type:

```
show running-config tunnel ipsec connection { connection }
esp algorithm
```

Where:

- `{ connection }` is the name of the connection

If algorithms have been configured, a table or list similar to the following example appears:

```
tunnel
 ipsec
  connection ipsec-12
   esp algorithm aes256 sha1
   !
  !
 !
!
```

If no algorithms have been configured, add algorithms as needed. For more information, refer to "Adding an ESP Algorithm" (Page 562).

12.8.8.3 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. Make sure the CLI is in Configuration mode.
2. Add the algorithm by typing:

   ```
   tunnel ipsec connection { connection } esp algorithm { ci
   pher } { method }
   ```

   Where:

   - `{ connection }` is the name of the connection.
   - `{ cipher }` is the cipher algorithm. Options include **3des**, **aes**, **aes128**, **aes192**, **aes256** and **any**.

     The default is **aes**.

The option **any** selects the default.

- `{ method }` is the hash method. Options include **any**, **md5**, **sha1** and **sha2**.

  The default is **sha1** for IKEv1. There is no default for IKEv2.

  The option **any** selects the default.

3. Type `commit` and press **Enter** to save the changes.

12.8.8.4 Deleting an ESP Algorithm

To delete an algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the algorithm by typing:

   ```
   no tunnel ipsec connection { connection } esp algorithm
   { cipher } { method }
   ```

   Where:

   - `{ connection }` is the name of the connection
   - `{ cipher }` is the cipher algorithm. Options include **3des**, **aes**, **aes128**, **aes192**, **aes256** and **any**. The default is **aes**. The option **any** selects the default.
   - `{ method }` is the hash method. Options include **any**, **md5**, **sha1** and **sha2**. The default is **sha1**. The option **any** selects the default.
3. Type `commit` and press **Enter** to save the changes.

12.8.9 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.

12.8.9.1 Configuring the Public IP Address for a Connection End

To configure the public IP address for a connection end, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***tunnel » ipsec » connection » { name } » { end } » public-ip***, where { name } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end.
3. Configure the following parameters:

⚠ NOTICE
Do not use a Virtual IP Address (VRIP) as the connection's public IP address if **use-virtual-mac** is enabled under VRRP.

Parameter	Description
`type { type }`	**Synopsis:** [none | default-route | any | address | hostname] **Default:** none The public IP address type.
`value { value }`	**Synopsis:** A string up to 1024 characters long The public hostname or IP address.

4. Type `commit` and press **Enter** to save the changes.

12.8.9.2 Configuring the System Public Key for a Connection End

To configure the system public key for a connection end, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection » { name } » { end } » key***, where { name } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end.
3. Configure the following parameter:

Parameter	Description
`type { type }`	**Synopsis:** [none | rsasig | certificate-any | certificate | ca-certificate] **Default:** none Key type.

4. If **rsasig** is the selected key type, configure the following parameters:

Parameter	Description
`rsa-sig { rsa-sig }`	**Synopsis:** A string between 1 and 255 characters long The RSA signature key name.
`rsa-sig-ipsec`	**Synopsis:** A string between 1 and 8192 characters long The RSA signature in IPsec format.

5. If **certificate** is the selected key type, configure the following parameters:

Parameter	Description
`certificate { certificate }`	**Synopsis:** 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 { ca-certificate }`	**Synopsis:** A string between 1 and 255 characters long The selected CA certificate.

7. Type `commit` and press **Enter** to save the changes.

12.8.9.3 Configuring the System Identifier for a Connection End

To configure the system identifier for a connection end, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection » { name } » { end } » identifier***, where { name } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end.
3. Configure the system identifier by configuring the following parameters:

Parameter	Description
`type { type }`	**Synopsis:** [default | none | from-certificate | address | hostname | der-asn1-dn | user-fqdn] **Default:** default The system identifier type. The default value is 'left side public-ip' unless overwritten by the default connection setting.
`value { value }`	**Synopsis:** A string up to 1024 characters long The hostname, IP address or the Distinguished Name in the certificate.

4. Type `commit` and press **Enter** to save the changes.

12.8.9.4 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection » { name } » { end } » nexthop***, where { name } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end.

3. Configure the following parameters:

Parameter	Description
`type { type }`	**Synopsis:** [default | default-route | address] **Default:** default The next hop type. The default value is 'right side public-ip' unless overwritten by the default connection setting.
`value { value }`	**Synopsis:** 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. Type `commit` and press **Enter** to save the changes.

12.8.9.5 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection » { name } » { end } » nexthop***, where { name } is the name of the connection and { end } is the either the left (local router) or right (remote router) connection end.
3. Configure the following parameters:

Parameter	Description
`nat-traversal-negotiation { nat-traversal-negotiation }`	**Synopsis:** [default | draft-ietf-ipsec-nat-t-ike-02 | rfc-3947] **Default:** 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 ID_FQDN: '@example.com', but when a Vista, Windows 7 or other RFC 3947 compliant client connects, Libreswan reports the main mode peer ID is ID_IPV4_ADDR: '192.168.1.1'. This will cause issues connecting to the IPsec server. In such cases, setting this option to draft-ietf-ipsec-nat-

Parameter	Description
	t-ike-02 will solve this problem. The default value is 'rfc-3947' unless overwritten by the default connection setting.

4. Type `commit` and press **Enter** to save the changes.

12.8.10 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.

12.8.10.1 Viewing a List of Addresses for Private Subnets

To view a list of IP addresses configured for private subnets, type:

```
show running-config tunnel ipsec connection { name } [ right
| left ] subnet
```

Where:

- `{ name }` is the name of the connection

If IP addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel ipsec connection ipsec-12 left subnet
tunnel
 ipsec
  connection ipsec-12
   left
    subnet 192.168.11.0/24
    !
   !
  !
 !
!
```

If no IP addresses have been configured, add addresses as needed. For more information, refer to "Adding an Address for a Private Subnet" (Page 567).

12.8.10.2 Adding an Address for a Private Subnet

To add an IP address for a private subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the IP address and prefix by typing:

   ```
   tunnel ipsec connection { name } [ right | left ] subnet
   { address }
   ```

Where:

- `{ name }` is the name of the connection
- `{ address }` is the IP address and prefix of the private subnet

3. Type `commit` and press **Enter** to save the changes.

12.8.10.3 Deleting an Address for a Private Subnet

To delete an IP address for a private subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the IP address by typing:

```
no tunnel ipsec connection { name } [ right | left ] sub
net { address }
```

Where:

- `{ name }` is the name of the connection
- `{ address }` is the IP address and prefix of the private subnet

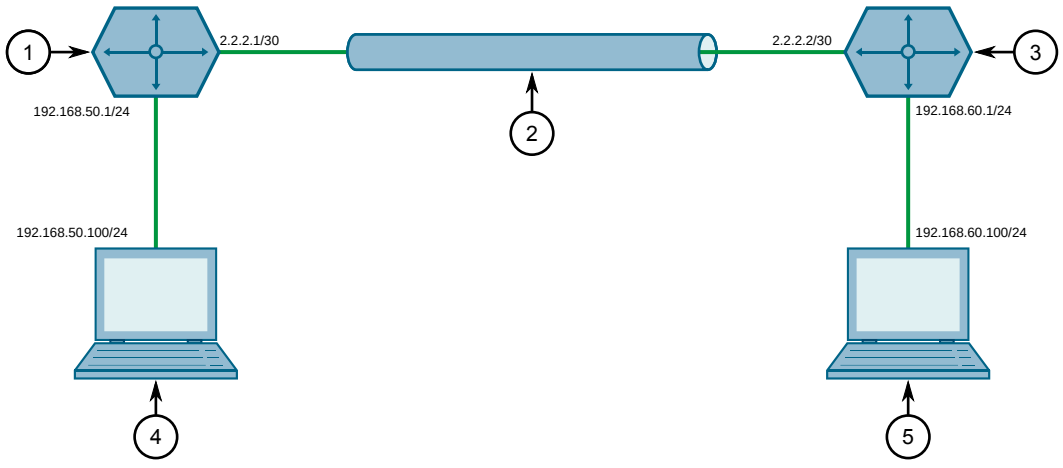
3. Type `commit` and press **Enter** to save the changes.

12.8.11 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.



① Device A
② IPsec Encrypted VPN Tunnel
③ Device B
④ Client 1
⑤ Client 2

Figure 12.8 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 555).
2. Configure Device A:
   a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 139).
   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 553).
   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 555).
   d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 560).
   e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 562).
   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 563).
   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 567).

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 563).

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 567).

3. Configure Device B:

a. Configure a host name for the device. For more information, refer to "Configuring the Host Name" (Page 139).

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 553).

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 555).

d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to "Adding an IKE Algorithm" (Page 560).

e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to "Adding an ESP Algorithm" (Page 562).

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 563).

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 567).

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 563).

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 567).

4. Enable the IPsec tunnel. For more information, refer to "Configuring IPsec Tunnels" (Page 549).
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 551).

   b. Capture the packets using Tcpdump on one of the tunnel interfaces. Encrypted traffic will display an *ESP* header. For more information about using the Tcpdump utility, refer to "Capturing Packets from a Network Interface" (Page 29).

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
```

12.9 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 267).

12.9.1 Enabling/Disabling 6in4 or 4in6 Tunnels

To enable or disable all 6in4 or 4in6 tunnels, do the following:

1. Make sure the CLI is in Configuration mode.

2. Enable or disable 6in4/4in6 tunnels by typing:

   Enabling

   ```
   tunnel [ ip6in4 | ip4in6 ] enabled
   ```

   Disabling

   ```
   no tunnel [ ip6in4 | ip4in6 ] enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

12.9.2 Viewing a List of 6in4 or 4in6 Tunnels

To view a list of 6in4 or 4in6 tunnels configured on the device, type:

```
show running-config tunnel [ ip6in4 | ip4in6 ] tunnel
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel ip6in4 tunnel | tab
NAME       ENABLED  LOCAL IP       REMOTE IP     MTU
-----------------------------------------------------
ruggedcom  true     192.168.30.14  172.23.30.14  1480

!
```

12.9.3 Viewing the Status of 6in4/4in6 Tunnels

To view the status of a 6in4 or 4in6 tunnel, type:

```
show interfaces [ ip6in4 | ip4in6 ] tunnel { name }
```

Where:

- `{ name }` is the name of the tunnel

A table or list similar to the following example appears:

```
ruggedcom# show interfaces ip6in4 tunnel
TUNNEL
NAME    LOCAL IP       REMOTE IP      STATUS
-----------------------------------------------
tu      192.168.20.10  192.168.20.20  Active
```

12.9.4 Adding a 6in4 or 4in6 Tunnel

To add a 6in4 or 4in6 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the tunnel by typing:

   ```
   tunnel [ ip6in4 | ip4in6 ] tunnel { name }
   ```

   Where:

   - `{ name }` is the name of the tunnel

3. Configure the following parameter(s) as required:

Parameter	Description
`{ name }`	**Synopsis:** A string between 1 and 11 characters long The tunnel name. May contain any lower case letter or numerical digit. The prefix 't64' or 't46-' is added automatically to create the iptunnel system interface name (ie. t64-location123)
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/disables the tunnel
`local-ip { local-ip }`	**Synopsis:** A string between 7 and 15 characters long The IP address of the local tunnel endpoint
`remote-ip { re mote-ip }`	**Synopsis:** A string between 7 and 15 characters long The IP address of the remote tunnel endpoint
`mtu { mtu }`	**Synopsis:** An integer between 68 and 1480 **Default:** 1480 The Maximum Transmission Unit (MTU) of the network interface

4. Type `commit` and press **Enter** to save the changes.

12.9.5 Deleting a 6in4 or 4in6 Tunnel

To delete a 6in4 or 4in6 tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tunnel by typing:

   ```
   no tunnel [ ip6in4 | ip4in6 ] tunnel { name }
   ```

   Where:

   - `{ name }` is the name of the tunnel

3. Type `commit` and press **Enter** to save the changes.

12.10 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.

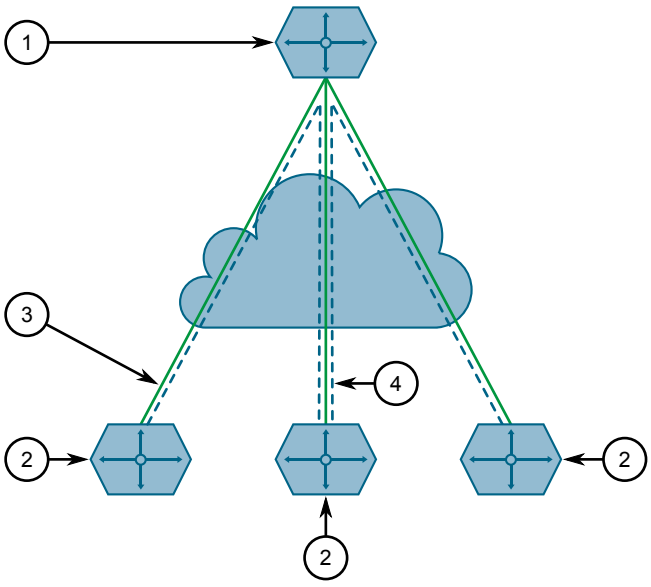
12.10.1 Understanding DMVPN

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.

DMPVN can be deployed in one of two ways.

- Hub-and-Spoke
- Spoke-to-Spoke

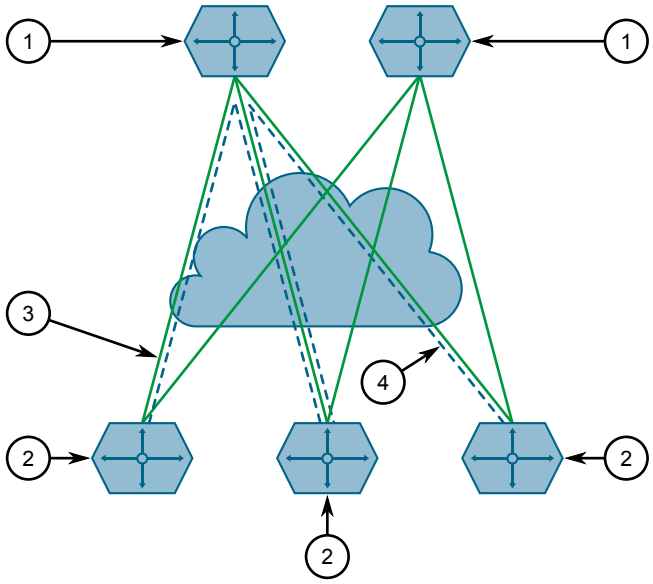
RUGGEDCOM ROX II supports hub-and-spoke deployments where a central router (the hub) uses Multipoint Generic Routing Encapsulation (mGRE) to establish GRE tunnels with one or more routers (the spokes). When spokes need to send traffic to one another, they send it to the hub first and the hub directs 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 12.9 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 12.10 Hub-and-Spoke Topology – Dual Hub

12.10.2 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 536).
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 549).
4. Configure a BGP route for the GRE tunnel. For more information, refer to "Configuring BGP" (Page 626).
5. Enable the DMVPN service by typing:

```
services nhrp enabled
```

Note

RUGGEDCOM ROX II supports up to two DMVPN interfaces, each of which can be assigned to different GRE tunnels.

6. Configure a DMVPN interface for each GRE tunnel. For more information, refer to "Adding a DMVPN Interface" (Page 577).
7. Configure an IPsec/GRE tunnel from the hub to the device, using the IP address defined for the device's DMVPN interface.
8. Verify the status of the DMVPN connection. For more information, refer to "Viewing the Status of DMVPN" (Page 579).

12.10.3 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.

12.10.3.1 Viewing a List of DMVPN Interfaces

To view a DMVPN interfaces, type:

```
show running-config services nhrp interface-nhrp
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services nhrp interface-nhrp | tab
IFNAME  ENABLED  ADDRESS           HOLDTIME  AUTHENTICATION  KEY
-------------------------------------------------------------------------------------
gre-t1  true     192.168.0.100/24  10        cisco           $4$wocla9w68FRwhYYI0d4IDw==

 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a DMVPN Interface" (Page 577).

12.10.3.2 Adding a DMVPN Interface

To add a DMVPN interface, do the following:

1. Add the interface for the desired GRE tunnel by typing:

   ```
   services nhrp interface-nhrp { gre-tunnel }
   ```

   Where `{ gre-tunnel }` is the name of the desired GRE tunnel.
2. 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 { address }`	**Synopsis:** A string between 9 and 18 characters long IPv4 address of remote GRE interface to be used for this NHRP session.
`holdtime { holdtime }`	**Synopsis:** An integer **Default:** 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 { au thentication }`	**Synopsis:** [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 { key }`	**Synopsis:** A string The authentication key to allow intercommunication between source and destination NHRP nodes. Maximum length is 8 characters.

3. Type `commit` and press **Enter** to save the changes.

12.10.3.3 Deleting a DMVPN Interface

To delete a DMVPN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address pool by typing:

   ```
   no services nhrp interface-nhrp { gre-tunnel }
   ```

   Where `{ gre-tunnel }` is the name of the desired GRE tunnel.
3. Type `commit` and press **Enter** to save the changes.

12.10.4 Viewing the Status of DMVPN

To view the status of the DMVPN service, type:

```
show services nhrp status
```

If DMVPN interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show services nhrp status
ROW  RAW FROM OPENNHRPCTL
--------------------------------------
0
1    Status: ok
2
3    Interface: gre-gre-1
4    Type: local
5    Protocol-Address: 192.168.0.1/32
6    Flags: up
7
8    Status: ok
9
10   Interface: gre-gre-1
11   Type: static
12   Protocol-Address: 192.168.0.2/24
13   NBMA-Address: 61.1.1.2
14   Flags: up
15
16   Status: ok
17
18   Interface: gre-gre-2
19   Type: local
20   Protocol-Address: 192.168.1.1/32
21   Flags: up
22
23   Status: ok
24
25   Interface: gre-gre-2
26   Type: static
27   Protocol-Address: 192.168.1.2/24
28   NBMA-Address: 71.1.1.2
29   Flags: up
30
```

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: • `shortcut-route` – Received or relayed resolution for the route • `incomplete` – Resolution request sent but no reponse received yet • `negative` – Negative cached	Type: local

Field	Description	Example
	• `cached` – Received or relayed resolution • `dynamic` – NHC registration • `dynamic-nhs` – Dynamic NHS from DNS map • `static` – Static map from the configuration file • `static-dns` – Static DNS map from the configuration file • `local-route` – Non-local destination, with local route • `local` – Local destination, IP or off-NBMA subnet	
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: • `unique` – The NHRP peer is unique. Its NRHP mapping entry cannot be overwritten by a mapping entry with the same IP address, even if the associated peer has a different NBMA address. • `used` – The NHRP peer is in the kernel ARP table. • `up` – A connection with the NHRP peer has been established and the link is up. • `lower-up` – A connection with the NHRP peer has been established.	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 **holdtime** is configured.	Expires-in: 120
Hostname	The host name of the NBMA responder, when available.	Hostname: ruggedcom

13 Unicast and Multicast Routing

This chapter describes how to configure, monitor and manage static and dynamic routes unicast and multicast traffic.

13.1 Viewing the Status of IPv4 Routes

To view the status of the IPv4 routes configured on the device, type:

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.

```
show routing status ipv4routes
```

If IPv4 routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ipv4routes
DESTINATION     GATEWAY  INTERFACE    TYPE    WEIGHT  METRIC
-------------------------------------------------------------
192.168.0.0/24           switch.0001  kernel
```

The following information is provided:

Parameter	Description
`destination`	**Synopsis:** A string The network/prefix.
`gateway`	**Synopsis:** A string The gateway address.
`interface`	**Synopsis:** A string The interface name.
`type`	**Synopsis:** A string The route type.
`weight`	**Synopsis:** A string The route weight.

Parameter	Description
metric	**Synopsis:** 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 269).

13.2 Viewing the Status of IPv6 Routes

To view the status of the IPv6 routes configured on the device, type:

```
show routing status ipv6routes
```

If IPv6 routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ipv6routes
DESTINATION  GATEWAY  INTERFACE    TYPE    WEIGHT  METRIC
------------------------------------------------------------
fe80:/64             switch       kernel          256
fe80:/64             dp1          kernel          256
fe80:/64             vrf_lo       kernel          256
fe80:/64             switch.0001  kernel          256
fe80:/64             fe-cm-1      kernel          256
fe80:/64             switch.4094  kernel          256
ff00:/8              switch                       256
ff00:/8              dp1                          256
ff00:/8              vrf_lo                       256
ff00:/8              switch.0001                  256
ff00:/8              fe-cm-1                      256
ff00:/8              switch.4094                  256
```

The following information is provided:

Parameter	Description
destination	**Synopsis:** A string The network/prefix.
gateway	**Synopsis:** A string The gateway address.
interface	**Synopsis:** A string The interface name.
type	**Synopsis:** A string The route type.
weight	**Synopsis:** A string The route weight.

Parameter	Description
metric	**Synopsis:** 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 745).

13.3 Viewing the Memory Statistics

To view statistics related to the Core, RIP, OSPF and BGP daemons, type:

```
show routing status memory
```

A list similar to the following example appears:

```
ruggedcom# show routing status memory
routing status memory
 zebra
  total 405504
  used  359424
  free  46080
 rip
  total 0
  used  0
  free  0
 ospf
  total 0
  used  0
  free  0
 bgp
  total 0
  used  0
  free  0
```

The following information is provided:

Parameter	Description
total	**Synopsis:** An integer The total heap allocated (in bytes).
used	**Synopsis:** An integer The number of used ordinary blocks (in bytes).
free	**Synopsis:** An integer The number of free ordinary blocks (in bytes).

13.4 Configuring ICMP

To configure how RUGGEDCOM ROX II manages ICMP redirect messages, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin*** and 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 { ignore-icmp-all }`	**Synopsis:** [true | false] **Default:** false Ignores all ICMP echo requests sent to it.
`ignore-icmp-broadcast { ignore-icmp-broadcast }`	**Synopsis:** [true | false] **Default:** true Ignores all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast.
`send-icmp-redirect { send-icmp-redirect }`	**Synopsis:** [true | false] **Default:** true Sends the ICMP redirect.

3. Type `commit` and press **Enter** to save the changes.

13.5 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.

13.5.1 Viewing a List of Event Trackers

To view a list of event trackers, type:

```
show running-config global tracking
```

If event trackers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config global tracking
global
 tracking
  event host-in-lan-11
   target   192.168.11.100
   timeout  500
   interval 500
   fall     3
   rise     3
  !
 !
!
```

If no event trackers have been configured, add event trackers as needed. For more information, refer to "Adding an Event Tracker" (Page 586).

13.5.2 Viewing Event Tracker Statistics

RUGGEDCOM ROX II records statistics for each event tracker.

To view the statistics for an event tracker, type:

```
show global tracking event statistics
```

A list similar to the following example appears:

```
ruggedcom# show global tracking event statistics
                                                        STANDARD
                ECHO      ECHO     MIN  AVERAGE  MAX  DEVIATION
NAME            ATTEMPTS  REPLIES  RTT  RTT      RTT  RTT
-------------------------------------------------------------------
host-in-lan-11  0         0        0.0  0.0      0.0  0.0
```

This list provides the following information:

Parameter	Description
`echo-attempts`	**Synopsis:** An integer The number of echo attempts.

Parameter	Description
`echo-replies`	**Synopsis:** An integer The number of echo replies.
`min-rtt`	**Synopsis:** A string The minimum of the round trip time (in milliseconds).
`average-rtt`	**Synopsis:** A string The average of the round trip time (in milliseconds).
`max-rtt`	**Synopsis:** A string The maximum of the round trip time (in milliseconds).
`standard-deviation-rtt`	**Synopsis:** A string The standard deviation of the round trip time (in milliseconds).

13.5.3 Adding an Event Tracker

To add an event tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the event tracker by typing:

   ```
   global tracking event { name }
   ```

   - `{ name }` is the name of the tracking event
3. Configure the following parameter(s) as required:

Parameter	Description
`target { target }`	**Synopsis:** A string between 1 and 253 characters long Configures the ping target as an IPv4 address or hostname.domain.
`source-ip { source-ip }`	**Synopsis:** 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 { source-interface }`	**Synopsis:** A string Forces a ping on a selected interface.
`timeout { timeout }`	**Synopsis:** An integer Determines how many milliseconds to wait for the ICMP response.
`interval { interval }`	**Synopsis:** An integer equal to or greater than 100 Determines how many milliseconds to wait before sending another ICMP request.

Parameter	Description
`fall { fall }`	**Synopsis:** 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 { rise }`	**Synopsis:** An integer equal to or greater than 1 The number of times success occurs before changing the tracking state from down to up.
`state`	**Synopsis:** [up | down] **Default:** up The state of the event.

4. Type `commit` and press **Enter** to save the changes.

13.5.4 Deleting an Event Tracker

To delete an event tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the event tracker by typing:

   ```
   no global tracking event { name }
   ```

   - `{ name }` is the name of the tracking event
3. Type `commit` and press **Enter** to save the changes.

13.6 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]).

13.6.1 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]. 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.

13.6.1.1 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.

13.6.1.2 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]). 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)
```

13.6.1.3 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 it's 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
- 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

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

13.6.2 Configuring IS-IS

To configure dynamic routing with IS-IS, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable IS-IS by typing:

   ```
   routing isis enabled
   ```

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 592).
4. Configure one or more interfaces on which to perform IS-IS routing. For more information, refer to "Managing Interfaces" (Page 595).
5. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

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.

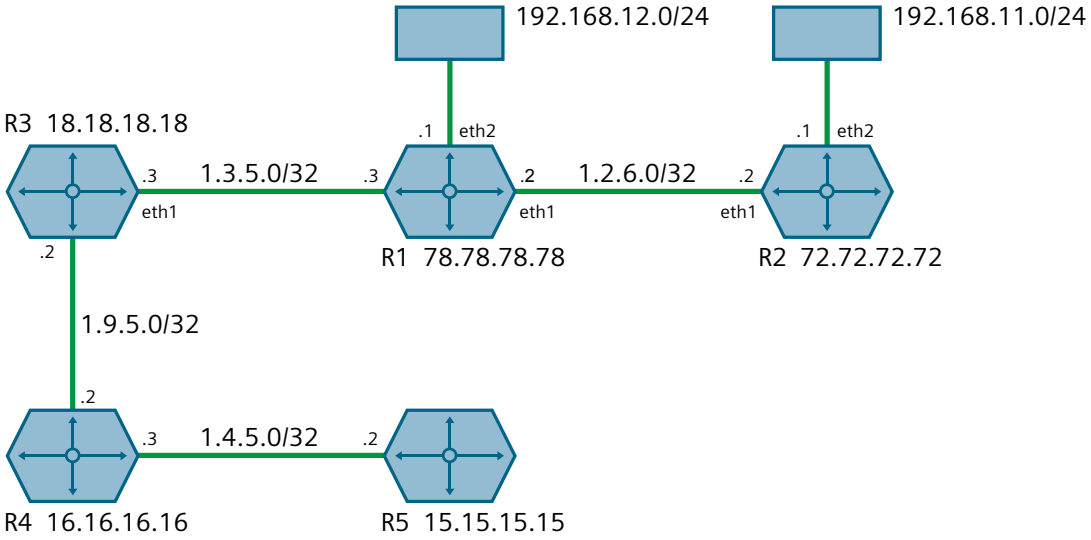


Figure 13.1 Multi-Level IS-IS Configuration

13.6.3 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 589).
2. View the status by typing:

   ```
   routing status isis isis-neighbors-status
   ```

   If IS-IS routes have been configured, a table similar to the following example appears:

   ```
   ruggedcom# routing status isis isis-neighbors-status
   isis-neighbors-status
   Area area1:

     System Id           Interface   L  State        Holdtime SNPA

     Spirent-            switch.0012 3  Up           24       2020.2020.2020
   ```

   This table displays the following information:

Parameter	Description
`System ID`	The system ID.
`Interface`	The name of the interface.

Parameter	Description
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).

13.6.4 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 589).
2. Display the basic status by typing:

   ```
   routing status isis isis-database-status
   ```

   Or display a more detailed status by typing:

   ```
   routing status isis isis-database-detail-status
   ```

   If IS-IS routes have been configured, a list similar to the following example appears:

```
ruggedcom# routing status isis isis-database-status
isis-database-status
Area area1:

IS-IS Level-1 link-state database:

LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL

R1.00-00             *     75   0x00000015  0xe43a    1129    0/0/0

    1 LSPs


IS-IS Level-2 link-state database:

LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL

Spirent-.00-00            121   0x0000000f  0xd5e6     871    0/0/0

R1.00-00             *     75   0x00000015  0xe636    1031    0/0/0

Spirent-right.00-00      1465   0x0000000f  0x3d65     871    0/0/0

Spirent-right.00-01       295   0x0000000f  0x6a0d     872    0/0/0

Spirent-right.00-00      1465   0x0000000f  0x4638     872    0/0/0

Spirent-right.00-01       287   0x0000000f  0x54d0     872    0/0/0
```

```
Spirent-right.00-00      1462   0x0000000f  0x6528     872    0/0/0
Spirent-right.00-01       269   0x0000000f  0x7e8a     872    0/0/0
Spirent-right.00-00      1463   0x0000000f  0x99a0     872    0/0/0
Spirent-right.00-01       261   0x0000000f  0xb0d2     872    0/0/0
Spirent-right.00-00      1460   0x0000000f  0x80c6     872    0/0/0
Spirent-right.00-01       253   0x0000000f  0x97fb     872    0/0/0
Spirent-right.00-00      1460   0x0000000f  0x1137     872    0/0/0
Spirent-right.00-01       237   0x0000000f  0x0db7     872    0/0/0
    14 LSPs
```

This list displays the following information:

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.

13.6.5 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.

13.6.5.1 Viewing a List of Area Tags

To view a list of area tags configured for dynamic IS-IS routes, type:

```
show running-config routing isis area
```

If area tags have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area
routing isis
 area Area_1
  is-type               level-1-2
  metric-style          narrow
  area-authorization    md5
  area-password         admin
  area-authentication   validate
  domain-authorization  md5
  domain-password       admin
  domain-authentication validate
  net 49.0001.1921.6800.1001.00
  !
  redistribute bgp
   is-type     level-1-2
   metric-type internal
   metric      10
  !
  lsp-gen-interval is-type level-1-only
   interval 60
  !
  lsp-refresh-interval is-type level-1-2
   interval 20
  !
  max-lsp-lifetime is-type level-2-only
   interval 10
  !
  spf-interval is-type level-1-2
   interval 5
  !
 !
!
```

If no area tags have been configured, add area tags as needed. For more information, refer to "Adding an Area Tag" (Page 593).

13.6.5.2 Adding an Area Tag

To add an area tag for dynamic IS-IS routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the area by typing:

   ```
   routing isis area { name }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
3. Configure the following parameter(s) as required:

Parameter	Description
`is-type { is-type }`	**Synopsis:** [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-

Parameter	Description
	only (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
`metric-style { metric-style }`	**Synopsis:** [narrow | transition | wide] **Default:** wide The metric style Type Length Value (TLV) for this area: narrow, transition or wide. Default is wide.
`area-authorization { area-authorization }`	**Synopsis:** [clear | md5] **Default:** clear The authorization type for the area password. Default is clear.
`area-password { area-password }`	**Synopsis:** A string up to 254 characters long The area password to be used for transmission of level-1 LSPs.
`area-authentication { area-authentication }`	**Synopsis:** [send-only | validate] **Default:** send-only The authentication option to be used with the area password on SNP PDUs. Default is send-only.
`domain-authorization { domain-authorization }`	**Synopsis:** [clear | md5] **Default:** clear The authorization type for the domain password. Default is clear.
`domain-password { domain-password }`	**Synopsis:** A string up to 254 characters long The domain password to be used for transmission of level-2 LSPs.
`domain-authentication { domain-authentication }`	**Synopsis:** [send-only | validate] **Default:** send-only The authentication option to be used with the domain password on SNP PDUs. Default is send-only.

4. Add one or more Network Entity Titles (NETs). For more information, refer to "Managing Network Entity Titles (NETs)" (Page 604).
5. 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 597).
6. 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 602).
7. If necessary, configure the minimum interval between consecutive SPF calculations. The default is 1 second. For more information, refer to "Managing SPF Calculations" (Page 599).

8. 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 600).
9. If necessary, define rules for redistributing static, RIP, BGP or OSPF routes. For more information, refer to "Managing Redistribution Metrics" (Page 606).
10. Type `commit` and press **Enter** to save the changes.

13.6.5.3 Deleting an Area Tag

To delete an area tag for dynamic IS-IS routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the area tag by typing:

   ```
   no routing isis area { name }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
3. Type `commit` and press **Enter** to save the changes.

13.6.6 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.

13.6.6.1 Viewing a List of Interfaces

To view a list of interfaces for dynamic IS-IS routes, type:

```
show running-config routing isis interface
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis interface | tab
             IPV4                  POINT
             AREA                  TO              CIRCUIT   CIRCUIT                CSNP      HELLO
   HELLO       PSNP
IFNAME       TAG     CIRCUIT TYPE  POINT  PASSIVE  PASSWORD  AUTHORIZATION  METRIC  INTERVAL  INTER
VAL  MULTIPLIER  INTERVAL
-------------------------------------------------------------------------------------
fe-cm-1      Area_1  level-1-2     true   true     admin     md5            10      10        3
   10          2
```

```
switch.0001  Area_2  level-1-only  false  true     admin     clear          10      10        3
   10          2

!
```

Interfaces are added automatically when a VLAN is created. For more information about creating a VLAN, refer to "Managing VLANs" (Page 374).

13.6.6.2 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. Make sure the CLI is in Configuration mode.
2. Navigate to the interface by typing:

   ```
   routing isis interface { name }
   ```

   Where:

   - `{ name }` is the name of the interface. If the desired interface is not available, it must be created as a VLAN. For more information about creating a VLAN, refer to "Managing VLANs" (Page 374).
3. Configure the following parameter(s) as required:

Parameter	Description
`ipv4-area-tag { ipv4-area-tag }`	**Synopsis:** A string up to 64 characters long Name of Area Tag to be used for IS-IS over IPv4.
`circuit-type { circuit-type }`	**Synopsis:** [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 { point-to-point }`	**Synopsis:** [true | false] **Default:** false Enable or disable point-to-point network communication
`passive { passive }`	**Synopsis:** [true | false] **Default:** 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 { circuit-password }`	**Synopsis:** A string up to 254 characters long The value to be used as a transmit password in IIH PDUs transmitted by this Intermediate System.

Parameter	Description
`circuit-authorization { circuit-authorization }`	**Synopsis:** [clear | md5] **Default:** clear The authorization type ot be associated with the transmit password in IIH PDUs transmitted by this Intermediate System.
`metric { metric }`	**Synopsis:** An integer between 1 and 16777214 **Default:** 10 Metric assigned to the link, used to calculate the cost of the route. Value ranges from 1 to 16777214. Default is 10.
`csnp-interval { csnp-interval }`	**Synopsis:** An integer between 1 and 600 **Default:** 10 CSNP interval in seconds, ranging from 1 to 600. Default is 10.
`hello-interval { hello-interval }`	**Synopsis:** An integer between 1 and 600 **Default:** 3 Hello interval in seconds, ranging from 1 to 600. Default is 3.
`hello-multiplier { hello-multiplier }`	**Synopsis:** An integer between 2 and 100 **Default:** 10 Multiplier for Hello holding time. Value ranges from 2 to 100. Default is 10.
`psnp-interval { psnp-interval }`	**Synopsis:** An integer between 1 and 120 **Default:** 2 PSNP interval in seconds, ranging from 1 to 120. Default is 2.

4. Type `commit` and press **Enter** to save the changes.

13.6.7 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.

13.6.7.1 Viewing a List of LSP Generation Intervals

To view a list of LSP generation intervals configured for an IS-IS area, type:

```
show running-config routing isis area { name } lsp-gen-interval
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.

If intervals have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area Area_1 lsp-gen-interval | tab
ISTYPE        INTERVAL
-----------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an LSP Generation Interval" (Page 598).

13.6.7.2 Adding an LSP Generation Interval

To add an LSP generation interval to an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

   ```
   routing isis area { name } lsp-gen-interval is-type [ lev
   el-1-2 | level-1-only | level-2-only ] interval { sec
   onds }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ level }` is the IS type.
   - `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type `commit` and press **Enter** to save the changes.

13.6.7.3 Deleting an LSP Generation Interval

To delete an LSP generation interval for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the LDP interface by typing:

   ```
   no routing isis area { name } lsp-gen-interval is-type
   [ level-1-2 | level-1-only | level-2-only ] interval
   { seconds }
   ```

   Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.
- `{ level }` is the IS type.
- `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.

3. Type `commit` and press **Enter** to save the changes.

13.6.8 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.

13.6.8.1 Viewing a List of SPF Calculation Intervals

To view a list of SPF calculation intervals configured for an IS-IS area, type:

```
show running-config routing isis area { name } spf-interval
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.

If intervals have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area Area_1 spf-interval | tab
ISTYPE        INTERVAL
-----------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an SPF Calculation Interval" (Page 599).

13.6.8.2 Adding an SPF Calculation Interval

To add an SPF calculation interval to an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add a new interval by typing:

   ```
   routing isis area { name } spf-interval is-type [ lev
   el-1-2 | level-1-only | level-2-only ] interval { sec
   onds }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ level }` is the IS type.
   - `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.

3. Type `commit` and press **Enter** to save the changes.

13.6.8.3 Deleting an SPF Calculation Interval

To delete an SPF calculation interval for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the LDP interface by typing:

   ```
   no routing isis area { name } spf-interval is-type [ lev
   el-1-2 | level-1-only | level-2-only ] interval { sec
   onds }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ level }` is the IS type.
   - `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.

3. Type `commit` and press **Enter** to save the changes.

13.6.9 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.

Th 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 602).

13.6.9.1 Viewing a List of LSP Lifetime Intervals

To view a list of LSP lifetime intervals configured for an IS-IS area, type:

```
show running-config routing isis area { name } max-lsp-life
time
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.

If intervals have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area Area_1 max-lsp-lifetime | tab
ISTYPE        INTERVAL
------------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an LSP Lifetime Interval" (Page 601).

13.6.9.2 Adding an LSP Lifetime Interval

To add an LSP lifetime interval to an IS-IS area, do the following:

⚠ NOTICE

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 602).

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

   ```
   routing isis area { name } max-lsp-lifetime is-type [ lev
   el-1-2 | level-1-only | level-2-only ] interval { sec
   onds }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.

- `{ level }` is the IS type.
- `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.

3. Type `commit` and press **Enter** to save the changes.

13.6.9.3 Deleting an LSP Lifetime Interval

To delete an LSP lifetime interval for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the LDP interface by typing:

```
no routing isis area { name } max-lsp-lifetime is-type
[ level-1-2 | level-1-only | level-2-only ] interval
{ seconds }
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.
- `{ level }` is the IS type.
- `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.

3. Type `commit` and press **Enter** to save the changes.

13.6.10 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 600).

13.6.10.1 Viewing a List of LSP Refresh Intervals

To view a list of LSP refresh intervals configured for an IS-IS area, type:

```
show running-config routing isis area { name } lsp-re
fresh-interval
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.

If intervals have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area Area_1 lsp-refresh-interval | tab
ISTYPE        INTERVAL
-----------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to "Adding an LSP Refresh Interval" (Page 603).

13.6.10.2 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 600).

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

   ```
   routing isis area { name } lsp-refresh-interval is-type
   [ level-1-2 | level-1-only | level-2-only ] interval
   { seconds }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ level }` is the IS type.
   - `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type `commit` and press **Enter** to save the changes.

13.6.10.3 Deleting an LSP Refresh Interval

To delete an LSP refresh interval for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the LDP interface by typing:

   ```
   no routing isis area { name } lsp-refresh-interval is-
   type [ level-1-2 | level-1-only | level-2-only ] interval
   { seconds }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ level }` is the IS type.
   - `{ seconds }` is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type `commit` and press **Enter** to save the changes.

13.6.11 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.

13.6.11.1 Viewing a List of NETs

To view a list of areas configured for dynamic IS-IS routes, type:

```
show running-config routing isis area { name } net
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.

If NETs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area Area_1 net | tab
NET TITLE
---------------------------
49.0001.1921.6800.1001.00

 !
!
```

If no NETs have been configured, add NETs as needed. For more information, refer to "Adding a NET" (Page 605).

13.6.11.2 Adding a NET

To add a Network Entity Title (NET) for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the NET by typing:

   ```
   routing isis area { name } net { title }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ title }` is the NET for the router, consisting of a two-octet area ID, a three-octet system ID and a one-octet selector. For example: 0001.1921.6800.1001.00
3. Type `commit` and press **Enter** to save the changes.

13.6.11.3 Deleting a NET

To delete a Network Entity Title (NET) for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the NET by typing:

   ```
   no routing isis area { name } net { title }
   ```

   Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.
- `{ title }` is the NET for the router, consisting of a two-octet area ID, a three-octet system ID and a one-octet selector. For example: 0001.1921.6800.1001.00

3. Type `commit` and press **Enter** to save the changes.

13.6.12 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.

13.6.12.1 Viewing a List of Redistribution Metrics

To view a list of redistribution metrics defined for an IS-IS area, type:

```
show running-config routing isis area { name } redistribute
```

Where:

- `{ name }` is the unique name for a routing process that belongs to a specific router.

If metrics have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing isis area Area_1 redistribute | tab
                   METRIC
SOURCE  IS TYPE    TYPE      METRIC
-------------------------------------
bgp     level-1-2  internal  10

 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 607).

13.6.12.2 Adding a Redistribution Metric

To add a redistribution metric for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the metric by typing:

   ```
   routing isis area { name } redistribute { source }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.
   - `{ source }` is the protocol transmitting packets over the IS-IS route. Options include bgp, connected, kernel, ospf, rip, and static.
3. Configure the following parameter(s) as required:

Parameter	Description
`is-type { is-type }`	**Synopsis:** [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 { metric-type }`	**Synopsis:** [internal | external] **Default:** external The IS-IS metric type for redistributed routes. Default is external
`metric { metric }`	**Synopsis:** An integer between 0 and 16777214 The metric for redistributed routes.

4. Type `commit` and press **Enter** to save the changes.

13.6.12.3 Deleting a Redistribution Metric

To delete a redistribution metric for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the metric by typing:

   ```
   no routing isis area { name } redistribute { source }
   ```

   Where:

   - `{ name }` is the unique name for a routing process that belongs to a specific router.

- `{ source }` is the protocol transmitting packets over the IS-IS route. Options include bgp, connected, kernel, ospf, rip, and static.

3. Type `commit` and press **Enter** to save the changes.

13.7 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] 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 668).

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.

13.7.1 Configuring RIP

To configure dynamic routing using the Routing Information Protocol (RIP) daemon, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » rip*** and configure the following parameter(s) as required:

Parameter	Description
`update { update }`	**Synopsis:** An integer between 5 and 2147483647 **Default:** 30 The routing table update timer (in seconds).
`timeout { timeout }`	**Synopsis:** An integer between 5 and 2147483647 **Default:** 180 The routing information timeout timer (in seconds).
`garbage { garbage }`	**Synopsis:** An integer between 5 and 2147483647 **Default:** 120 The garbage collection timer (in seconds).
`enabled`	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 { default-metric }`	**Synopsis:** An integer between 1 and 16 **Default:** 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 { distance-default }`	**Synopsis:** An integer between 1 and 255 Sets the default RIP distance.
`version { version }`	**Synopsis:** 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.

3. Configure prefix lists. For more information, refer to "Adding a Prefix List" (Page 612).
4. Configure a network. For more information, refer to "Configuring a Network" (Page 615).
5. Configure the prefix list distribution. For more information, refer to "Adding a Prefix List Distribution Path" (Page 619).
6. Configure key chains. For more information, refer to "Adding a Key Chain" (Page 621).
7. Configure redistribution metrics. For more information, refer to "Adding a Redistribution Metric" (Page 624).

8. Configure interfaces. For more information, refer to "Configuring a Routing Interface" (Page 625).
9. Type `commit` and press **Enter** to save the changes.

13.7.2 Viewing the Status of Dynamic RIP Routes

To view the status of the dynamic RIP routes configured on the device, type:

```
show routing status rip route
```

If RIP routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status rip route | tab
NETWORK          TYPE       SUB TYPE   NEXT HOP     METRIC  FROM         TAG  TI
-------------------------------------------------------------------------------
192.168.0.0/24   connected  interface  0.0.0.0      1       self         0
192.168.5.0/24   rip        normal     192.168.0.3  2       192.168.0.3  0    02
192.168.6.0/24   rip        normal     192.168.0.3  2       192.168.0.3  0    02
192.168.50.0/24  connected  interface  0.0.0.0      1       self         0
192.168.60.0/24  connected  interface  0.0.0.0      1       self         0
```

This list provides the following information:

Parameter	Description
`{ network }`	**Synopsis:** A string The network.
`type`	**Synopsis:** A string The route type.
`sub-type`	**Synopsis:** A string The route sub type.
`next-hop`	**Synopsis:** A string The next hop.
`metric`	**Synopsis:** A string The metric value.
`from`	**Synopsis:** A string Where this route comes from.
`tag`	**Synopsis:** A string Tag.
`time`	**Synopsis:** A string The route update time.

To view the status of the RIP interfaces configured on the device, type:

```
show routing status rip interface
```

If RIP interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status rip interface | tab
                                                        NEXT
NAME         NETWORK          TYPE       SUB TYPE     HOP      METRIC  FROM  TAG
 TIME
-------------------------------------------------------------------------------------
switch.1112
             192.168.11.0/24  connected  interface    0.0.0.0  1       self  0
```

This list provides the following information:

Parameter	Description
`{ network }`	**Synopsis:** A string The network.
`type`	**Synopsis:** A string The route type.
`sub-type`	**Synopsis:** A string The route sub type.
`next-hop`	**Synopsis:** A string Next hop.
`metric`	**Synopsis:** A string The metric value.
`from`	**Synopsis:** A string Where this route comes from.
`tag`	**Synopsis:** A string Tag.
`time`	**Synopsis:** 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 608).

13.7.3 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.

13.7.3.1 Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic RIP routes, type:

```
show running-config routing rip filter prefix-list
```

If prefix lists have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip filter prefix-list | tab
NAME                 DESCRIPTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22   -
                                  100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11 -
                                  100  permit  192.168.33.0/24  -   -
                                  200  permit  192.168.33.0/24  32  -

!
```

If no prefix lists have been configured, add lists as needed. For more information, refer to "Adding a Prefix List" (Page 612).

13.7.3.2 Viewing a List of Prefix Entries

To view a list of entries for dynamic RIP prefix lists, type:

```
show running-config routing rip filter prefix-list { name }
entry
```

Where:

- `{ name }` is the name of the prefix list

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -

 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 613).

13.7.3.3 Adding a Prefix List

To add a prefix list for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the list by typing:

   ```
   routing rip filter prefix-list { name }
   ```

   Where:

   - `{ name }` is the name of the prefix list

3. Configure the following parameter(s) as required:

Parameter	Description
`description { description }`	**Synopsis:** A string up to 1024 characters long The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 613).
5. Type `commit` and press **Enter** to save the changes.

13.7.3.4 Adding a Prefix Entry

To add an entry for a dynamic RIP prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the entry by typing:

   ```
   routing rip filter prefix-list { name } entry { number }
   ```

   Where:

   - `{ name }` is the name of the prefix list
   - `{ number }` is the sequence number for the entry

3. Configure the following parameter(s) as required:

Parameter	Description
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit The action that will be performed.
`subnet { subnet }`	**Synopsis:** A string between 9 and 18 characters long The IPv4 network address and prefix.
`le { le }`	**Synopsis:** An integer between 1 and 32 The maximum prefix length to be matched.
`ge { ge }`	**Synopsis:** An integer between 1 and 32 The minimum prefix length to be matched.

4. Type `commit` and press **Enter** to save the changes.

13.7.3.5 Deleting a Prefix List

To delete a prefix list for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.

   Note

   Deleting a prefix list removes all associate prefix entries as well.

2. Delete the list by typing:

   ```
   no routing rip filter prefix-list { name }
   ```

   Where:

   - `{ name }` is the name of the prefix list
3. Type `commit` and press **Enter** to save the changes.

13.7.3.6 Deleting a Prefix Entry

To delete an entry for a dynamic RIP prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:

   ```
   no routing rip filter prefix-list { name } entry { num
   ber }
   ```

   Where:

   - `{ name }` is the name of the prefix list
   - `{ number }` is the sequence number for the entry
3. Type `commit` and press **Enter** to save the changes.

13.7.4 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 618).

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 618).

13.7.4.1 Configuring a Network

To configure a network for the RIP protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add one or more network IP addresses. For more information, refer to "Adding a Network IP Address" (Page 616).
3. Add one or more network interfaces. For more information, refer to "Adding a Network Interface" (Page 617).
4. Add one or more neighbors. For more information, refer to "Adding a Neighbor" (Page 618).

13.7.4.2 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 584).

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 the CLI is in Configuration mode.
2. Navigate to ***routing » rip » distribute-prefix-list » { direction} {interface } » track***, where { direction } is the direction (incoming or outgoing) in which to filter routing updates and { interface } is the name of the interface.
3. Configure the following parameter(s) as required:

Parameter	Description
`event { event }`	**Synopsis:** 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.

Parameter	Description
`apply-when { ap ply-when }`	**Synopsis:** [up | down] **Default:** up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

4. Type `commit` and press **Enter** to save the changes.

13.7.5 Managing Network IP Addresses

This section describes how to manage IP addresses for RIP networks.

13.7.5.1 Viewing a List of Network IP Addresses

To view a list of IP addresses configured for a RIP network, type:

```
show running-config routing rip network ip
```

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip network ip
routing rip
 network ip 192.168.33.0/24
 !
!
```

If no IP addresses have been configured, add addresses as needed. For more information, refer to "Adding a Network IP Address" (Page 616).

13.7.5.2 Adding a Network IP Address

To add an IP address for a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing rip network ip { address }
   ```

   Where:

   - `{ address }` is the IP subnet address and prefix for the network
3. Type `commit` and press **Enter** to save the changes.

13.7.5.3 Deleting a Network IP Address

To delete an IP address from a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the IP address by typing:

   ```
   no routing rip network ip { address }
   ```

   Where:

   - `{ address }` is the IP subnet address and prefix for the network
3. Type `commit` and press **Enter** to save the changes.

13.7.6 Managing Network Interfaces

This section describes how to manage interfaces used by RIP networks.

13.7.6.1 Viewing a List of Network Interfaces

To view a list of interfaces configured for a RIP network, type:

```
show running-config routing rip network interface
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip network interface
routing rip
 network interface switch.4084
 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Network Interface" (Page 617).

13.7.6.2 Adding a Network Interface

To add an interface for a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing rip network interface { name }
   ```

   Where:

   - `{ name }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

13.7.6.3 Deleting a Network Interface

To delete an interface from a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing rip network interface { name }
   ```

   Where:

   - `{ name }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

13.7.7 Managing Neighbors

Neighbors are other routers with which to exchange routes.

13.7.7.1 Viewing a List of Neighbors

To view a list of neighbors configured for a RIP network, type:

```
show running-config routing rip network neighbor
```

If neighbors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip network neighbor
routing rip
 network neighbor 192.168.33.2
 !
!
```

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 618).

13.7.7.2 Adding a Neighbor

To add a neighbor for a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing rip network neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor
3. Type `commit` and press **Enter** to save the changes.

13.7.7.3 Deleting a Neighbor

To delete a neighbor from a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing rip network neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor
3. Type `commit` and press **Enter** to save the changes.

13.7.8 Managing the Prefix List Distribution

This section describes how to manage the distribution of prefix lists.

13.7.8.1 Viewing a List of Prefix List Distribution Paths

To view a list of prefix list distribution paths for dynamic RIP routes, type:

```
show running-config routing rip distribute-prefix-list
```

If distribution paths have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip distribute-prefix-list
routing rip
 distribute-prefix-list out ""
  prefix-list list-permit-lan-22
 !
!
```

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 619).

13.7.8.2 Adding a Prefix List Distribution Path

To add a prefix list distribution path for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the path by typing:

   ```
   routing rip distribute-prefix-list { direction } { inter
   face }
   ```

   Where:

- `{ direction }` is the direction (incoming or outgoing) in which to filter routing updates.
- `{ interface }` is the name of the interface. This parameter is optional.

3. Configure the following parameter(s) as required:

Parameter	Description
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The name of the prefix list.

4. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands" (Page 615).
5. Type `commit` and press **Enter** to save the changes.

13.7.8.3 Deleting a Prefix List Distribution Path

To delete a prefix list distribution path for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the path by typing:

```
no routing rip distribute-prefix-list { direction } { interface }
```

Where:

- `{ direction }` is the direction (incoming or outgoing) in which to filter routing updates.
- `{ interface }` is the name of the interface. This parameter is optional.

3. Type `commit` and press **Enter** to save the changes.

13.7.9 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.

13.7.9.1 Viewing a List of Key Chains

To view a list of key chains for dynamic RIP routes, type:

```
show running-config routing rip key-chain
```

If key chains have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip key-chain
routing rip
 key-chain key-1
  key 1
   key-string RUGGEDCOM
   accept-lifetime start 2013-01-01T01:01:01-00:00
   accept-lifetime expire 2022-01-01T01:01:01-00:00
   send-lifetime start 2013-01-01T01:01:01-00:00
   send-lifetime expire 2022-01-01T01:01:01-00:00
  !
 !
!
```

If no key chains have been configured, add key chains as needed. For more information, refer to "Adding a Key Chain" (Page 621).

13.7.9.2 Viewing a List of Keys

To view a list of keys in a key chain, type:

```
show running-config routing rip rip key-chain { name } key
```

Where:

- `{ name }` is the name of the key chain

If keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip key-chain key
routing rip
 key-chain key-1
  key 1
   key-string RUGGEDCOM
   accept-lifetime start 2013-01-01T01:01:01-00:00
   accept-lifetime expire 2022-01-01T01:01:01-00:00
   send-lifetime start 2013-01-01T01:01:01-00:00
   send-lifetime expire 2022-01-01T01:01:01-00:00
  !
 !
!
```

If no keys have been configured, add keys as needed. For more information, refer to "Adding a Key" (Page 622).

13.7.9.3 Adding a Key Chain

To add a key chain for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the path by typing:

   ```
   routing rip key-chain { name }
   ```

   Where:

- `{ name }` is the name of the key chain

3. Configure one or more keys for the key chain. For more information, refer to "Adding a Key" (Page 622).
4. Configure a routing interface to use the key chain for authentication purposes. For more information, refer to "Configuring a Routing Interface" (Page 625).
5. Type `commit` and press **Enter** to save the changes.

13.7.9.4 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 they 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. Make sure the CLI is in Configuration mode.
2. Add the key by typing:

   ```
   routing rip key-chain { name } key { id }
   ```

   Where:

   - `{ name }` is the name of the key chain
   - `{ id }` is the ID of the key

3. Configure the key name setting by configuring the following parameter(s):

Parameter	Description
`key-string { key-string }`	**Synopsis:** A string Sets the key string.

4. Configure the accept lifetime settings by configuring the following parameter(s):

Parameter	Description
`start { start }`	**Synopsis:** A string The beginning time in which the key is considered valid.
`expire { expire }`	**Synopsis:** A string or [infinite] Expire time.

5. Configure the send lifetime settings by configuring the following parameter(s):

Parameter	Description
`start { start }`	**Synopsis:** A string Sets the time period in which the key on the key chain is considered valid.
`expire { expire }`	**Synopsis:** A string or [infinite] The time at which the key expires.

6. Type `commit` and press **Enter** to save the changes.

13.7.9.5 Deleting a Key Chain

To delete a key chain for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the key chain by typing:

   ```
   no routing rip key-chain { name }
   ```

   Where:

   - `{ name }` is the name of the key chain
3. Type `commit` and press **Enter** to save the changes.

13.7.9.6 Deleting a Key

To delete a key from a key chain, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the key by typing:

   ```
   no routing rip key-chain { name } key { id }
   ```

   Where:

   - `{ name }` is the name of the key chain
   - `{ id }` is the ID of the key
3. Type `commit` and press **Enter** to save the changes.

13.7.10 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.

13.7.10.1 Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic RIP routes, type:

```
show running-config routing rip redistribute
```

If metrics have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip redistribute
routing rip
 redistribute bgp
  no metric
 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 624).

13.7.10.2 Adding a Redistribution Metric

To add a redistribution metric for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the metric by typing:

   ```
   routing rip redistribute [ { bgp } | { ospf } | { connect
   ed } | { static } | { kernel } ]
   ```

3. Type `commit` and press **Enter** to save the changes.

13.7.10.3 Deleting a Redistribution Metric

To delete a redistribution metric for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the metric by typing:

   ```
   no routing rip redistribute [ { bgp } | { ospf } | { con
   nected } | { static } | { kernel } ]
   ```

3. Type `commit` and press **Enter** to save the changes.

13.7.11 Managing Routing Interfaces

This section describes how to manage interfaces for RIP routes.

13.7.11.1 Viewing a List of Routing Interfaces

To view a list of routing interfaces for a RIP network, type:

```
show running-config routing rip interface
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip interface | tab
                    KEY                       RECEIVE  SEND     SPLIT
IFNAME       MODE   CHAIN  STRING  PASSIVE   VERSION  VERSION  HORIZON
-------------------------------------------------------------------------
dummy0       -      -      -       -         -        -        yes
fe-cm-1      -      -      -       -         -        -        yes
switch.0001  -      -      -       -         -        -        yes
```

13.7.11.2 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » rip » interface » { name }***, where { name } is the name of the interface.
3. Configure the authentication settings by typing the following commands:

Parameter	Description
`mode { mode }`	**Synopsis:** [md5-rfc | md5-old-ripd | text | none] The authentication mode.
`key-chain { key-chain }`	**Synopsis:** A string between 1 and 1024 characters long The authentication key chain.
`string { string }`	**Synopsis:** A string up to 16 characters long The authentication string.

4. Configure the interface settings by typing the following commands:

Parameter	Description
`passive`	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.

Parameter	Description
`receive-version { receive-version }`	**Synopsis:** [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 { send-version }`	**Synopsis:** [1 | 2 | 1,2 | 2,1] The version of RIP to send packets with. By default, version 2 packets will be sent.
`split-horizon { split-horizon }`	**Synopsis:** [yes | no | poisoned-reverse] **Default:** yes A split horizon.

5. Type `commit` and press **Enter** to save the changes.

13.8 Managing BGP

The Border Gateway Protocol (BGP) as defined by RFC 4271 [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.

13.8.1 Configuring BGP

To configure dynamic routing with BGP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » bgp*** and configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables BGP.

Parameter	Description
`as-id { as-id }`	**Synopsis:** 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 { reachability-check }`	**Synopsis:** [true | false] **Default:** 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 { default-local-preference }`	**Synopsis:** An integer **Default:** 100 Default local preference value.
`deterministic-med`	Pick the best-MED path among paths advertised from neighboring AS.
`router-id { router-id }`	**Synopsis:** A string between 7 and 15 characters long Router ID for BGP.

3. Configure autonomous system path filters. For more information, refer to "Adding an Autonomous System Path Filter" (Page 640).
4. Configure prefix list filters. For more information, refer to "Adding a Prefix List" (Page 637).
5. Configure route map filters. For more information, refer to "Adding a Route Map Filter" (Page 629).
6. Configure a network. For more information, refer to "Adding a Network" (Page 646).
7. Configure IP addresses for neighbors. For more information, refer to "Adding a Neighbor" (Page 642).
8. Configure aggregate addresses. For more information, refer to "Adding an Aggregate Address" (Page 648).
9. Configure redistribution metrics. For more information, refer to "Adding a Redistribution Metric" (Page 650).
10. Type `commit` and press **Enter** to save 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.

11. Reset the BGP session. For more information, refer to "Resetting a BGP Session" (Page 667).

13.8.2 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.

13.8.2.1 Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic BGP routes, type:

```
show running-config routing bgp filter route-map
```

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter route-map | tab
                       ON
                       MATCH  AS    PREFIX  PREFIX  PREFIX                                LOCAL
                  NEXT          ORIGINATOR
TAG  SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
  OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT
-------------------------------------------------------------------------------------
map
     10   permit  -     -      -     -       -       -       -       -     -       -   -   -
  -          -      -     -       -           -

!
```

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 640).

13.8.2.2 Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either BGP, type:

```
show running-config routing bgp filter route-map { tag } en
try
```

Where:

- `{ tag }` is the tag for the route map filter

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter route-map map entry | tab
                  ON
                  MATCH  AS    PREFIX  PREFIX  PREFIX                                LOCAL
              NEXT          ORIGINATOR
SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE  OP
ERATION  VALUE  HOP   ORIGIN  ID         WEIGHT  AS
-------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -           -
       -      -     -       -          -

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 640).

13.8.2.3 Adding a Route Map Filter

To add a route map filter for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:

   ```
   routing bgp filter route-map { tag }
   ```

   Where:

   - `{ tag }` is the tag for the route map filter
3. Add one or more entries. For more information, refer to "Adding a Route Map Filter Entry" (Page 629).
4. Type `commit` and press **Enter** to save the changes.

13.8.2.4 Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:

   ```
   routing bgp filter route-map { tag } entry { number }
   ```

   Where:

   - `{ tag }` is the tag for the route map filter
   - `{ number }` is the sequence number for the entry
3. Configure the following parameter(s) as required:

Parameter	Description
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit Action.
`call { call }`	**Synopsis:** A string between 1 and 1024 characters long Jump to another route-map after match+set.
`on-match-goto { on-match-goto }`	**Synopsis:** An integer between 1 and 65535 Go to this entry on match.

4. Configure the match rules for the route map filter. For more information, refer to "Configuring Match Rules" (Page 631).
5. Configure a set for the route map filter. For more information, refer to "Configuring a Set" (Page 632).
6. Type `commit` and press **Enter** to save the changes.

13.8.2.5 Deleting a Route Map Filter

To delete a route map filter for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

   ```
   no routing bgp filter route-map { tag }
   ```

   Where:

   - `{ tag }` is the tag for the route map filter
3. Type `commit` and press **Enter** to save the changes.

13.8.2.6 Deleting a Route Map Filter Entry

To delete an entry for a route map filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

   ```
   no routing bgp filter route-map { tag } entry { number }
   ```

   Where:

   - `{ tag }` is the tag for the route map filter
   - `{ number }` is the sequence number for the entry
3. Type `commit` and press **Enter** to save the changes.

13.8.2.7 Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » bgp » filter » route-map » { tag } » entry » { number } » match***, where { tag } is the tag for the route map filter and { number } is the sequence number for the entry.
3. Configure the following parameters:

Parameter	Description
`as-path { as-path }`	**Synopsis:** A string between 1 and 1024 characters long Match the BGP AS path filter.
`metric { metric }`	**Synopsis:** An integer Match the route metric.
`peer { peer }`	**Synopsis:** A string between 7 and 15 characters long This parameter is not supported and any value is ignored by the system.s
`origin { origin }`	**Synopsis:** [egp | igp | incomplete] Match the BGP origin code.

4. To match based on the route's IP address, navigate to **ip** and configure the following parameters:

Parameter	Description
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.

5. To match based on the route's next hop address, navigate to **next-hop** and configure the following parameters:

Parameter	Description
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.

6. To match based on the route's advertised source address, navigate to **route-source** and configure the following parameters:

Parameter	Description
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.

7. Type `commit` and press **Enter** to save the changes.

13.8.2.8 Configuring a Set

To configure a set for a route map filter entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » bgp » filter » route-map » { tag } » entry » { number } » set***, where { tag } is the tag for the route map filter and { number } is the sequence number for the entry.
3. Configure the entry set by configuring the following parameters:

Parameter	Description
`local-preference { local-preference }`	**Synopsis:** An integer Local preference.
`next-hop { next-hop }`	**Synopsis:** 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 { origin }`	**Synopsis:** [egp | igp | incomplete] The origin code.
`originator-id { originator-id }`	**Synopsis:** A string between 7 and 15 characters long This parameter is not supported and any value is ignored by the system.
`weight { weight }`	**Synopsis:** An integer Weight.

4. Configure the aggregator settings by configuring the following parameters:

Parameter	Description
`as { as }`	**Synopsis:** An integer between 1 and 4294967295 AS number.
`ip { ip }`	**Synopsis:** A string between 7 and 15 characters long IP address of aggregator.

5. Configure the metric settings by configuring the following parameters:

Parameter	Description
`operation { operation }`	**Synopsis:** [set | add | sub] Set , add or subtract the metric value.
`value { value }`	**Synopsis:** An integer Value.

6. Add pre-pended and/or excluded autonomous system paths. For more information, refer to "Adding a Prepended Autonomous System Path

Filter" (Page 634) and/or "Adding an Excluded Autonomous System Path filter" (Page 635).

7. Type `commit` and press **Enter** to save the changes.

13.8.3 Managing Prepended and Excluded Autonomous System Path Filters

This section describes how to configure and manage prepended and excluded autonomous system path filters.

13.8.3.1 Viewing a List of Prepended Autonomous System Path Filters

To view a list of prepended autonomous system path filters configured for a BGP route map entry, type:

```
show running-config routing bgp filter route-map { name } en
try { number } set as-path prepend
```

Where:

- `{ name }` is the name of the route map
- `{ number }` is the entry number

Note

The repeat count is only displayed when higher than 1.

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter route-map route entry 10 set as-
path prepend
routing bgp
 filter route-map route
  entry 10
   set as-path prepend 120
    repeat-count 2
   !
  !
 !
!
```

If no prepended autonomous system path filters have been configured, add filters as needed. For more information, refer to "Adding a Prepended Autonomous System Path Filter" (Page 634).

13.8.3.2 Viewing a List of Excluded Autonomous System Paths

To view a list of excluded autonomous system path filters configured for a BGP route map entry, type:

```
show running-config routing bgp filter route-map { name } en
try { number } set as-path exclude
```

Where:

- `{ name }` is the name of the route map
- `{ number }` is the entry number

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter route-map route entry 10 set as-
path exclude
routing bgp
 filter route-map route
  entry 10
   set as-path exclude 110
   !
  !
 !
!
```

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 635).

13.8.3.3 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. Make sure the CLI is in Configuration mode.
2. Add the path by typing:

   ```
   routing bgp filter route-map { name } entry { number } set
   as-path prepend { path }
   ```

   Where:

   - `{ name }` is the name of the route map
   - `{ number }` is the entry number
   - `{ path }` is the number for the autonomous system path
3. Type `commit` and press **Enter** to save the changes.

13.8.3.4 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. Make sure the CLI is in Configuration mode.
2. Add the path by typing:

   ```
   routing bgp filter route-map { name } entry { number } set
   as-path exclude { path }
   ```

   Where:

   - `{ name }` is the name of the route map
   - `{ number }` is the entry number
   - `{ path }` is the number for the autonomous system path
3. Type `commit` and press **Enter** to save the changes.

13.8.3.5 Deleting a Prepended Autonomous System Path Filter

To delete a prepended autonomous system path filter from a BGP route map entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing bgp filter route-map { name } entry { number }
   set as-path prepend { path }
   ```

   Where:

   - `{ name }` is the name of the route map
   - `{ number }` is the entry number
   - `{ path }` is the number for the autonomous system path
3. Type `commit` and press **Enter** to save the changes.

13.8.3.6 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. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing bgp filter route-map { name } entry { number }
   set as-path exclude { path }
   ```

   Where:

- `{ name }` is the name of the route map
- `{ number }` is the entry number
- `{ path }` is the number for the autonomous system path

3. Type `commit` and press **Enter** to save the changes.

13.8.4 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.

13.8.4.1 Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic BGP routes, type:

```
routing bgp filter prefix-list
```

If prefix lists have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter prefix-list | tab
NAME                 DESCBGPTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22   -
                                  100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11 -
                                  100  permit  192.168.33.0/24  -   -
                                  200  permit  192.168.33.0/24  32  -

!
```

If no prefix lists have been configured, add lists as needed. For more information, refer to "Adding a Prefix List" (Page 637).

13.8.4.2 Viewing a List of Prefix Entries

To view a list of entries for dynamic BGP, OSPF, or BGP prefix lists, type:

```
routing bgp filter prefix-list { name } entry
```

Where:

- `{ name }` is the name of the prefix list

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -
```

```
 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 637).

13.8.4.3 Adding a Prefix List

To add a prefix list for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the list by typing:

   ```
   routing bgp filter prefix-list { name }
   ```

   Where:

   - `{ name }` is the name of the prefix list
3. Configure the following parameter(s) as required:

Parameter	Description
`description { description }`	**Synopsis:** A string up to 1024 characters long The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 637).
5. Type `commit` and press **Enter** to save the changes.

13.8.4.4 Adding a Prefix Entry

To add an entry for a dynamic BGP prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the entry by typing:

   ```
   routing bgp filter prefix-list { name } entry { number }
   ```

   Where:

   - `{ name }` is the name of the prefix list
   - `{ number }` is the sequence number for the entry
3. Configure the following parameter(s) as required:

Parameter	Description
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit Action.
`subnet { subnet }`	**Synopsis:** A string between 9 and 18 characters long Network (xxx.xxx.xxx.xxx/xx).
`le { le }`	**Synopsis:** An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
`ge { ge }`	**Synopsis:** An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

4. Type `commit` and press **Enter** to save the changes.

13.8.4.5 Deleting a Prefix List

To delete a prefix list for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.

   Note

   Deleting a prefix list removes all associate prefix entries as well.

2. Delete the list by typing:

   ```
   no routing bgp filter prefix-list { name }
   ```

   Where:

   - `{ name }` is the name of the prefix list
3. Type `commit` and press **Enter** to save the changes.

13.8.4.6 Deleting a Prefix Entry

To delete an entry for a dynamic BGP prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:

   ```
   no routing bgp filter prefix-list { name } entry { num
   ber }
   ```

   Where:

   - `{ name }` is the name of the prefix list

- `{ number }` is the sequence number for the entry

3. Type `commit` and press **Enter** to save the changes.

13.8.5 Managing Autonomous System Paths and Entries

This section describes how to configure autonomous system paths and entries for dynamic BGP routes.

13.8.5.1 Viewing a List of Autonomous System Paths

To view a list of autonomous system path filters for dynamic BGP routes, type:

```
show running-config routing bgp filter as-path
```

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter as-path | tab
NAME              ACTION  MATCH
---------------------------------
filter-allow-120
                  permit  120

!
```

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 640).

13.8.5.2 Viewing a List of Autonomous System Path Entries

To view a list of entries for an autonomous system path filter, type:

```
show running-config routing bgp filter as-path { name } entry
```

Where:

- `{ name }` is the name of the autonomous system path filter

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp filter as-path filter-allow-120 entry |
 tab
ACTION  MATCH
---------------
permit  120

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to "Adding an Autonomous System Path Filter" (Page 640).

13.8.5.3 Adding an Autonomous System Path Filter

To add an autonomous system path filter for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:

   ```
   routing bgp filter as-path { name }
   ```

   Where:

   - `{ name }` is the name of the autonomous system path filter
3. Add one or more entries. For more information, refer to "Adding an Autonomous System Path Filter Entry" (Page 640).
4. Type `commit` and press **Enter** to save the changes.

13.8.5.4 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.

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: • Each space ( ) and comma (,) • Each AS set delimiter (e.g. *{* and *}*) • Each AS confederation delimiter (e.g. *(* and *)*) • The beginning and end of the line Therefore, the underscore can be used to match AS values.	_100,100_, _100_

To add an entry for an autonomous system path filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:

   ```
   routing bgp filter as-path { name } entry { action }
   { match }
   ```

Where:

- `{ name }` is the name of the autonomous system path filter.
- `{ action }` is the action.
- `{ match }` is the regular expression to match with the autonomous system path. For more information about regular expressions, refer to "Using Regular Expressions" (Page 42).

3. Type `commit` and press **Enter** to save the changes.

13.8.5.5 Deleting an Autonomous System Path

To delete an autonomous system path filter for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

```
no routing bgp filter as-path { name }
```

Where:

- `{ name }` is the name of the autonomous system path filter

3. Type `commit` and press **Enter** to save the changes.

13.8.5.6 Deleting an Autonomous System Path Filter Entry

To delete an entry for an autonomous system path filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

```
no routing bgp filter as-path { name } entry { action }
{ match }
```

Where:

- `{ name }` is the name of the autonomous system path filter
- `{ action }` is the action
- `{ match }` is the regular expression to match with the autonomous system path

3. Type `commit` and press **Enter** to save the changes.

13.8.6 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 645).

13.8.6.1 Viewing a List of Neighbors

To view a list of neighbors configured for a BGP network, type:

```
show running-config routing bgp neighbor
```

If neighbors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp neighbor
routing bgp
 neighbor 192.168.123.3
  remote-as 100
  no ebgp-multihop
  no maximum-prefix
  no next-hop-self
  no password
  no route-map in
  no route-map out
  no soft-reconfiguration
  no weight
 !
!
```

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 642).

13.8.6.2 Adding a Neighbor

To add a neighbor for a BGP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing bgp neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor
3. [Optional] Enable the neighbor as a route reflector client by configuring the following parameter:

Parameter	Description
`enabled`	If enabled and Route Reflector enabled, makes this neighbor a client for Route Reflector.

4. [Optional] Configure the route map settings by configuring the following parameter(s):

Parameter	Description
`in { in }`	**Synopsis:** A string between 1 and 1024 characters long Apply route map to incoming routes.
`out { out }`	**Synopsis:** A string between 1 and 1024 characters long Apply route map to outbound routes.

5. [Optional] Configure the neighbor settings by configuring the following parameter(s):

Parameter	Description
`remote-as { remote-as }`	**Synopsis:** An integer between 1 and 4294967295 A BGP neighbor.
`ebgp-multihop { ebgp-multihop }`	**Synopsis:** An integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
`maximum-prefix { maximum-prefix }`	**Synopsis:** An integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
`next-hop-self`	Disables the next hop calculation for this neighbor.
`password { password }`	**Synopsis:** A string Password.
`update-source { update-source }`	**Synopsis:** 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 { weight }`	**Synopsis:** An integer The default weight for routes from this neighbor.

6. Type `commit` and press **Enter** to save the changes.

13.8.6.3 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 CLI is in Configuration mode.

2. Apply the desired prefix list the chosen route direction (incoming or outbound) by typing:

   ```
   routing bgp neighbor { address } distribute-prefix-list
   [ in | out ] prefix-list { prefix }
   ```

   Where:

   - `{ address }` is the address of the chosen neighbor
   - `{ prefix }` is the chosen BGP prefix list
3. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands for BGP Neighbors" (Page 644).
4. Type `commit` and press **Enter** to save the changes.

13.8.6.4 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 584).

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:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » dynamic » bgp » network » { address } » track***, where { address } is the IP address of the neighbor.
3. Configure the following parameter(s) as required:

Parameter	Description
`event { event }`	**Synopsis:** 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 { apply-when }`	**Synopsis:** [up | down] **Default:** up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

4. Type `commit` and press **Enter** to save the changes.

13.8.6.5 Deleting a Neighbor

To delete a neighbor from a BGP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing bgp neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor
3. Type `commit` and press **Enter** to save the changes.

13.8.7 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 642).

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 641).

13.8.7.1 Viewing a List of Networks

To view a list of networks configured for the BGP protocol, type:

```
show running-config routing bgp network
```

If networks have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp network
routing bgp
```

```
 network 192.168.12.0/24
 !
 network 192.168.123.0/24
 !
!
```

If no networks have been configured, add networks as needed. For more information, refer to "Adding a Network" (Page 646).

13.8.7.2 Adding a Network

To add a network for the BGP protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the network by typing:

   `routing bgp network { address }`

   Where:

   - `{ address }` is the IP subnet address and prefix for the network
3. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands for a BGP Network" (Page 646).
4. Type `commit` and press **Enter** to save the changes.

13.8.7.3 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 584).

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. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » bgp » network » { address } » track***, where { address } is the IP subnet address and prefix for the network.
3. Configure the following parameter(s) as required:

Parameter	Description
`event { event }`	**Synopsis:** A string up to 64 characters long Select an event.

Parameter	Description
`apply-when { apply-when }`	**Synopsis:** [up | down] **Default:** up Advertises the network when the tracked event state goes UP or stops advertising the network when the tracked event goes DOWN.

4. Type `commit` and press **Enter** to save the changes.

13.8.7.4 Deleting a Network

To delete a network configured for the BGP protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing bgp network { address }
   ```

   Where:

   - `{ address }` is the IP subnet address and prefix for the network
3. Type `commit` and press **Enter** to save the changes.

13.8.8 Managing Aggregate Addresses

This section describes how to aggregate multiple addresses into a single dynamic BGP route.

13.8.8.1 Viewing a List of Aggregate Addresses

To view a list of aggregate addresses for dynamic BGP routes, type:

```
show running-config routing bgp aggregate-address
```

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp aggregate-address
routing bgp
 aggregate-address 11.11.0.0/16
  options summary-only
  !
 !
!
```

If no aggregate addresses have been configured, add addresses as needed. For more information, refer to "Adding an Aggregate Address" (Page 648).

13.8.8.2 Adding an Aggregate Address

To add an aggregate address for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the path by typing:

   ```
   routing bgp aggregate-address { address }
   ```

   Where:

   - `{ address }` is the subnet address and prefix for the aggregate address
3. If necessary, configure options for the address. For more information, refer to "Adding an Aggregate Address Option" (Page 649).
4. Type `commit` and press **Enter** to save the changes.

13.8.8.3 Deleting an Aggregate Address

To delete an aggregate address for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no routing bgp aggregate-address { address }
   ```

   Where:

   - `{ address }` is the subnet address and prefix for the aggregate address
3. Type `commit` and press **Enter** to save the changes.

13.8.9 Managing Aggregate Address Options

This section describes how to set the **as-set** and **summary-only** options for BGP aggregate addresses.

13.8.9.1 Viewing a List of Aggregate Address Options

To view a list of options for an aggregate address, type:

```
routing bgp aggregate-address { address } options
```

If options have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp aggregate-address 11.11.0.0/16 options
routing bgp
 aggregate-address 11.11.0.0/16
  options summary-only
  !
 !
```

```
!
```

If no options have been configured, add options as needed. For more information, refer to "Adding an Aggregate Address Option" (Page 649).

13.8.9.2 Adding an Aggregate Address Option

To add an option for an aggregate address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the path by typing:

   ```
   routing bgp aggregate-address { address } options [ summa
   ry-only | as-set ]
   ```

   Where:

   - { address } is the subnet address and prefix for the aggregate address
3. Type `commit` and press **Enter** to save the changes.

13.8.9.3 Deleting an Aggregate Address Option

To delete an option for an aggregate address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the option by typing:

   ```
   no routing bgp aggregate-address { address } options
   [ { summary-only } | { as-set } ]
   ```

   Where:

   - `{ address }` is the subnet address and prefix for the aggregate address
3. Type `commit` and press **Enter** to save the changes.

13.8.10 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.

13.8.10.1 Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic BGP routes, type:

```
show running-config routing bgp redistribute
```

If metrics have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp redistribute
routing bgp
 redistribute rip
  no metric
 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 650).

13.8.10.2 Adding a Redistribution Metric

To add a redistribution metric for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the metric by typing:

   ```
   routing bgp redistribute [ { rip } | { ospf } | { connect
   ed } | { static } | { kernel } ] metric { metric }
   ```

   Where:

   - `{ metric }` is the metric for redistributed routes
3. Type `commit` and press **Enter** to save the changes.

13.8.10.3 Deleting a Redistribution Metric

To delete a redistribution metric for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the metric by typing:

   ```
   no routing bgp redistribute [ { rip } | { ospf } | { con
   nected } | { static } | { kernel } ]
   ```

3. Type `commit` and press **Enter** to save the changes.

13.8.11 Managing Route Reflector Options

This section describes how to configure the device as a route reflector for BGP networks.

13.8.11.1 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).

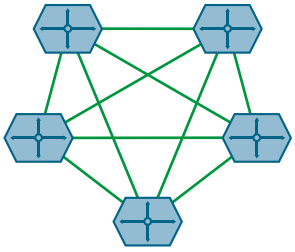


Figure 13.2 A Simple BGP Topology Without a Route Reflector

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.

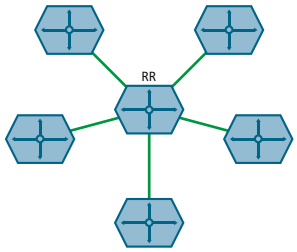
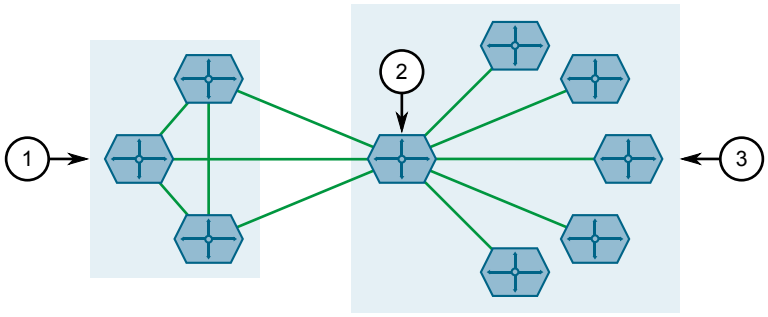


Figure 13.3 A Simple BGP Topology With a Route Reflector

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 13.4 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.

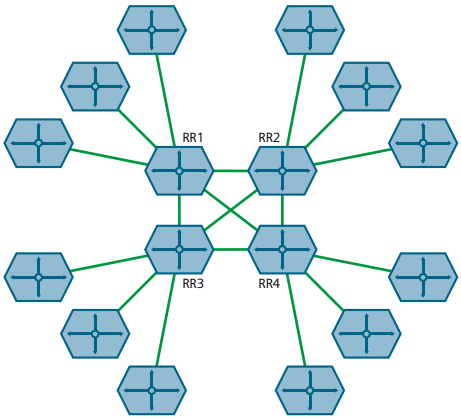


Figure 13.5 Multiple Clusters Fully-Meshed

Route reflectors can also be partially-meshed by combining them in a cluster of their own.

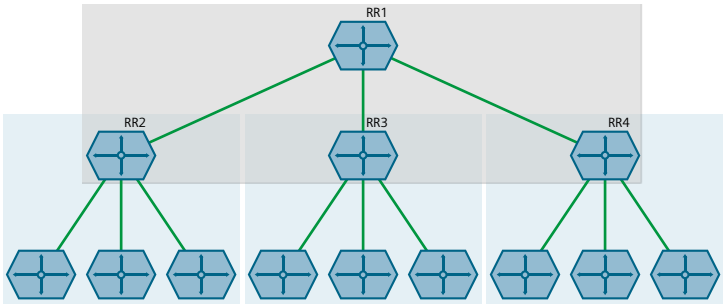
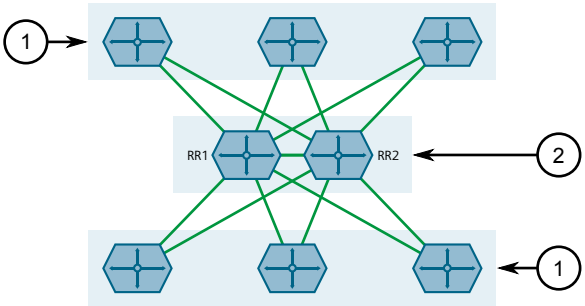


Figure 13.6 Multiple Clusters Partially-Meshed

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 13.7 Redundant Route Reflector Topology

13.8.11.2 Configuring the Device as a Route Reflector

To configure the device to be a route reflector for a specific cluster, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the device as a route reflector by typing:

   ```
   routing bgp route-reflector enabled cluster-id { id }
   ```

   Where { id } is the 4-byte ID of the cluster to which the device belongs (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 654).
4. Type `commit` and press **Enter** to save the changes.

13.8.11.3 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 642).
2. Configure the desired BGP neighbor to be a client of the route reflector by typing:

   ```
   routing bgp neighbor { address } route-reflector-client
   enabled
   ```

   Where { address } is the IP address of the BGP neighbor.
3. Type `commit` and press **Enter** to save the changes.

BGP Neighbors In an IPv4 Address Family

To configure a BPG 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 727).

2. Configure the desired BGP neighbor in the IPv4 address family to be a client of the route reflector by typing:

   ```
   routing bgp address-family vrf { definition } neighbor
   { address } route-reflector-client enabled
   ```

   Where:

   - { definition } is the name of the VRF definition
   - { address } is the IP address of the BGP neighbor

3. Type `commit` and press **Enter** to save the changes.

BGP Neighbors In a VPNv4 Address Family

To configure a BPG 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 725).
2. Configure the desired BGP neighbor in the VPNv4 address family to be a client of the route reflector by typing:

   ```
   routing bgp address-family vpnv4 { address } route-reflec
   tor-client enabled
   ```

   Where { address } is the IP address of the BGP neighbor.

3. Type `commit` and press **Enter** to save the changes.

13.8.11.4 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).

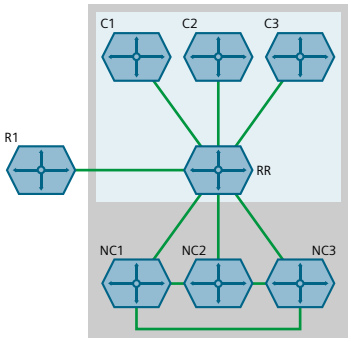


Figure 13.8 Basic Route Reflection Topology

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 654).
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 642).
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 654).

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
 !
!
```

13.8.11.5 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.

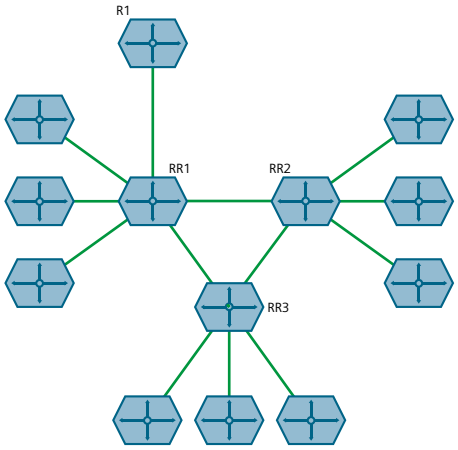


Figure 13.9 Linked Clusters

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 654).

2. For each route reflector, define the other route reflectors as BGP neighbors. For more information, refer to "Adding a Neighbor" (Page 642).

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
 !
!
```

13.8.11.6 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.

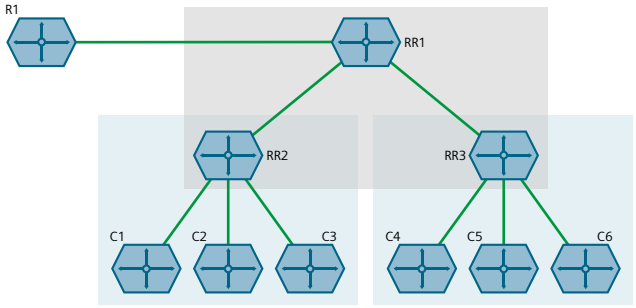


Figure 13.10 Hierarchical Clusters Topology

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 654).
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 654).

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
 !
!
```

13.8.11.7 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).

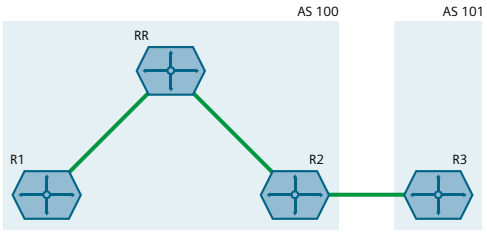


Figure 13.11 Route Reflection in a VRF Instance

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 715).

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 717).

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 662) to forward traffic to VRF1. For more information, refer to "Configuring a VRF Interface" (Page 714).

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 654).

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 727).

h. Define a redistribution metric for IPv4 family of type **connected**. For more information, refer to "Adding a Redistribution" (Page 728).

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 626).

b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.1.2

Parameter	Value
Autonomous System ID	100

For more information, refer to "Adding a Neighbor" (Page 642).

c. Define a redistribution metric for BGP of type **connected**. For more information, refer to "Adding a Redistribution Metric" (Page 650).

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 626).

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 642).

c. Define a redistribution metric for BGP of type **connected**. For more information, refer to "Adding a Redistribution Metric" (Page 650).

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 626).

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 642).

c. Define a redistribution metric for BGP of type **connected**. For more information, refer to "Adding a Redistribution Metric" (Page 650).

Verification

Verify the configuration by navigating to ***routing » status » bgp » route*** on R1. The following routes should be displayed:

```
                                                    LOCAL              AS
NETWORK       ADDRESS      SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  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
```

13.8.11.8 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]".

13.8.12 Viewing the Status of Dynamic BGP Routes

To view the status of the dynamic BGP routes configured on the device, type:

```
show routing status bgp route
```

If BGP routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status bgp route | tab
                                                          LOCAL              AS
NETWORK       ADDRESS      SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
-------------------------------------------------------------------------------------
192.168.1.0
              192.168.1.2  true      true      0       100         0             IGP
192.168.6.0
              2.0.0.1      true      false     0                   0       200   IGP
192.168.12.0
              192.168.1.2  true      true      0       100         0             IGP
192.168.13.0
              0.0.0.0      true      false     0                   32768         IGP
```

The list provides the following information:

Parameter	Description
`network`	**Synopsis:** A string Network.
`{ address }`	**Synopsis:** A string Next-hop address.
`selected`	**Synopsis:** [true | false] Selected next-hop for this route.
`internal`	**Synopsis:** [true | false] Internal route.
`metric`	**Synopsis:** A string Metric.
`local-preference`	**Synopsis:** A string Local preference.
`weight`	**Synopsis:** An integer Weight.

Parameter	Description
as-path	**Synopsis:** A string AS path.
origin	**Synopsis:** A string Origin.

To view the routing information advertised to the network by a BGP neighbor, type:

```
show routing status bgp neighbor { IP Address } adver
tised-router
```

Where:

- { IP Address } is the IP address of a specific neighbor

If BGP neighbors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status bgp neighbor 2.0.0.2 advertised-route | tab
                                                                LOCAL
NETWORK             NEXT HOP         SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  AS PATH
         ORIGIN
-------------------------------------------------------------------------------------------------
192.168.11.0        2.0.0.1          true      true      0                   32768   100 100 100 100
 100 ...  IGP
192.168.12.0        2.0.0.1          true      true      0       100         0       100 100 100 100
 100 ...  IGP
```

The list provides the following information:

Parameter	Description
{ network }	**Synopsis:** A string Network.
next-hop	**Synopsis:** A string Next-hop address.
selected	**Synopsis:** [true | false] Selected next-hop for this route.
internal	**Synopsis:** [true | false] Internal route.
metric	**Synopsis:** An integer Metric value.
local-preference	**Synopsis:** A string Local preference.
weight	**Synopsis:** An integer Weight.

Parameter	Description
`as-path`	**Synopsis:** A string Path.
`origin`	**Synopsis:** 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 626).

13.8.13 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:

   ```
   routing dynamic bgp all-peers-reset
   ```

2. Configure the following parameter(s) as required:

Parameter	Description
`reset-type { reset-type }`	**Synopsis:** [hard | soft-inbound | soft-outbound | soft] The method for resetting all BGP peering sessions. Options include: • hard: Tears down and re-establishes all BGP sessions. • soft: The existing peering sessions continue to run while running both inbound and outbound actions. • soft-inbound: The existing peering sessions continue to run while generating inbound updates from all neighbors. • soft-outbound: The existing peering sessions continue to run while sending outbound updates to all neighbors.

3. Type `commit` and press **Enter** to save the changes.

Resetting a BGP Session for a Specified Neighbor

To reset a BGP session for a specified neighbor, do the following:

1. Navigate to:

   ```
   routing dynamic bgp neighbor { ip address } peer-reset
   ```

   Where:

   - `{ ip address }` is the ip address of the neighbor
2. Configure the following parameter(s) as required:

Parameter	Description
`reset-type { reset-type }`	**Synopsis:** [hard | soft-inbound | soft-outbound | soft] The method for resetting the selected BGP peering session. Options include: • hard: Tears down the existing peering session then re-establishes it. • soft: The existing peering session continues to run while running both inbound and outbound actions. • soft-inbound: The existing peering session continues to run while generating inbound updates from its neighbor. • soft-outbound: The existing peering session continues to run while sending outbound updates to its neighbor.

3. Type `commit` and press **Enter** to save the changes.

13.9 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] compliant implementation of OSPF version 2. The daemon also adheres to the Opaque LSA (RFC 2370 [http://tools.ietf.org/html/rfc2370]) and ABR-Types (RFC 3509 [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 711).

13.9.1 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.

13.9.2 Configuring OSPF

To configure dynamic routing using the Open Shortest Path First (OSPF) daemon, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***routing » ospf*** and configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables the OSPF dynamic routing protocol.
`abr-type { abr-type }`	**Synopsis:** [cisco | ibm | shortcut | standard] **Default:** cisco The OSPF ABR type.
`auto-cost-reference-bandwidth { auto-cost-reference-bandwidth }`	**Synopsis:** An integer between 1 and 4294967 **Default:** 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
`compatible-rfc1583`	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
`default-information-originate`	Advertises the default route.
`default-metric { default-metric }`	**Synopsis:** An integer between 0 and 16777214 The default metric of redistribute routes.
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The administrative distance.
`opaque-lsa`	Enables the Opaque-LSA capability (RFC2370).
`passive-default { passive-default }`	**Synopsis:** [true | false] **Default:** true Default passive value for new interface.
`refresh-timer { refresh-timer }`	**Synopsis:** An integer between 10 and 1800 **Default:** 10 The refresh timer.
`router-id { router-id }`	**Synopsis:** A string between 7 and 15 characters long The Router ID for OSPF.

3. Configure the OSPF distance settings by configuring the following parameters:

Parameter	Description
`external { external }`	**Synopsis:** An integer between 1 and 255 The administrative distance for external routes.
`inter-area { inter-area }`	**Synopsis:** An integer between 1 and 255 The administrative distance for inter-area routes.

Parameter	Description
`intra-area { intra-area }`	**Synopsis:** An integer between 1 and 255 The administrative distance for intra-area routes.

4. Configure the OSPF distance settings by configuring the following parameters:

Parameter	Description
`external { external }`	**Synopsis:** An integer between 1 and 255 The administrative distance for external routes.
`inter-area { inter-area }`	**Synopsis:** An integer between 1 and 255 The administrative distance for inter-area routes.
`intra-area { intra-area }`	**Synopsis:** An integer between 1 and 255 The administrative distance for intra-area routes.

5. If **default-information-originate** was enabled in step 3 (Page 670), configure the following:

Parameter	Description
`always { always }`	**Synopsis:** [true | false] **Default:** false Always advertise default route even when there is no default route present in routing table.
`metric { metric }`	**Synopsis:** An integer between 0 and 16777214 The metric value for default route.
`metric-type { metric-type }`	**Synopsis:** An integer between 1 and 2 **Default:** 2 The metric type for default route.
`route-map { route-map }`	**Synopsis:** 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 676).
7. Configure areas. For more information, refer to "Adding an Area" (Page 679).
8. Configure route map filters. For more information, refer to "Adding a Route Map Filter" (Page 682).
9. Configure redistribution metrics. For more information, refer to "Adding a Redistribution Metric" (Page 687).
10. Configure interfaces. For more information, refer to "Configuring a Routing Interface" (Page 689).
11. Type `commit` and press **Enter** to save the changes.

13.9.3 Viewing the Status of Dynamic OSPF Routes

To view the status of the dynamic OSPF routes configured on the device, type:

```
show routing status ospf route network
```

If OSPF routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ospf route network | tab
ID              DISCARD  INTER AREA  COST  AREA     HOW
-------------------------------------------------------------------------------
192.168.1.0/24  no       intra area  10    0.0.0.0
                                                    directly attached to fe-1-2
192.168.2.0/24  no       intra area  10    0.0.0.0
                                                    directly attached to fe-1-4
```

This list provides the following information:

Parameter	Description
`{ id }`	**Synopsis:** A string Network Prefix.
`destination`	**Synopsis:** A string Destination (network or discard).
`path-type`	**Synopsis:** A string Path type (inter-area or intra-area).
`cost`	**Synopsis:** A string Cost.
`area`	**Synopsis:** A string Area.
`how`	**Synopsis:** A string How to reach this network.

To view the status of the dynamic OSPF neighbor configured on the device, type:

```
show routing status ospf neighbor
```

If an OSPF neighbor have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ospf neighbor
                                                                          DEAD
ID           ADDRESS         INTERFACE                   PRIORITY  STATE       TIME
-------------------------------------------------------------------------------------
21.21.21.21  192.168.212.21  switch.0212:192.168.212.22  1         Full/Backup 31.249s
```

This list provides the following information:

Parameter	Description
`{ id }`	**Synopsis:** A string Neighbor ID.
`{ address }`	**Synopsis:** A string Address.
`{ interface }`	**Synopsis:** A string Interface.
`priority`	**Synopsis:** A string Priority.
`state`	**Synopsis:** A string State.
`dead-time`	**Synopsis:** A string Dead Time.

To view the status of the dynamic OSPF database configured on the device, type:

```
show routing status ospf database
```

If an OSPF neighbor have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ospf database
 router
                                                          LINK
ID           AREA     ADV ROUTER   AGE   SEQNUM      COUNT
-------------------------------------------------------------
21.21.21.21  0.0.0.0  21.21.21.21  1307  0x80000017  2
22.22.22.22  0.0.0.0  22.22.22.22  614   0x8000001c  1
22.22.22.22  0.0.0.1  22.22.22.22  1364  0x8000000e  1

 net
ID              AREA     ADV ROUTER   AGE  SEQNUM
-----------------------------------------------------
192.168.212.22  0.0.0.0  22.22.22.22  584  0x80000009

 summary
ID             AREA     ADV ROUTER   AGE   SEQNUM      ROUTE
-------------------------------------------------------------------------
192.168.22.0   0.0.0.0  22.22.22.22  1354  0x80000008  192.168.22.0/24
192.168.21.0   0.0.0.1  22.22.22.22  1434  0x80000009  192.168.21.0/24
192.168.212.0  0.0.0.1  22.22.22.22  44    0x80000008  192.168.212.0/24

 as-external
                                          METRIC
```

This list provides the following information:

Router

Parameter	Description
`area`	**Synopsis:** A string Area.
`{ link-id }`	**Synopsis:** A string Link ID.
`{ adv-router }`	**Synopsis:** A string Advertising Router.
`age`	**Synopsis:** A string Age.
`seqnum`	**Synopsis:** A string Sequence number.
`checksum`	**Synopsis:** A string Checksum.
`link-count`	**Synopsis:** A string Link count.

Net

Parameter	Description
`area`	**Synopsis:** A string Area ID.
`{ link-id }`	**Synopsis:** A string Link ID.
`{ adv-router }`	**Synopsis:** A string Advertising Router.
`age`	**Synopsis:** A string Age.
`seqnum`	**Synopsis:** A string Sequence number.

Summary

Parameter	Description
`area`	**Synopsis:** A string Area ID.
`{ link-id }`	**Synopsis:** A string Link ID.

Parameter	Description
`{ adv-router }`	**Synopsis:** A string Advertising Router.
`age`	**Synopsis:** A string Age.
`seqnum`	**Synopsis:** A string Sequence number.
`route`	**Synopsis:** A string Route.

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 669).

13.9.4 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.

13.9.4.1 Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic OSPF routes, type:

- **For Standard OSPF Routes**
  `routing ospf filter prefix-list`
- **For VRF Routes via OSPF**
  `routing ospf vrf { vrf } filter prefix-list`

Where:

- `{ vrf }` is the name of the chosen VRF

If prefix lists have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf filter prefix-list | tab
NAME                 DESCOSPFTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22   -
                                   100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11  -
                                   100  permit  192.168.33.0/24  -   -
                                   200  permit  192.168.33.0/24  32  -

!
```

If no prefix lists have been configured, add lists as needed. For more information, refer to "Adding a Prefix List" (Page 676).

13.9.4.2 Viewing a List of Prefix Entries

To view a list of entries for dynamic OSPF, OSPF, or OSPF prefix lists, type:

- **For Standard OSPF Routes**
  `routing ospf filter prefix-list { name } entry`
- **For VRF Routes via OSPF**
  `routing ospf vrf { vrf } filter prefix-list { name } entry`

Where:

- `{ vrf }` is the name of the chosen VRF
- `{ name }` is the name of the prefix list

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -

 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 677).

13.9.4.3 Adding a Prefix List

To add a prefix list for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the list by typing:
   - **For Standard OSPF Routes**
     `routing ospf filter prefix-list { name }`
   - **For VRF Routes via OSPF**
     `routing ospf vrf { vrf } filter prefix-list { name }`

   Where:
   - `{ vrf }` is the name of the chosen VRF
   - `{ name }` is the name of the prefix list
3. Configure the following parameter(s) as required:

Parameter	Description
`description { description }`	**Synopsis:** A string up to 1024 characters long The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to "Adding a Prefix Entry" (Page 677).
5. Type `commit` and press **Enter** to save the changes.

13.9.4.4 Adding a Prefix Entry

To add an entry for a dynamic OSPF prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the entry by typing:
   - **For Standard OSPF Routes**
     ```
     routing ospf filter prefix-list { name } entry { number }
     ```
   - **For VRF Routes via OSPF**
     ```
     routing ospf vrf { vrf } filter prefix-list { name } entry { number }
     ```

   Where:
   - `{ vrf }` is the name of the chosen VRF
   - `{ name }` is the name of the prefix list
   - `{ number }` is the sequence number for the entry
3. Configure the following parameter(s) as required:

Parameter	Description
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit Action.
`subnet { subnet }`	**Synopsis:** A string between 9 and 18 characters long Network (xxx.xxx.xxx.xxx/xx).
`le { le }`	**Synopsis:** An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
`ge { ge }`	**Synopsis:** An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

4. Type `commit` and press **Enter** to save the changes.

13.9.4.5 Deleting a Prefix List

To delete a prefix list for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.

   Note

   Deleting a prefix list removes all associate prefix entries as well.

2. Delete the list by typing:
   - **For Standard OSPF Routes**

     ```
     no routing ospf filter prefix-list { name }
     ```
   - **For VRF Routes via OSPF**

     ```
     no routing ospf vrf { vrf } filter prefix-list { name }
     ```

   Where:
   - `{ vrf }` is the name of the chosen VRF
   - `{ name }` is the name of the prefix list
3. Type `commit` and press **Enter** to save the changes.

13.9.4.6 Deleting a Prefix Entry

To delete an entry for a dynamic OSPF prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:
   - **For Standard OSPF Routes**

     ```
     no routing ospf filter prefix-list { name } entry
     { number }
     ```
   - **For VRF Routes via OSPF**

     ```
     no routing ospf vrf { vrf } filter prefix-list { name }
     entry { number }
     ```

   Where:
   - `{ vrf }` is the name of the chosen VRF
   - `{ name }` is the name of the prefix list
   - `{ number }` is the sequence number for the entry
3. Type `commit` and press **Enter** to save the changes.

13.9.5 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).

13.9.5.1 Viewing a List of Areas

To view a list of areas configured for dynamic OSPF routes, type:

- **For Standard OSPF Routes**

  ```
  show running-config routing ospf area
  ```

- **For VRF Routes via OSPF**

  ```
  show running-config routing ospf vrf { vrf } area
  ```

Where:

- `{ vrf }` is the name of the chosen VRF

If areas have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf area | tab
AREA     NETWORK
--------------------------
0.0.0.0  192.168.12.0/24

!
```

If no areas have been configured, add areas as needed. For more information, refer to "Adding an Area" (Page 679).

13.9.5.2 Adding an Area

To add an area for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the area by typing:
   - **For Standard OSPF Routes**

     ```
     routing ospf area { id } { network/prefix }
     ```

   - **For VRF Routes via OSPF**

     ```
     routing ospf vrf { vrf } area { id } { network/prefix }
     ```

Where:

- `{ vrf }` is the name of the chosen VRF
- `{ id }` is the ID for the OSPF area. The ID must be in the format of *A.B.C.D*.
- `{ network/prefix }` is the network and prefix for the OSPF area.

3. Configure the following parameter(s) as required:

Parameter	Description
`shortcut { shortcut }`	**Synopsis:** [default | disable | enable] **Default:** default Sets the area's shortcutting mode. Options include: • Default: 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. • Enable: 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. • Disable: The ABR does not use this area for shortcutting, or set the new bit (S-bit) in the router-LSA originated for it.

4. Type `commit` and press **Enter** to save the changes.

13.9.5.3 Deleting an Area

To delete an area for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the area by typing:
   - **For Standard OSPF Routes**
     ```
     no routing ospf area { id } { network/prefix }
     ```
   - **For VRF Routes via OSPF**
     ```
     no routing ospf vrf { vrf } area { id } { network/pre
     fix }
     ```

   Where:

   - `{ vrf }` is the name of the chosen VRF
   - `{ id }` is the ID for the OSPF area. The ID must be in the format of *A.B.C.D*
   - `{ network/prefix }` is the network and prefix for the OSPF area
3. Type `commit` and press **Enter** to save the changes.

13.9.6 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.

13.9.6.1 Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic OSPF routes, type:

- **For Standard OSPF Routes**
  `show running-config routing ospf filter route-map`
- **For VRF Routes via OSPF**
  `show running-config routing ospf vrf { vrf } filter route-map`

Where:

- `{ vrf }` is the name of the chosen VRF

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf filter route-map | tab
                        ON
                        MATCH  AS    PREFIX  PREFIX  PREFIX                                LOCAL
                    NEXT          ORIGINATOR
TAG  SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
  OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT
-------------------------------------------------------------------------------------------------
map
     10   permit  -     -      -     -       -       -       -       -     -       -   -   -
  -          -      -     -       -           -

!
```

If no filters have been configured, add filters as needed. For more information, refer to "Adding a Route Map Filter" (Page 682).

13.9.6.2 Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either OSPF, type:

- **For Standard OSPF Routes**

  ```
  show running-config routing ospf filter route-map { tag }
  entry
  ```

- **For VRF Routes via OSPF**

  ```
  show running-config routing ospf vrf { vrf } filter route-
  map { tag } entry
  ```

Where:

- `{ vrf }` is the name of the chosen VRF
- `{ tag }` is the tag for the route map filter

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf filter route-map map entry | tab
                  ON
                  MATCH  AS    PREFIX  PREFIX  PREFIX                                LOCAL
              NEXT          ORIGINATOR
SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE  OP
ERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
-------------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -           -
       -      -     -       -           -

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to "Adding a Route Map Filter Entry" (Page 683).

13.9.6.3 Adding a Route Map Filter

To add a route map filter for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:
   - **For Standard OSPF Routes**

     ```
     routing ospf filter route-map { tag }
     ```

   - **For VRF Routes via OSPF**

     ```
     routing ospf vrf { vrf } filter route-map { tag }
     ```

   Where:

   - `{ vrf }` is the name of the chosen VRF
   - `{ tag }` is the tag for the route map filter
3. Add one or more entries. For more information, refer to "Adding a Route Map Filter Entry" (Page 683).
4. Type `commit` and press **Enter** to save the changes.

13.9.6.4 Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:
   - **For Standard OSPF Routes**
     ```
     routing ospf filter route-map { tag } entry { number }
     ```
   - **For VRF Routes via OSPF**
     ```
     routing ospf vrf { vrf } filter route-map { tag } entry
     { number }
     ```

     Where:
     - `{ vrf }` is the name of the chosen VRF
     - `{ tag }` is the tag for the route map filter
     - `{ number }` is the sequence number for the entry
3. Configure the following parameter(s) as required:

Parameter	Description
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit Action.
`call { call }`	**Synopsis:** A string between 1 and 1024 characters long Jump to another route-map after match+set.
`on-match-goto { on-match-goto }`	**Synopsis:** An integer between 1 and 65535 Go to this entry on match.
`metric { metric }`	**Synopsis:** An integer Metric value.
`metric-type { metric-type }`	**Synopsis:** An integer between 1 and 2 External route type.

4. Configure the match rules for the route map filter. For more information, refer to "Configuring Match Rules" (Page 684).
5. Type `commit` and press **Enter** to save the changes.

13.9.6.5 Deleting a Route Map Filter

To delete a route map filter for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

- **For Standard OSPF Routes**

  ```
  no routing ospf filter route-map { tag }
  ```

- **For VRF Routes via OSPF**

  ```
  no routing ospf vrf { vrf } filter route-map { tag }
  ```

  Where:

  - `{ vrf }` is the name of the chosen VRF
  - `{ tag }` is the tag for the route map filter

3. Type `commit` and press **Enter** to save the changes.

13.9.6.6 Deleting a Route Map Filter Entry

To delete an entry for a route map filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

   - **For Standard OSPF Routes**

     ```
     no routing ospf filter route-map { tag } entry { num
     ber }
     ```

   - **For VRF Routes via OSPF**

     ```
     no routing ospf vrf { vrf } filter route-map { tag }
     entry { number }
     ```

     Where:

     - `{ vrf }` is the name of the chosen VRF
     - `{ tag }` is the tag for the route map filter
     - `{ number }` is the sequence number for the entry

3. Type `commit` and press **Enter** to save the changes.

13.9.6.7 Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to either:

   - **For Standard OSPF Routes**
     routing » dynamic » ospf » filter » route-map » { tag } » entry » { number } » match
   - **For VRF Routes via OSPF**
     routing » dynamic » ospf » vrf » { vrf } » filter » route-map » { tag } » entry » { number } » match

Where:

- { vrf } is the chosen VRF
- { tag } is the tag for the route map filter
- { number } is the sequence number for the entry

3. Configure the following parameters as required:

Parameter	Description
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.
`ifname { ifname }`	**Synopsis:** A string between 1 and 32 characters long The interface name.

4. Type `commit` and press **Enter** to save the changes.

13.9.7 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 681).

13.9.7.1 Viewing List of Incoming Route Filters

To view a list of route filters configured for incoming advertised routes, type:

- **For Standard OSPF Routes**

  ```
  show running-config routing ospf incoming-route-filter
  ```

- **For VRF Routes via OSPF**

  ```
  show running-config routing ospf vrf { vrf } incoming-route-filter
  ```

Where:

- `{ vrf }` is the name of the chosen VRF

If route filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf incoming-route-filter
```

```
routing ospf
 incoming-route-filter ospf_route_1
 !
!
```

If no route filters have been configured, add filters as needed. For more information, refer to "Adding an Incoming Route Filter" (Page 686).

13.9.7.2 Adding an Incoming Route Filter

To add a route filter for incoming advertised routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a route map has been configured. For more information, refer to "Managing Route Maps" (Page 681).
3. Create the new incoming route filter by typing:
   - **For Standard OSPF Routes**

     `routing ospf incoming-route-filter { route-map }`
   - **For VRF Routes via OSPF**

     `routing ospf vrf { vrf } incoming-route-filter { route-map }`

   Where:
   - `{ vrf }` is the name of the chosen VRF
   - `{ route-map }` is the name of the route map
4. Type `commit` and press **Enter** to save the changes.

13.9.7.3 Deleting an Incoming Route Filter

To delete a route filter configured for incoming advertised routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:
   - **For Standard OSPF Routes**

     `no routing ospf incoming-route-filter { route-map }`
   - **For VRF Routes via OSPF**

     `no routing ospf vrf { vrf } incoming-route-filter { route-map }`

   Where:
   - `{ vrf }` is the name of the chosen VRF
   - `{ route-map }` is the name of the route map
3. Type `commit` and press **Enter** to save the changes.

13.9.8 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.

13.9.8.1 Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic OSPF routes, type:

- **For Standard OSPF Routes**

  ```
  routing ospf redistribute
  ```

- **For VRF Routes via OSPF**

  ```
  routing ospf vrf { vrf } redistribute
  ```

Where:

- `{ vrf }` is the name of the chosen VRF

If metrics have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf redistribute
routing ospf
 redistribute bgp
  no metric-type
  no metric
 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to "Adding a Redistribution Metric" (Page 687).

13.9.8.2 Adding a Redistribution Metric

To add a redistribution metric for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the metric by typing:
   - **For Standard OSPF Routes**

     ```
     routing ospf redistribute [ { bgp } | { rip } |
     { connected } | { static } | { kernel } ]
     ```

   - **For VRF Routes via OSPF**

     ```
     routing ospf vrf { vrf } redistribute [ { bgp } |
     { rip } | { connected } | { static } | { kernel }
      ]
     ```

     Where:

     - `{ vrf }` is the name of the chosen VRF

3. Configure the following parameter(s) as required:

Parameter	Description
`metric-type { metric-type }`	**Synopsis:** An integer between 1 and 2 **Default:** 2 The OSPF exterior metric type for redistributed routes.
`metric { metric }`	**Synopsis:** An integer between 0 and 16777214 The metric for redistributed routes.
`route-map { route-map }`	**Synopsis:** A string between 1 and 1024 characters long The route map name.

4. Type `commit` and press **Enter** to save the changes.

13.9.8.3 Deleting a Redistribution Metric

To delete a redistribution metric for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the metric by typing:
   - **For Standard OSPF Routes**
     ```
     no routing ospf redistribute [ { bgp } | { rip } | { connected } | { static } | { kernel } ]
     ```
   - **For VRF Routes via OSPF**
     ```
     no routing ospf vrf { vrf } redistribute [ { bgp } | { rip } | { connected } | { static } | { kernel } ]
     ```

   Where:
   - `{ vrf }` is the name of the chosen VRF
3. Type `commit` and press **Enter** to save the changes.

13.9.9 Managing Routing Interfaces

This section describes how to manage interfaces for OSPF routes.

13.9.9.1 Viewing a List of Routing Interfaces

To view a list of routing interfaces for an OSPF network, type:

- **For Standard OSPF Routes**
  ```
  show running-config routing ospf interface
  ```

- **For VRF Routes via OSPF**

  `show running-config routing ospf vrf { vrf } interface`

Where:

- `{ vrf }` is the name of the chosen VRF

A table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf interface | tab
                                        MINIMAL
                                DEAD    HELLO       HELLO                       RETRANSMIT
 TRANSMIT  KEY
IFNAME       AUTHENTICATION  COST  INTERVAL  MULTIPLIER  INTERVAL  PRIORITY  PASSIVE  INTERVAL    DE
LAY     ID   MD5
-------------------------------------------------------------------------------------------------
dummy0       -               -     40        -           10        1         true     5           1
fe-cm-1      -               -     40        -           10        1         true     5           1
switch.0001  -               -     40        -           10        1         true     5           1
```

13.9.9.2 Configuring a Routing Interface

To configure a routing interface for an OSPF network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to either:
   - **For Standard OSPF Routes**
     routing » dynamic » ospf » interface » { name }
   - **For VRF Routes via OSPF**
     routing » dynamic » ospf » vrf » { vrf } » interface » { name }

   Where:

   - { vrf } is the chosen VRF
   - { name } is the name of the interface
3. Configure the dead interval settings by typing the following commands:

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 `minimal-hello-multiplier` 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 { dead-interval }`	**Synopsis:** An integer between 1 and 65535 **Default:** 40 The time before considering a router dead (in seconds).
`minimal-hello-multiplier { minimal-hello-multiplier }`	**Synopsis:** An integer between 1 and 10 The number of times a hello message can be sent within one second.

4. Configure the interface settings by typing the following commands:

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 267).

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 { authentication }`	**Synopsis:** [message-digest | null] The authentication type on this interface.

Parameter	Description
`cost { cost }`	**Synopsis:** 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 { hel lo-interval }`	**Synopsis:** An integer between 1 and 65535 **Default:** 10 The time (in seconds) between sending hello packets.
`priority { priority }`	**Synopsis:** An integer between 0 and 255 **Default:** 1 Priority of interface.
`passive { passive }`	**Synopsis:** [true | false] **Default:** 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 { retransmit-inter val }`	**Synopsis:** An integer between 1 and 65535 **Default:** 5 Time (in seconds) between retransmitting lost link state advertisements.
`transmit-delay { transmit-delay }`	**Synopsis:** An integer between 1 and 65535 **Default:** 1 The link state transmit delay (in seconds).

5. Type `commit` and press **Enter** to save the changes.

13.9.10 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.

13.9.10.1 Viewing a List of Message Digest Keys

To view a list of message digest keys for an OSPF routing interface, type:

- **For Standard OSPF Routes**

  ```
  show running-config routing ospf interface { name } mes
  sage-digest-key
  ```

- **For VRF Routes via OSPF**

  ```
  show running-config routing ospf interface { name } mes
  sage-digest-key
  ```

Where:

- `{ vrf }` is the name of the chosen VRF
- `{ name }` is the name of the routing interface

If keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf interface switch.0001 message-di
gest-key
routing ospf
 interface switch.0001
  message-digest-key 1
   md5 RUGGEDCOM
  !
 !
!
```

If no message digest keys have been configured, add keys as needed. For more information, refer to "Adding a Message Digest Key" (Page 692).

13.9.10.2 Adding a Message Digest Key

To add a message digest key to an OSPF routing interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the key by typing:
   - **For Standard OSPF Routes**

     ```
     routing ospf interface { name } message-digest-key
     { id }
     ```

   - **For VRF Routes via OSPF**

     ```
     routing ospf vrf { vrf } interface { name } message-di
     gest-key { id }
     ```

Where:

- `{ vrf }` is the name of the chosen VRF
- `{ name }` is the name of the routing interface
- `{ id }` is the ID for the message digest key

3. Type `commit` and press **Enter** to save the changes.

13.9.10.3 Deleting a Message Digest Key

To delete a message digest key from an OSPF routing interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the key by typing:
   - **For Standard OSPF Routes**

     ```
     no routing ospf interface { name } message-digest-key
     { id }
     ```

   - **For VRF Routes via OSPF**

     ```
     no routing ospf vrf { vrf } interface { name } mes
     sage-digest-key { id }
     ```

   Where:

   - `{ vrf }` is the name of the chosen VRF
   - `{ name }` is the name of the routing interface
   - `{ id }` is the ID for the message digest key
3. Type `commit` and press **Enter** to save the changes.

13.9.11 Managing ABR Route Summarization

An inherent problem with OSFP 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.

13.9.11.1 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.

13.9.11.2 Viewing a List of Summary Routes

To view a list of summary routes configured on the device, type:

```
show running-config routing ospf area-range
```

If summary routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf area-range | tab
                          ACTION
AREA ID  AREA RANGE       TYPE       COST
-----------------------------------------
0.0.0.0  192.168.10.0/24  advertise  -
0.0.0.1  172.168.1.0/24   advertise  -

!
```

If no summary routes have been configured, add routes as needed. For more information, refer to "Adding a Summary Route" (Page 694).

13.9.11.3 Adding a Summary Route

To add a summary route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the area range by typing:

   ```
   routing ospf area-range { area-id } { network-prefix } ac
   tion-type [ advertise | not-advertise ] cost { cost }
   ```

   Where:

   - { area-id } is the ID (in the form of A.B.C.D) of the area to be summarized
   - { network-prefix } is the network range and prefix of the associated area
   - { cost } is the cost of the summarized route
3. Type `commit` and press **Enter** to save the changes.

13.9.11.4 Deleting a Summary Route

To delete a summary route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the area range by typing:

   ```
   no routing ospf area-range { area-id } { network-prefix }
   ```

   Where:

   - { area-id } is the ID (in the form of A.B.C.D) of the area to be summarized
   - { network-prefix } is the network range and prefix of the associated area
3. Type `commit` and press **Enter** to save the changes.

13.9.11.5 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)

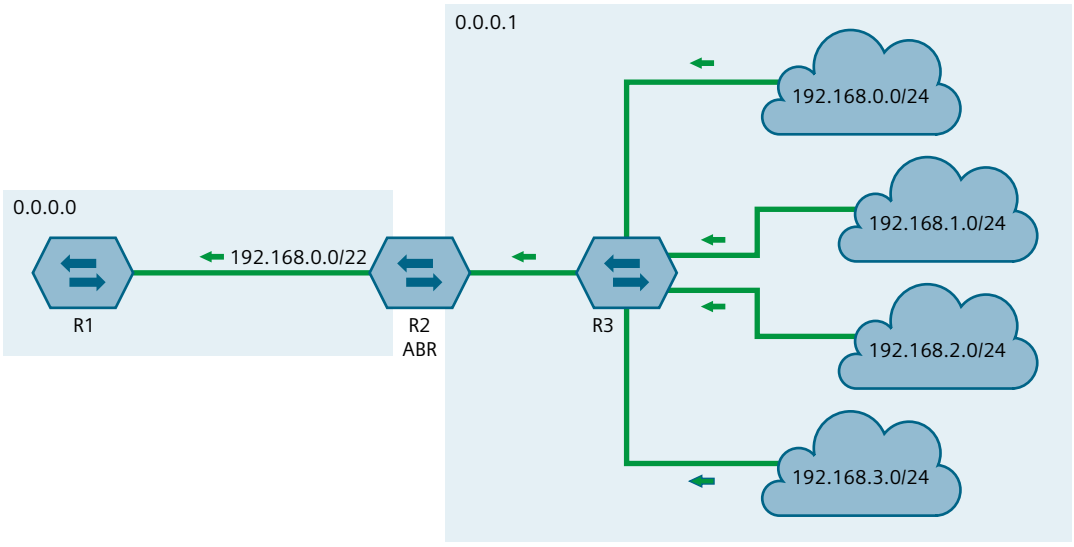


Figure 13.12 Basic ABR Router Summarization

Configuring a Summary Route to Summarize LSAs

To configure a summary route for R2, do the following:

1. Assign IP interfaces to interfaces.

Interface	IP Address/Prefix
fe-1	172.168.1.2/24
fe-2	192.168.10.2/24

2. Configure OSPF.
   a. Enable OSPF
   b. 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

   c. Define fe-1 and fe-2 as routing interfaces.
3. 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

4. On R1, review the routing table and verify the only LSA recieved 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
192.168.0.0/22	**192.168.10.2**	**fe-1-2**	**zebra**		**20**
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:

1. Navigate to area range 0.0.0.1 for IP address 192.168.0.0/22.
2. Change **cost** to any number between 1 and 65535.
3. 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		**30**
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:

1. Navigate to area range 0.0.0.1 for IP address 192.168.0.0/22.
2. Change **action-type** from **advertise** to **not-advertise**.

3. 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		

13.10 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.

13.10.1 Viewing the Status of IP Binding

To view the status of the IP binding on the device, type:

```
show mpls status ip-binding
```

If IP binding has been configured, a table similar to the following example appears:

```
ruggedcom# show mpls status ip-binding
                 LOCAL                  REMOTE
PREFIX           LABEL     NEXT HOP     LABEL
-----------------------------------------------------
1.1.1.1/32       17        192.168.10.1  imp-null
2.2.2.2/32       18        192.168.10.1  imp-null
3.3.3.3/32       imp-null
4.4.4.4/32       imp-null
5.5.5.5/32       19        192.168.20.2  imp-null
6.6.6.6/32       20        192.168.20.2  imp-null
10.200.16.0/20   16
172.30.128.0/19  imp-null
192.168.10.0/24  imp-null
192.168.20.0/24  imp-null
192.168.100.0/24 21        192.168.10.1  imp-null
192.168.200.0/24 22        192.168.20.2  imp-null
```

This table provides the following information:

Parameter	Description
`prefix`	**Synopsis:** A string The destination address prefix.
`local-label`	**Synopsis:** A string The incoming (local) label.

Parameter	Description
next-hop	**Synopsis:** A string The destination next hop router.
remote-label	**Synopsis:** A string The remote label

13.10.2 Viewing the Status of the Forwarding Table

To view the status of the forwarding table on the device, type:

```
show mpls status forwarding-table
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls status forwarding-table
LOCAL  OUTGOING                    OUTGOING
LABEL  LABEL     PREFIX            INTERFACE    NEXT HOP      UPTIME
-------------------------------------------------------------------------
17     Pop       1.1.1.1/32        switch.0010  192.168.10.1  01:04:31
18     Pop       2.2.2.2/32        switch.0010  192.168.10.1  01:04:31
19     Pop       5.5.5.5/32        switch.0020  192.168.20.2  01:04:33
20     Pop       6.6.6.6/32        switch.0020  192.168.20.2  01:04:33
21     Pop       192.168.100.0/24  switch.0010  192.168.10.1  01:04:31
22     Pop       192.168.200.0/24  switch.0020  192.168.20.2  01:04:33
```

The following information is provided:

Parameter	Description
local-label	**Synopsis:** A string The incoming (local) label
outgoing-label	**Synopsis:** A string The outgoing (remote) label.
prefix	**Synopsis:** A string The destination address prefix.
outgoing-interface	**Synopsis:** A string The outgoing interface.
next-hop	**Synopsis:** A string The destination next hop router.
uptime	**Synopsis:** A string The time this entry has been up.

13.10.3 Enabling/Disabling MPLS

To enable MPLS routing, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable MPLS by typing the following commands:

   Enable

   ```
   mpls enable
   ```

   Disable

   ```
   no mpls enable
   ```

3. Type `commit` and press **Enter** to save the changes.

13.10.4 Managing the MPLS Interfaces

This section describes how to manage the MPLS interfaces.

13.10.4.1 Viewing the Status of MPLS Interfaces

To view the status of the MPLS interfaces on the device, type:

```
show mpls status interfaces
```

If MPLS interfaces have been enabled on the device, a table similar to the following example appears:

```
show mpls status interfaces
MPLS
INTERFACES   STATUS
--------------------
switch.0010  yes
switch.0020  yes
```

This table provides the following information:

Parameter	Description
`mpls-interfaces`	**Synopsis:** A string The interface that has been enabled for MPLS.
`status`	**Synopsis:** A string The operational status.

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 700).

13.10.4.2 Viewing a List of MPLS Interfaces

To view a list of MPLS interfaces, type:

```
show running-config mpls interface-mpls
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config mpls interface-mpls | tab
IFNAME     ENABLED
---------------------
fe-cm-1     false
switch.0001  false
switch.0010  true
switch.0020  false

!
```

Where:

- `{ IFNAME }` is the name of the interface
- `{ ENABLED }` refers to the status of the MPLS operation on the interface

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 700).

13.10.4.3 Enabling/Disabling an MPLS Interface

To enable or disable an MPLS interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable MPLS interfaces by typing the following commands:

   Enable

   ```
   mpls interface-mpls { interface } enable
   ```

   Disable

   ```
   no mpls interface-mpls { interface } enable
   ```

   Where:

   - `{ interface }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

13.10.5 Managing Static Label Binding

This section describes how to bind (or reserve) labels for IPv4 network prefixes.

13.10.5.1 Viewing the Status of Static Label Binding

To view the status of all configured static label binding, type:

```
show mpls status static-binding
```

If static label binding has been configured, a table similar to the following example appears:

```
ruggedcom# show mpls status static-binding
                 IN     OUT
IP ADDRESS       LABEL  LABEL  NEXTHOP
-----------------------------------------------
192.168.20.0/24   90     101    192.168.10.2
192.168.200.0/24  95     100    192.168.10.2
```

This table provides the following information:

Parameter	Description
`ip-address`	**Synopsis:** A string The destination address prefix.
`in-label`	**Synopsis:** A string The incoming (local) label.
`out-label`	**Synopsis:** A string The outgoing (remote) label.
`nexthop`	**Synopsis:** A string The destination next hop router.

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 702).

13.10.5.2 Viewing a List of Static Labels

To view a list of static labels, type:

```
show running-config mpls static-mpls binding ipv4
```

If static labels have been configured, a list similar to the following example appears:

```
ruggedcom# show running-config mpls static-mpls binding ipv4
mpls
 static-mpls
  binding
   ipv4
    dest-address 192.168.52.52/32
     next-hop  192.168.10.2
     out-label 16
    !
   !
  !
 !
```

```
!
```

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 702).

13.10.5.3 Adding a Static Label

To add a static label, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a static label by typing:

   ```
   mpls static-mpls binding ipv4 dest-address { address }
   ```

   Where:

   - `{ address }` is the destination address and prefix.
3. Configure the following parameter(s) as required:

Parameter	Description
`in-label { in-label }`	**Synopsis:** An integer between 16 and 1048575 The incoming label: integer 16 -> 1048575.
`next-hop { next-hop }`	**Synopsis:** A string between 7 and 15 characters long The IP address for the destination next-hop router.
`out-label { out-label }`	**Synopsis:** [explicit-null | implicit-null] or An integer between 16 and 1048575 The outgoing label: • **implicit null** - 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 of label lookups that need to be performed by the egress router • **explicit null** - 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

4. Type `commit` and press **Enter** to save the changes.

13.10.5.4 Deleting a Static Label

To delete a static label, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete a static label by typing:

   ```
   no mpls static-mpls binding ipv4 dest-address { address }
   ```

   Where:

   - `{ address }` is the destination address and prefix.

3. Type `commit` and press **Enter** to save the changes.

13.10.6 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).

13.10.6.1 Viewing the Status of Static Cross-Connects

To view the status of all configured static cross-connects, type:

```
show mpls status static-crossconnect
```

If static cross-connects have been configured, a table similar to the following example appears:

```
ruggedcom# show mpls status static-crossconnect
LOCAL  OUTGOING  OUTGOING
LABEL  LABEL     INTERFACE    NEXT HOP
-------------------------------------------
200    205       switch.0010  192.168.10.2
215    250       switch.0010  192.168.10.2
```

This table provides the following information:

Parameter	Description
`local-label`	**Synopsis:** A string The incoming (local) label.
`outgoing-label`	**Synopsis:** A string The outgoing (remote) label.
`outgoing-interface`	**Synopsis:** A string The outgoing interface.
`next-hop`	**Synopsis:** 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 704).

13.10.6.2 Viewing a List of Static Cross-Connects

To view a list of configured static cross-connects, type:

```
show running-config mpls static-mpls crossconnects
```

If static cross-connects have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config mpls static-mpls crossconnect | tab
       OUT                       OUT
LABEL  INTERFACE    NEXT HOP     LABEL
---------------------------------------
20     switch.0001  192.168.10.2  32

 !
!
```

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 704).

13.10.6.3 Adding a Static Cross-Connect

To add a static cross-connect, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a static cross-connect by typing:

   ```
   mpls static-mpls crossconnect in-label { in-label }
   ```

   Where:

   - `{ in-label }` is the incoming label
3. Configure the following parameter(s) as required:

Parameter	Description
`out-interface { out-interface }`	**Synopsis:** A string The outgoing interface.
`next-hop { next-hop }`	**Synopsis:** 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).

Parameter	Description
`out-label { out-label }`	**Synopsis:** [explicit-null | implicit-null] or An integer between 16 and 1048575 The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575.

4. Type `commit` and press **Enter** to save the changes.

13.10.6.4 Deleting a Static Cross-Connect

To delete a static cross-connect, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete a static cross-connect by typing:

   ```
   no mpls static-mpls crossconnect in-label { in-label }
   ```

   Where:

   - `{ in-label }` is the incoming label
3. Type `commit` and press **Enter** to save the changes.

13.10.7 Managing LDP

LDP (Label Distribution Protocol), defined by RFC 5036 [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.

13.10.7.1 Viewing the Status of LDP Binding

To view the status of the LDP binding on the device, type:

```
show mpls ldp status binding
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls ldp status binding
               LOCAL     NEXT      REMOTE
PREFIX         LABEL     HOP       LABEL     IN USE
```

```
-------------------------------------------------
1.1.1.1        17        2.2.2.2  imp-null  in-use
1.1.1.1        17        6.6.6.6  17
2.2.2.2        18        2.2.2.2  imp-null  in-use
2.2.2.2        18        6.6.6.6  18
3.3.3.3        imp-null
4.4.4.4        imp-null
5.5.5.5        19        2.2.2.2  19
5.5.5.5        19        6.6.6.6  imp-null  in-use
```

This table or list provides the following information:

Parameter	Description
`prefix`	**Synopsis:** A string The LDP transport prefix.
`local-label`	**Synopsis:** A string The incoming (local) label.
`next-hop`	**Synopsis:** A string The destination next hop router.
`remote-label`	**Synopsis:** A string The LDP remote label.
`in-use`	**Synopsis:** A string The LDP in-use flag.

13.10.7.2 Viewing the Status of the LDP Discovery Interfaces

To view the status of the LDP discovery interfaces on the device, type:

```
show mpls ldp status discovery
```

If LDP discovery interfaces have been configured, a table similar to the following example appears:

```
ruggedcom# show mpls ldp status discovery
status discovery
 local id 4.4.4.4
 interfaces
INTERFACE    SRC IP ADDR   PEER ID  PEER IP       STATE
-----------------------------------------------------------
switch.0010  192.168.10.2  2.2.2.2  192.168.10.1  OPER
switch.0020  192.168.20.1  6.6.6.6  192.168.20.2  OPER
```

This table provides the following information:

Parameter	Description
`interface`	**Synopsis:** A string The LDP discovery interface.

Parameter	Description
src-ip-addr	**Synopsis:** A string The LDP discovery source IP address.
peer-id	**Synopsis:** A string The LDP discovery peer ID.
peer-ip	**Synopsis:** A string LDP discovery peer IP address
state	**Synopsis:** A string The LDP discovery interface state.

For more information about configuring LDP discovery interfaces, refer to "Enabling/ Disabling an LDP Interface" (Page 710).

13.10.7.3 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, type:

```
show mpls ldp status neighbor local-node-information
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls ldp status neighbor local-node-information
                   KEEPALIVE
LDP ID   HOLDTIME  INTERVAL
------------------------------
4.4.4.4   15s       180s
```

The following information is provided:

Parameter	Description
ldp-id	**Synopsis:** A string The LDP ID of the neighbor local node.
hello-holdtime	**Synopsis:** A string LDP hello holdtime of the neighbor local node.
session-holdtime	**Synopsis:** A string The LDP session holdtime of the neighbor local node.

13.10.7.4 Viewing the Status of the LDP Neighbor Connection Information

To view the status of the LDP neighbor connection on the device, type:

```
show mpls ldp status neighbor connection-information
```

A table similar to the following example appears:

```
ruggedcom# show mpls ldp status neighbor connection-information
         TCP
PEER ID  CONNECTION    STATE  UPTIME
----------------------------------------
2.2.2.2  192.168.10.1  OPER   00:51:51
-        192.168.10.2
6.6.6.6  192.168.20.2  OPER   00:51:53
-        192.168.20.1
```

The following information is provided:

Parameter	Description
`peer-id`	**Synopsis:** A string The peer ID of the LDP neighbor connection.
`tcp-connection`	**Synopsis:** A string The TCP connection of the LDP neighbor connection.
`state`	**Synopsis:** A string The state of the LDP neighbor connection.
`uptime`	**Synopsis:** A string The up time of the LDP neighbor connection.

13.10.7.5 Viewing the Status of the LDP Neighbor Discovery Information

To view the status of the LDP neighbor discovery information on the device, type:

`show mpls ldp status neighbor discovery-information`

A table or list similar to the following example appears:

```
ruggedcom# show mpls ldp status neighbor discovery-information
                                                            P
                                                  P         KEEPALIVE
PEER ID  PEER IP       INTERFACE    LOCAL IP      HOLDTIME  INTERVAL
-----------------------------------------------------------------------
2.2.2.2  192.168.10.1  switch.0010  192.168.10.2  15s       180s
6.6.6.6  192.168.20.2  switch.0020  192.168.20.1  15s       180s
```

The following information is provided:

Parameter	Description
`peer-id`	**Synopsis:** A string The peer ID of the LDP neighbor discovery.
`peer-ip`	**Synopsis:** A string The peer ID of the LDP neighbor discovery.

Parameter	Description
`interface`	**Synopsis:** A string The local IP address of the LDP neighbor discovery.
`local-ip`	**Synopsis:** A string LDP neighbor discovery state.
`peer-hello-holdtime`	**Synopsis:** A string The peer hello holdtime of the LDP neighbor discovery.
`agreed-hello-holdtime`	**Synopsis:** A string The agreed upon hello holdtime (shorter holdtime of local/peer) of the LDP neighbor discovery.
`peer-session-holdtime`	**Synopsis:** A string The peer session holdtime of the LDP neighbor discovery.

13.10.7.6 Configuring LDP

To configure the LDP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the LDP by typing the following commands:

   Enable

   ```
   mpls ldp enable
   ```

   Disable

   ```
   no mpls ldp enable
   ```

3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false A boolean flag to indicate that Label Distribution Protocol (LDP) is enabled.
`holdtime { holdtime }`	**Synopsis:** An integer **Default:** 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.

13.10.7.7 Configuring Neighbor Discovery

To configure the LDP neighbor discovery, do the following:

1. Make sure the CLI is in Configuration mode.
2. To configure the LDP Neighbor Discovery, type the following command:

   ```
   mpls ldp discovery
   ```

3. Configure the following parameter(s) as required:

Parameter	Description
`interval { interval }`	**Synopsis:** An integer **Default:** 5 The time (in seconds) between the sending of consecutive Hello messages.
`holdtime { holdtime }`	**Synopsis:** An integer **Default:** 15 The time (in seconds) that a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.

13.10.7.8 Viewing a List of LDP Interfaces

To view a list of LDP interfaces, type:

```
show running-config mpls ldp interface-ldp
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config mpls ldp interface-ldp | tab
TRANSPORT             TRANSPORT IP
IFNAME       ENABLED  ADDRESS
-----------------------------------
fe-cm-1      false    -
switch.0001  false    -
switch.0010  true     192.168.10.1
switch.0020  false    -

 !
!
```

For more information about enabling LDP interfaces, refer to "Enabling/Disabling an LDP Interface" (Page 710).

13.10.7.9 Enabling/Disabling an LDP Interface

To enable or disable an LDP interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Enable/disable the LDP interface by typing the following commands:

   Enable

   ```
   mpls ldp interface-ldp { name }
   ```

   Disable

   ```
   no mpls ldp interface-ldp { name }
   ```

   Where:

   - `{ name }` is the name of the transport interface to be enabled or disabled.

3. Set the IP address for the transport interface, by typing:

   ```
   mpls ldp interface-ldp transport-ip-address { address }
   ```

   Where { address } is an IPv4 address.

4. Type `commit` and press **Enter** to save the changes.

13.11 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 RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 devices can be configured to act as a CE, PE or P (provider core) router.

13.11.1 VRF Concepts

This section describes some of the concepts important to the implementation of Virtual Routing and Forwarding (VRF) in RUGGEDCOM ROX II.

13.11.1.1 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.

13.11.1.2 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
- 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

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

13.11.2 Viewing VRF Interface Statistics

To view statistics for interfaces associated with a VRF instance, type:

```
show interfaces vrf { vrf } ip
```

Where:

- `{ vrf }` is the chosen VRF list

A table or list similar to the following example appears:

```
ruggedcom# show interfaces vrf VRF1 ip | tab
        ADMIN                           RX       RX       RX      RX       TX       TX       TX
 TX       TX          IPV4
NAME    STATE    STATE    POINTOPOINT  BYTES    PACKETS  ERRORS  DROPPED  BYTES    PACKETS  ERRORS
 DROPPED  COLLISIONS  ADDRESS
-------------------------------------------------------------------------------------------------
fe-1-1  not set  not set  false        8842726  117751   0       0        5366914  64721    0       0
        0

                    1.9.5.2/24
fe-1-2  not set  not set  false        4874496  70821    0       0        5849272  71022    0       0
        0
```

```
                    1.7.5.1/24
fe-1-3  not set  not set  false        7730176  120784   0       0        9423076  120810   0       0
        0

                    1.1.1.1/32
```

The following information is provided:

Parameter	Description
`admin-state`	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] The port's administrative status.
`state`	**Synopsis:** [not set | up | down | testing | unknown | dormant | notPresent | lowerLayerDown] Shows whether the link is up or down.
`pointopoint`	**Synopsis:** [true | false] The point-to-point link.

13.11.3 Configuring VRF

To configure Virtual Routing and Forwarding (VRF), do the following:

⚠ **NOTICE**
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 626).
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to "Adding a VRF Definition" (Page 715).
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to "Configuring a VRF Interface" (Page 714).
4. Enable OSPF. For more information, refer to "Configuring OSPF" (Page 669).
5. Configure one or more VRF instances for OSPF. For more information, refer to "Configuring OSPF" (Page 669).
6. Add one or more BGP neighbors. For more information, refer to "Adding a Neighbor" (Page 642).
7. Configure one or more IP/VPN tunnels for each interface. For more information, refer to "Adding an IP/VPN Tunnel" (Page 724).
8. Add one or more BGP neighbors to the VPNv4 address family. For more information, refer to "Adding a Neighbor" (Page 725).

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 626).
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to "Adding a VRF Definition" (Page 715).
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to "Configuring a VRF Interface" (Page 714).
4. Enable OSPF. For more information, refer to "Configuring OSPF" (Page 669).
5. Configure one or more VRF instances for OSPF. For more information, refer to "Configuring OSPF" (Page 669).
6. Configure an IPv4 address family for each VRF instance. For more information, refer to "Adding an IPv4 Address Family" (Page 727).
7. Configure one or more static VRF routes. For more information, refer to "Adding a Static VRF Route" (Page 733).
8. Verify the network configuration.

13.11.4 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. Make sure the CLI is in Configuration mode.
2. Set the costing by typing:

   ```
   ip { interface } vrf-forwarding { vrf }
   ```

   Where:

   - `{ interface }` is the name of the routable interface
   - `{ vrf }` is the desired VRF instance
3. Configure an IPv4 or IPv6 address for the interface. For more information, refer to "Adding an IPv4 Address" (Page 269) or "Adding an IPv6 Address" (Page 270).
4. Type `commit` and press **Enter** to save the changes.

13.11.5 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.

13.11.5.1 Viewing a List of VRF Definitions

To view a list of VRF definitions, type:

```
show running-config global vrf
```

If definitions have been configured, a table or list similar to the following example appears:

```
show running-config global vrf | tab
global
 vrf
  definition
VRF   VRF                 EXPORT     IMPORT     BOTH
NAME  DESCRIPTION  RD     COMMUNITY  COMMUNITY  COMMUNITY
-------------------------------------------------------------
vrf1  Site A       100:1
                                                100:2
vrf2  Site B       100:2
                                                100:1

 !
!
```

If no VRF definitions have been configured, add definitions as needed. For more information, refer to "Adding a VRF Definition" (Page 715).

13.11.5.2 Adding a VRF Definition

To add a VRF definition, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the definition by typing:

   ```
   global vrf definition { name }
   ```

   Where:

   - `{ name }` is the name for definition. The name must be unique and not exceed 32 characters or contain spaces. The first character must also not be a special character. Only the following special characters are permitted in

the remainder of the name: hyphen (-), underscore (_), colon (:), and period (.).

3. Configure the following parameter(s) as required:

Parameter	Description
`vrf-description { vrf-description }`	**Synopsis:** A string between 0 and 256 characters long A string that can be used to describe the vrf. Maximum length 256 characters, including blanks.
`rd { rd }`	**Synopsis:** A string between 0 and 32 characters long 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.

4. Add one or more route targets. For more information, refer to "Adding a Route Target" (Page 717).
5. Configure a routable interface for the VRF instance. For more information, refer to "Configuring a VRF Interface" (Page 714).
6. Type `commit` and press **Enter** to save the changes.

13.11.5.3 Deleting a VRF Definition

To delete a VRF definition, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set **vrf-forwarding** for the associated routable interface to another VRF definition or none at all.
3. Delete the associated VRF instance under OSPF. For more information, refer to "Deleting a VRF Instance" (Page 723).
4. Delete the associated IPv4 address family under BGP. For more information, refer to "Deleting an IPv4 Address Family" (Page 727).
5. Delete the definition key by typing:

   ```
   no routing vrf definition { name }
   ```

   Where:

   - `{ name }` is the name of the definition
6. Type `commit` and press **Enter** to save the changes.

13.11.6 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.

13.11.6.1 Viewing a List of Route Targets

To view a list of VRF definitions, type:

```
show running-config global vrf definition { name } rout
ing-target
```

If definitions have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config global vrf definition vrf1 route-target
global
 vrf
  definition vrf1
   route-target export 200:1
   !
   route-target import 200:2
   !
   route-target both 100:2
   !
  !
 !
!
```

If no VRF definitions have been configured, add definitions as needed. For more information, refer to "Adding a VRF Definition" (Page 715).

13.11.6.2 Adding a Route Target

To add a route target, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the definition by typing:

   ```
   global vrf definition { name } routing-target [ export |
   import | both ] { community }
   ```

   Where:

   - `{ name }` is the name of the VRF definition
   - `{ community }` is the route distinguisher for the target VRF to either export the routing table to, import the routing table from, or both
3. Type `commit` and press **Enter** to save the changes.

13.11.6.3 Deleting a Route Target

To delete a route target, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the definition key by typing:

   ```
   no global vrf definition { name } routing-target [ export | import | both ] { community }
   ```

   Where:

   - `{ name }` is the name of the VRF definition
   - `{ community }` is the route distinguisher for the target VRF to either export the routing table to, import the routing table from, or both
3. Type `commit` and press **Enter** to save the changes.

13.11.7 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).

13.11.7.1 Viewing a List of VRF Instances

To view a list of VRF instances defined for OSPF, type:

```
show running-config routing ospf vrf
```

If definitions have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf vrf
routing ospf
 vrf VRF1
  enabled
.
.
.
 vrf VRF2
  enabled
.
.
.
```

If no VRF definitions have been configured, add definitions as needed. For more information, refer to "Adding a VRF Definition" (Page 715).

13.11.7.2 Adding a VRF Instance and Configuring OSPF

To add a VRF instance and configure OSPF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » dynamic » ospf » vrf*** and configure the following parameter(s) as required:

Parameter	Description
`{ vrf-name }`	**Synopsis:** A string between 1 and 32 characters long The VRF name.
`enabled`	Enables the OSPF dynamic routing protocol.
`abr-type { abr-type }`	**Synopsis:** [cisco | ibm | shortcut | standard] **Default:** cisco The OSPF ABR type.
`auto-cost-reference-bandwidth { auto-cost-reference-bandwidth }`	**Synopsis:** An integer between 1 and 4294967 **Default:** 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
`compatible-rfc1583`	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
`default-information-originate`	Advertises the default route.
`default-metric { default-metric }`	**Synopsis:** An integer between 0 and 16777214 The default metric of redistribute routes.
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The administrative distance.
`opaque-lsa`	Enables the Opaque-LSA capability (RFC2370).
`passive-default { passive-default }`	**Synopsis:** [true | false] **Default:** true Default passive value for new interface.
`refresh-timer { refresh-timer }`	**Synopsis:** An integer between 10 and 1800 **Default:** 10 The refresh timer.
`router-id { router-id }`	**Synopsis:** A string between 7 and 15 characters long The Router ID for OSPF.
`{ name }`	**Synopsis:** A string between 1 and 1024 characters long The name of the prefix list.

Parameter	Description
`description { description }`	**Synopsis:** A string up to 1024 characters long The description of the prefix list.
`{ seq }`	**Synopsis:** An integer between 1 and 4294967295 Sequence number of the entry.
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit Action.
`subnet { subnet }`	**Synopsis:** A string between 9 and 18 characters long Network (xxx.xxx.xxx.xxx/xx).
`le { le }`	**Synopsis:** An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
`ge { ge }`	**Synopsis:** An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.
`tag { tag }`	**Synopsis:** A string between 1 and 1024 characters long Route map tag.
`{ seq }`	**Synopsis:** An integer between 1 and 65535 The sequence number of the route-map entry.
`action { action }`	**Synopsis:** [deny | permit] **Default:** permit Action.
`call { call }`	**Synopsis:** A string between 1 and 1024 characters long Jump to another route-map after match+set.
`on-match-goto { on-match-goto }`	**Synopsis:** An integer between 1 and 65535 Go to this entry on match.
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.
`prefix-list { prefix-list }`	**Synopsis:** A string between 1 and 1024 characters long The prefix list name.
`ifname { ifname }`	**Synopsis:** A string The interface name.
`metric { metric }`	**Synopsis:** An integer Metric value.

Parameter	Description
`metric-type { metric-type }`	**Synopsis:** An integer between 1 and 2 External route type.
`route-map { route-map }`	**Synopsis:** A string between 1 and 1024 characters long Route map name.
`{ area }`	**Synopsis:** A string between 7 and 15 characters long The OSPF Area ID (format: A.B.C.D).
`{ network }`	**Synopsis:** A string between 9 and 18 characters long The OSPF area network/prefix.
`shortcut { shortcut }`	**Synopsis:** [default | disable | enable] **Default:** default Sets the area's shortcutting mode. Options include: • Default: 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. • Enable: 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. • Disable: The ABR does not use this area for shortcutting, or set the new bit (S-bit) in the router-LSA originated for it.
`always { always }`	**Synopsis:** [true | false] **Default:** false Always advertise default route even when there is no default route present in routing table.
`metric { metric }`	**Synopsis:** An integer between 0 and 16777214 The metric value for default route.
`metric-type { metric-type }`	**Synopsis:** An integer between 1 and 2 **Default:** 2 The metric type for default route.
`route-map { route-map }`	**Synopsis:** A string between 1 and 1024 characters long The route map name.
`external { external }`	**Synopsis:** An integer between 1 and 255 The administrative distance for external routes.

Parameter	Description
`inter-area { inter-area }`	**Synopsis:** An integer between 1 and 255 The administrative distance for inter-area routes.
`intra-area { intra-area }`	**Synopsis:** An integer between 1 and 255 The administrative distance for intra-area routes.
`{ type }`	**Synopsis:** [kernel | static | connected | rip | bgp] Redistributes the route type.
`metric-type { metric-type }`	**Synopsis:** An integer between 1 and 2 **Default:** 2 The OSPF exterior metric type for redistributed routes.
`metric { metric }`	**Synopsis:** An integer between 0 and 16777214 The metric for redistributed routes.
`route-map { route-map }`	**Synopsis:** A string between 1 and 1024 characters long The route map name.
`{ ifname }`	**Synopsis:** A string Interface name.
`authentication { authentication }`	**Synopsis:** [message-digest | null] The authentication type on this interface.
`cost { cost }`	**Synopsis:** 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 { hello-interval }`	**Synopsis:** An integer between 1 and 65535 **Default:** 10 The time (in seconds) between sending hello packets.
`priority { priority }`	**Synopsis:** An integer between 0 and 255 **Default:** 1 Priority of interface.
`passive { passive }`	**Synopsis:** [true | false] **Default:** 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 { retransmit-interval }`	**Synopsis:** An integer between 1 and 65535 **Default:** 5 Time (in seconds) between retransmitting lost link state advertisements.

Parameter	Description
`transmit-delay { transmit-delay }`	**Synopsis:** An integer between 1 and 65535 **Default:** 1 The link state transmit delay (in seconds).
`dead-interval { dead-interval }`	**Synopsis:** An integer between 1 and 65535 **Default:** 40 The time before considering a router dead (in seconds).
`minimal-hello-multiplier { minimal-hello-multiplier }`	**Synopsis:** An integer between 1 and 10 The number of times a hello message can be sent within one second.
`{ key-id }`	**Synopsis:** An integer up to 255 The key ID.
`md5 { md5 }`	**Synopsis:** A string up to 1024 characters long The OSPF password (key).

3. Configure prefix list filters for the VRF instance. For more information, refer to "Adding a Prefix List" (Page 676).
4. Configure areas for the VRF instance. For more information, refer to "Adding an Area" (Page 679).
5. Configure route map filters for the VRF instance. For more information, refer to "Adding a Route Map Filter" (Page 682).
6. Configure redistribution metrics for the VRF instance. For more information, refer to "Adding a Redistribution Metric" (Page 687).
7. Configure interfaces for the VRF instance. For more information, refer to "Configuring a Routing Interface" (Page 689).
8. Type `commit` and press **Enter** to save the changes.

13.11.7.3 Deleting a VRF Instance

To delete a VRF instance under OSPF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the definition key by typing:

   ```
   no routing ospf vrf { name }
   ```

   Where:

   - `{ name }` is the name of the VRF instance
3. Type `commit` and press **Enter** to save the changes.

13.11.8 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.

13.11.8.1 Viewing a List of IP/VPN Tunnels

To view a list of IP/VPN tunnels configured for VRF, type:

```
show running-config routing bgp address-family vpnv4
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp address-family vpnv4 | tab
routing bgp
 address-family vpnv4
  neighbor
          SEND
IP        COMMUNITY
--------------------
1.2.6.2   both

 !
!
```

13.11.8.2 Adding an IP/VPN Tunnel

To add a new IP/VPN tunnel for VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing bgp address-family vpnv4 neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor
3. [Optional] Set the send community by typing:

   ```
   send-community [ both | extended | none | standard ]
   ```
4. [Optional] Enable the IP/VPN tunnel as a VPNv4 route reflector client by typing:

   ```
   route-reflector-client enabled
   ```
5. Type `commit` and press **Enter** to save the changes.

13.11.8.3 Deleting an IP/VPN Tunnels

To delete an IP/VPN tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no routing bgp address-family vpnv4 neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor
3. Type `commit` and press **Enter** to save the changes.

13.11.9 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.

13.11.9.1 Viewing a List of Neighbors

To view a list of configured VPNv4 neighbors, type:

```
show running-config routing bgp address-family vpnv4 neighbor
```

If neighbors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp address-family vpnv4 neighbor | tab
         SEND
IP       COMMUNITY
--------------------
1.2.6.2  both

 !
!
```

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 730).

13.11.9.2 Adding a Neighbor

To add a new VPNv4 neighbor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing bgp address-family vpnv4 neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor

3. [Optional] Set the send community by typing:

   ```
   send-community [ both | extended | none | standard ]
   ```

4. [Optional] Enable the neighbor as a route reflector client by typing:

   ```
   route-reflector-client enabled
   ```

5. Type `commit` and press **Enter** to save the changes.

13.11.9.3 Deleting a Neighbor

To delete a VPNv4 neighbor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing bgp address-family vpnv4 neighbor { address }
   ```

   Where:

   - `{ address }` is the IP address of the neighbor

3. Type `commit` and press **Enter** to save the changes.

13.11.10 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.

13.11.10.1 Viewing a List of IPv4 Address Families

To view a list of IPv4 address families configured for VRF, type:

```
show running-config routing bgp address-family ipv4 vrf
```

If IPv4 address families have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp address-family ipv4 vrf
routing bgp
 address-family ipv4
  vrf VRF1
   redistribute connected
    no metric
    no route-map
   !
   redistribute ospf
```

```
    no metric
    no route-map
   !
   redistribute static
    no metric
    no route-map
   !
  !
 !
!
```

If no IPv4 address families have been configured, add them as needed. For more information, refer to "Adding an IPv4 Address Family" (Page 727).

13.11.10.2 Adding an IPv4 Address Family

To add an IPv4 address family, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the IPv4 address family by typing:

   ```
   routing bgp address-family ipv4 vrf { vrf }
   ```

   Where:

   - `{ vrf }` is the name of the associated VRF definition
3. [Optional] Add one or more neighbors. For more information, refer to "Adding a Neighbor" (Page 730).
4. [Optional] Add one or more redistributions. For more information, refer to "Adding a Redistribution" (Page 728).
5. Type `commit` and press **Enter** to save the changes.

13.11.10.3 Deleting an IPv4 Address Family

To delete an IPv4 address family, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the IPv4 address family by typing:

   ```
   no routing bgp address-family ipv4 vrf { vrf }
   ```

   Where:

   - `{ vrf }` is the name of the associated VRF definition
3. Type `commit` and press **Enter** to save the changes.

13.11.11 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.

13.11.11.1 Viewing a List of Redistributions

To view a list of redistributions for an IPv4 address family, type:

```
show running-config routing bgp address-family ipv4 vrf
{ vrf } redistribute
```

Where:

- `{ vrf }` is the chosen VRF instance

If redistributions have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing bgp address-family ipv4 vrf VRF1 redistrib
ute | tab
                   ROUTE
SOURCE     METRIC  MAP
-------------------------
connected  -       -
ospf       -       -
static     -       -

  !
 !
!
```

If no redistributions have been configured, add them as needed. For more information, refer to "Adding a Redistribution" (Page 728).

13.11.11.2 Adding a Redistribution

To add a redistribution for an IPv4 address family, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the redistribution by typing:

   ```
   routing bgp address-family ipv4 vrf { vrf } redistribute
   [ { connected } | { ospf } | { static } ]
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance

3. Configure the following parameter(s) as required:

Parameter	Description
`metric { metric }`	**Synopsis:** An integer between 0 and 4294967295 The metric for redistributed routes.
`route-map { route-map }`	**Synopsis:** A string between 1 and 1024 characters long The route map name.

4. Type `commit` and press **Enter** to save the changes.

13.11.11.3 Deleting a Redistribution

To delete a redistribution defined for an IPv4 address family, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the redistribution by typing:

```
no routing bgp address-family ipv4 vrf { vrf } redistrib
ute [ { connected } | { ospf } | { static } ]
```

Where:

- `{ vrf }` is the chosen VRF instance

3. Type `commit` and press **Enter** to save the changes.

13.11.12 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.

13.11.12.1 Viewing a List of Neighbors

To view a list of neighbors configured for an IPv4 address family, type:

```
show running-config routing bgp address-family ipv4 vrf
{ vrf } neighbor
```

Where:

- `{ vrf }` is the chosen VRF instance

If neighbors have been configured, a table or list similar to the following example appears:

```
show running-config routing bgp address-family ipv4 vrf VRF1 neighbor
routing bgp
 address-family ipv4
  vrf VRF1
```

```
   neighbor 192.168.12.30
    remote-as 1
    no ebgp-multihop
    no maximum-prefix
    no next-hop-self
    no password
    no disable-connected-check
    no soft-reconfiguration
    no weight
    no route-map in
    no route-map out
   !
  !
 !
!
```

If no neighbors have been configured, add neighbors as needed. For more information, refer to "Adding a Neighbor" (Page 730).

13.11.12.2 Adding a Neighbor

To add a new neighbor to an IPv4 address family, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the neighbor by typing:

   ```
   routing bgp address-family ipv4 vrf { vrf } neighbor { ad
   dress }
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance
   - `{ address }` is the IP address of the neighbor
3. Configure the neighbor settings by configuring the following parameter(s):

Parameter	Description
`send-community { send-community }`	**Synopsis:** [standard | extended | both | none] **Default:** both Identifies the send Community. Default is both.
`remote-as { re mote-as }`	**Synopsis:** An integer between 1 and 4294967295 A BGP neighbor.
`ebgp-multihop { ebgp-multihop }`	**Synopsis:** An integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
`maximum-prefix { maxi mum-prefix }`	**Synopsis:** An integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
`next-hop-self`	Disables the next hop calculation for this neighbor.

Parameter	Description
`password { password }`	**Synopsis:** A string Password.
`update-source { update-source }`	**Synopsis:** 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 { weight }`	**Synopsis:** An integer The default weight for routes from this neighbor.

4. Configure the route map settings by configuring the following parameter(s):

Parameter	Description
`in { in }`	**Synopsis:** A string between 1 and 1024 characters long Apply route map to incoming routes.
`out { out }`	**Synopsis:** A string between 1 and 1024 characters long Apply route map to outbound routes.

5. Configure the prefix list distribution. For more information, refer to "Configuring the Distribution of Prefix Lists" (Page 731).
6. Type `commit` and press **Enter** to save the changes.

13.11.12.3 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 CLI is in Configuration mode.
2. Apply the desired prefix list the chosen route direction (incoming or outbound) by typing:

```
routing bgp address-family ipv4 vrf { vrf } neighbor { address } distribute-prefix-list [ in | out ] prefix-list { prefix }
```

Where:

- `{ vrf }` is the chosen VRF instance
- `{ address }` is the address of the chosen neighbor
- `{ prefix }` is the chosen BGP prefix list

3. If necessary, configure an event tracker to track network commands. For more information, refer to "Tracking Commands" (Page 732).
4. Type `commit` and press **Enter** to save the changes.

13.11.12.4 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 584).

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 the CLI is in Configuration mode.
2. Navigate to ***routing » dynamic » bgp » address-family » ipv4 » { vrf } » neighbor » { address } » distribute-prefix-list » In|out***, where { vrf } is the chosen VRF instance and { address } is the IP address of the neighbor.
3. Configure the following parameter(s) as required:

Parameter	Description
`event { event }`	**Synopsis:** 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 { apply-when }`	**Synopsis:** [up | down] **Default:** up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

4. Type `commit` and press **Enter** to save the changes.

13.11.12.5 Deleting a Neighbor

To delete a VPNv4 neighbor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the network by typing:

   ```
   no routing address-family ipv4 vrf { vrf } neighbor { address }
   ```

   Where:

- `{ vrf }` is the chosen VRF instance
- `{ address }` is the IP address of the neighbor

3. Type `commit` and press **Enter** to save the changes.

13.11.13 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.

13.11.13.1 Viewing a List of Static VRF Routes

To view a list of routable Ethernet ports, type:

```
show running-config routing vrf { vrf } ipv4
```

Where:

- `{ vrf }` is the chosen VRF instance

If routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing vrf VRF1 ipv4 | tab
                          HW
NETWORK          DISTANCE  ACCELERATE  GW       DISTANCE  INTERFACE  DISTANCE
-------------------------------------------------------------------------------
192.168.10.0/24  -         -
                                       1.9.5.1  -

!
```

If no static routes have been configured, add routes as needed. For more information, refer to "Adding a Static VRF Route" (Page 733).

13.11.13.2 Adding a Static VRF Route

To add an IPv4 static route for a VRF instance, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static VRF route by typing:

   ```
   routing vrf { vrf } ipv4 route { subnet }
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance
   - `{ subnet }` is the subnet (network/prefix) of the static route

3. 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.

4. 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 734).
5. If necessary, add gateways for the static route. For more information, refer to "Adding a Gateway for a Static VRF Route" (Page 735).
6. If necessary, add interfaces for the static route. For more information, refer to "Adding a Gateway for a Static VRF Route" (Page 737).
7. Type `commit` and press **Enter** to save the changes.

13.11.13.3 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. Make sure the CLI is in Configuration mode.
2. Configure the black hole connection by typing:

   ```
   routing vrf { vrf } ipv4 route { subnet } blackhole dis
   tance { distance }
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance.
   - `{ subnet }` is the subnet (network/prefix) of the static route.
   - `{ distance }` is the administrative distance. The default value is 1.
3. Type `commit` and press **Enter** to save the changes.

13.11.13.4 Deleting a Static VRF Route

To delete an IPv4 static route configured for a VRF instance, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the static route by typing:

   ```
   no routing vrf { vrf } ipv4 route { subnet }
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance
   - `{ subnet }` is the subnet (network/prefix) of the static route

3. Type `commit` and press **Enter** to save the changes.

13.11.14 Managing Gateways for Static VRF Routes

This section describes how to configure and manage gateways for static VRF routes.

13.11.14.1 Viewing a List of Gateways for Static VRF Routes

To view a list of gateway addresses assigned to an IPv4 static route, type:

```
show running-config routing vrf { vrf } ipv4 route { subnet } via
```

Where:

- `{ vrf }` is the chosen VRF instance.
- `{ subnet }` is the subnet (network/prefix) of the static route

If gateway addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing vrf VRF1 ipv4 route via | tab
NETWORK          GW       DISTANCE
-------------------------------------
192.168.10.0/24
                 1.9.5.1  -

!
```

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 735).

13.11.14.2 Adding a Gateway for a Static VRF Route

To add a gateway address for a static VRF route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   ```
   routing vrf { vrf } ipv4 route { subnet } via { gateway }
   ```

   Where:

- `{ vrf }` is the chosen VRF instance.
- `{ subnet }` is the subnet (network/prefix) of the static route
- `{ gateway }` is the gateway address for the static route

3. Configure the following parameter(s) as required:

Parameter	Description
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The distance for the static route.

4. Type `commit` and press **Enter** to save the changes.

13.11.14.3 Deleting a Gateway for a Static VRF Route

To delete a gateway address assigned to a static VRF route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the gateway address by typing:

```
no routing vrf { vrf } ipv4 route { subnet } via { gate
way }
```

Where:

- `{ vrf }` is the chosen VRF instance.
- `{ subnet }` is the subnet (network/prefix) of the static route
- `{ gateway }` is the gateway address for the static route

3. Type `commit` and press **Enter** to save the changes.

13.11.15 Managing Interfaces for Static VRF Routes

This section describes how to manage interfaces used for static VRF routes.

13.11.15.1 Viewing a List of Interfaces for Static VRF Routes

To view a list of interfaces assigned to an IPv4 static route, type:

```
show running-config routing vrf { vrf } ipv4 route dev
```

Where:

- `{ vrf }` is the chosen VRF instance.

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing vrf VRF1 ipv4 route dev | tab
```

```
NETWORK          INTERFACE  DISTANCE
-------------------------------------
192.168.10.0/24
                 fe-cm-1    -

!
```

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 737).

13.11.15.2 Adding a Gateway for a Static VRF Route

To add an interface for an static VRF route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   ```
   routing vrf { vrf } ipv4 route { subnet } dev { inter
   face }
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance.
   - `{ subnet }` is the subnet (network/prefix) of the static route
   - `{ interface }` is the name of the interface for the static route
3. Configure the following parameter(s) as required:

Parameter	Description
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The distance for the static route.

4. Type `commit` and press **Enter** to save the changes.

13.11.15.3 Deleting a Gateway for a Static VRF Route

To delete an interface assigned to a static VRF route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the gateway address by typing:

   ```
   no routing vrf { vrf } ipv4 route { subnet } dev { gate
   way }
   ```

   Where:

   - `{ vrf }` is the chosen VRF instance.
   - `{ subnet }` is the subnet (network/prefix) of the static route
   - `{ interface }` is the name of the interface for the static route

3. Type `commit` and press **Enter** to save the changes.

13.11.16 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.

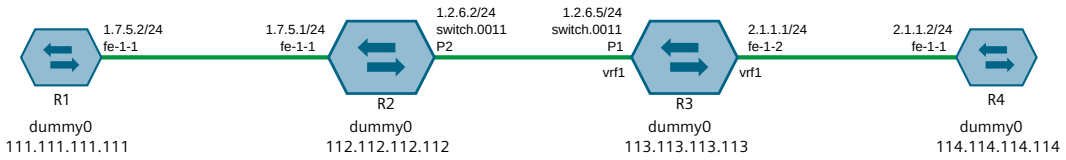


Figure 13.13 Topology – VRF-Lite Instance Configured with OSPF

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.

1. Enable OSPF. For more information, refer to "Configuring OSPF" (Page 669).
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 719).
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 679).
4. Add interface *fe-1-1* for the OSPF network. For more information, refer to "Configuring a Routing Interface" (Page 689).
5. Set the default passive value of the interface to *false*. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 719).
6. Add interface *switch.0011*. For more information, refer to "Configuring a Routing Interface" (Page 689).
7. Assign IP address *1.2.6.2/24* to the switch.0011 interface. For more information, refer to "Adding an IPv4 Address" (Page 269).
8. Set the default passive value of the interface to *false*. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 719).
9. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

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 719).
2. Configure a VRF definition for *vrf1* with a route distinguisher of *10*. For more information, refer to "Adding a VRF Definition" (Page 715).
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 717).
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 719).
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 679).
6. Add interface *fe-1-2* for the OSPF network. For more information, refer to "Configuring a Routing Interface" (Page 689).
7. Set the default passive value of the interface to *false*. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 719).
8. Add interface *switch.0011*. For more information, refer to "Configuring a Routing Interface" (Page 689).
9. Assign IP address *1.2.6.5/24* to the switch.0011 interface. For more information, refer to "Adding an IPv4 Address" (Page 269).
10. Set the default passive value of the interface to *false*. For more information, refer to "Adding a VRF Instance and Configuring OSPF" (Page 719).
11. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Step 3: Verify the configuration

1. Verify R2 and R3 have established an OSPF neighbor relationship.
   - For R2, type:

     ```
     show routing status OSPF neighbor
     ```

     Values similar to the following are provided:

ID	113.113.113.113
Address	1.2.6.5
Interface	switch.0011:1.2.6.2
Priority	1
State	Full/Back
Dead Time	38.320s

- For R3, type:

  ```
  show ip 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

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 28).
3. 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
```

13.11.17 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.

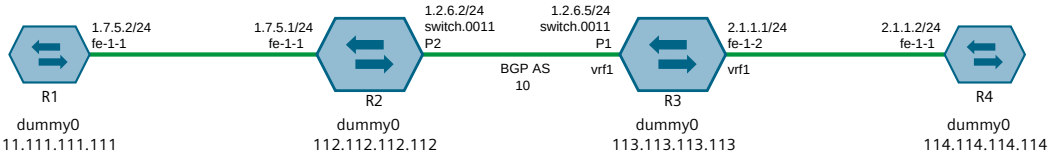


Figure 13.14 Topology – VRF-Lite Instance Configured with BGP

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 386).
2. Assign PVID 11 to port P2. For more information, refer to "Configuring a Switched Ethernet Port" (Page 335).
3. Assign IP address *1.2.6.2/24* to the switch.0011 interface. For more information, refer to "Adding an IPv4 Address" (Page 269).
4. Assign IP address *112.112.112.112* to the *dummy0* interface. For more information, refer to "Adding an IPv4 Address" (Page 269).
5. Enable BGP. For more information, refer to "Configuring BGP" (Page 626).
6. Assign Autonomous System ID (AS-ID) 10. For more information, refer to "Configuring BGP" (Page 626).
7. Add neighbor 1.2.6.5 and remote AS 10. For more information, refer to "Adding a Neighbor" (Page 642).
8. Define a redistribution metric for IPv4 family of type **connected**. For more information, refer to "Adding a Redistribution" (Page 728).
9. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

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 269).
2. Configure a VRF definition for *VRF1* with a route distinguisher of **`200:1`**. For more information, refer to "Adding a VRF Definition" (Page 715).
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 717).
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 741) to forward traffic to VRF1. For more information, refer to "Configuring a VRF Interface" (Page 714).
6. Enable BGP. For more information, refer to "Configuring BGP" (Page 626).
7. Assign Autonomous System ID (AS-ID) 10. For more information, refer to "Configuring BGP" (Page 626).
8. Add neighbor 1.2.6.2 and remote AS 10. For more information, refer to "Adding a Neighbor" (Page 725).
9. Define a redistribution metric for IPv4 family of type **connected**. For more information, refer to "Adding a Redistribution" (Page 728).
10. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Step 3: Verify the configuration

1. Verify R2 and R3 have established an OSPF neighbor relationship.
   - For R2, type:

     ```
     show routing status bgp neighbor
     ```

     Values similar to the following are provided:

ID	1.2.6.5
Version	4
Local AS	10
MSGRCVD	6
MSGSENT	13
Uptime	00:04:25
State	Established
Prefix Received	1

   - For R3, type:

     ```
     show ip bgp vrf1 neighbors
     ```

     Values similar to the following are provided:

BGP Neighbor	1.2.6.2
Remote AS	10
Local AS	10
BGP Version	4
Remote Router ID	192.168.1.112
BGP State	Established
Up For	00:24:44
Last Read	05:52:03
Hold Time	180
Keepalive Interval	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 28).
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
```

13.12 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.

13.12.1 Viewing a List of Static Routes

To view a list of routable Ethernet ports, type:

```
show running-config routing { protocol }
```

Where:

- `{ protocol }` is either *IPv4* or *IPv6*

If routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ipv4 | tab
                        HW
NETWORK         DISTANCE  ACCELERATE  GW            DISTANCE  INTERFACE    DIS
TANCE
-------------------------------------------------------------------------------
0.0.0.0/0       -         -
                                      172.30.128.1  -
                                                    switch.0001  -
10.200.16.0/20  -         -
```

If no static routes have been configured, add routes as needed. For more information, refer to "Adding an IPv4 Static Route" (Page 744) or "Adding an IPv6 Static Route" (Page 745).

13.12.2 Adding an IPv4 Static Route

To add an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.

   ⚠ 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.

2. Add the IPv4 static route by typing:

   ```
   routing ipv4 route { subnet }
   ```

   Where:

- `{ subnet }` is the subnet (network/prefix) of the static route

3. 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.

4. [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 746).
5. [Optional] 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 748) or "Adding an Interface for an IPv4 Static Route" (Page 750).
6. Type `commit` and press **Enter** to save the changes.

13.12.3 Adding an IPv6 Static Route

To add an IPv6 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the IPv6 static route by typing:

```
routing ipv6 route { subnet }
```

Where:

- `{ subnet }` is the subnet (network/prefix) of the static route

3. 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 747) or "Configuring Interfaces for IPv6 Static Routes" (Page 749).
4. Type `commit` and press **Enter** to save the changes.

13.12.4 Deleting a Static Route

To delete a static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the static route by typing:

   ```
   no routing { protocol } route { subnet }
   ```

   Where:

   - `{ protocol }` is either *IPv4* or *IPv6*
   - `{ subnet }` is the subnet (network/prefix) of the static route
3. Type `commit` and press **Enter** to save the changes.

13.12.5 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » ipv4 » {subnet} » blackhole***, where *subnet* is the subnet (network/prefix) of the static route.
3. Configure the following parameter(s) as required:

⚠ NOTICE
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 { distance }`	**Synopsis:** An integer between 1 and 255 **Default:** 1 The distance for this static route's blackhole. Default is 1.

4. Type `commit` and press **Enter** to save the changes.

13.12.6 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.

13.12.6.1 Configuring Gateways for IPv6 Static Routes

To configure a gateway address for an IPv6 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » ipv6 » route » {subnet} » via***, where *subnet* is the subnet (network/prefix) of the static route.
3. Configure the following parameter(s) as required:

Parameter	Description
`gw { gw }`	**Synopsis:** A string between 6 and 40 characters long The gateway for the static route.
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The distance for the static route.

4. Type `commit` and press **Enter** to save the changes.

13.12.6.2 Viewing a List of Gateways for IPv4 Static Routes

To view a list of gateway addresses assigned to an IPv4 static route, type:

```
show running-config routing ipv4 route { subnet } via
```

Where:

- `{ subnet }` is the subnet (network/prefix) of the static route

If gateway addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ipv4 route 0.0.0.0/0 via
```

```
routing ipv4 route 0.0.0.0/0
 via 172.30.128.1
  no distance
 !
!
```

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 748).

13.12.6.3 Adding a Gateway for an IPv4 Static Route

To add a gateway address for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   `routing ipv4 route { subnet } via { gateway }`

   Where:

   - `{ subnet }` is the subnet (network/prefix) of the static route
   - `{ gateway }` is the gateway address for the static route
3. Configure the following parameter(s) as required:

Parameter	Description
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The distance for the static route.

4. Type `commit` and press **Enter** to save the changes.

13.12.6.4 Deleting a Gateway for an IPv4 Static Route

To delete a gateway for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the gateway address by typing:

   `no routing ipv4 route { subnet } via { gateway }`

   Where:

   - `{ subnet }` is the subnet (network/prefix) of the static route
   - `{ gateway }` is the gateway address for the static route
3. Type `commit` and press **Enter** to save the changes.

13.12.7 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 determines the next hop IP address.

In the case of IPv6 static routes, only one interface can be selected per route.

13.12.7.1 Configuring Interfaces for IPv6 Static Routes

To configure an interface for an IPv6 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » ipv6 » route » {subnet} » dev***, where *subnet* is the subnet (network/prefix) of the static route.
3. Configure the following parameter(s) as required:

Parameter	Description
`interface { interface }`	**Synopsis:** A string The interface for the static route.
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The distance for the static route.

4. Type `commit` and press **Enter** to save the changes.

13.12.7.2 Viewing a List of Interfaces for IPv4 Static Routes

To view a list of interfaces assigned to an IPv4 static route, type:

```
show running-config routing ipv4 route { subnet } dev
```

Where:

- `{ subnet }` is the subnet (network/prefix) of the static route

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ipv4 route 0.0.0.0/0 dev
routing ipv4 route 0.0.0.0/0
 dev switch.0001
  no distance
 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding an Interface for an IPv4 Static Route" (Page 750).

13.12.7.3 Adding an Interface for an IPv4 Static Route

To add an interface for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   ```
   routing ipv4 route { subnet } dev { interface }
   ```

   Where:

   - `{ subnet }` is the subnet (network/prefix) of the static route
   - `{ interface }` is the name of the interface for the static route
3. Configure the following parameter(s) as required:

Parameter	Description
`distance { distance }`	**Synopsis:** An integer between 1 and 255 The distance for the static route.

4. Type `commit` and press **Enter** to save the changes.

13.12.7.4 Deleting an Interface for an IPv4 Static Route

To delete an interface for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the gateway address by typing:

   ```
   no routing ipv4 route { subnet } dev { interface }
   ```

   Where:

   - `{ subnet }` is the subnet (network/prefix) of the static route
   - `{ interface }` is the name of the interface for the static route
3. Type `commit` and press **Enter** to save the changes.

13.13 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.

13.13.1 Enabling/Disabling Static Multicast Routing

To enable or disable static multicast routing, do the following:

1. Make sure the CLI is in Configuration mode.

2. Enable or disable static multicast routing by typing:

   ```
   routing multicast static [ enable | disable ]
   ```

3. Type `commit` and press **Enter** to save the changes.

13.13.2 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).

13.13.2.1 Viewing a List of Static Multicast Groups

To view a list of static multicast groups, type:

```
show running-config routing multicast static
```

If static multicast groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing multicast static | tab
routing multicast static enabled
routing multicast static mcast-groups
                            MULTICAST    IN           HW
DESCRIPTION  SOURCE IP      IP           INTERFACE    ACCELERATE  IFNAME
-------------------------------------------------------------------------
test.001     169.150.24.12  238.1.12.12  switch.0001  -           fe-cm-1
```

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 751).

13.13.2.2 Adding a Static Multicast Group

To add a static multicast group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the multicast group by typing:

   ```
   routing multicast static mcast-groups { description }
   ```

   Where:

   - `{ description }` is the name of the multicast group. Up to 32 characters are allowed, excluding spaces.

3. Configure the following parameter(s) as required:

Parameter	Description
`source-ip { source-ip }`	**Synopsis:** 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 { multicast-ip }`	**Synopsis:** 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 { in-interface }`	**Synopsis:** 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.

4. Configure out-interfaces. For more information, refer to "Adding an Out-Interface" (Page 753).
5. Type `commit` and press **Enter** to save the changes.

13.13.2.3 Deleting a Static Multicast Group

To delete a static multicast group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the multicast group by typing:

   ```
   no routing multicast static mcast-groups { description }
   ```

   Where:

   - `{ description }` is the name of the multicast group to be deleted
3. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

13.13.3 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.

13.13.3.1 Viewing a List of Out-Interfaces

To view a list of out-interfaces, type:

```
show runing-config routing multicast static mcast-group out-
interface
```

If out-interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing multicast static mcast-groups out-interface
routing multicast static mcast-groups test
 out-interface fe-cm-1
 !
!
```

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 753).

13.13.3.2 Adding an Out-Interface

To add an out-interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the out-interface by typing:

   ```
   routing multicast static mcast-groups { group } out-inter
   face { ifname }
   ```

   Where:

   - `{ group }` is the name of the multicast group
   - `{ ifname }` is a string of up to 15 characters used to name the out-interface
3. Type `commit` and press **Enter** to save the changes.

13.13.3.3 Deleting an Out-Interface

To delete an out-interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the out-interface by typing:

   ```
   no routing multicast static mcast-groups { group } out-in
   terface { ifname }
   ```

   Where:

   - `{ group }` is the name of the group with the out-interface to be deleted
   - `{ ifname }` is the name of the out-interface to be deleted

3. Type `commit` and press **Enter** to save the changes.

13.14 Managing Dynamic Multicast Routing

This section describes concepts and configuration related to dynamic multicast routing using PIM-SM and PIM-SSM.

13.14.1 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).

13.14.1.1 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 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.

13.14.1.2 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.

13.14.1.3 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 765).

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.

13.14.2 Viewing the Status of PIM-SM

To view the status of PIM-SM, do the following:

1. Make sure the CLI is in Configuration mode.
2. At the command prompt, type **`show routing status pim-sm`** and press **Enter**. The PIM-SM routing status information appears:

   Note

   A default routing protocol with a local address of *169.254.0.1* always appears when the **`show routing status pim-sm`** command is run. This internal routing protocol is a placeholder to reserve the source-specific multicast address range.

```
ruggedcom# show routing status pim-sm
routing status pim-sm
 bsr 192.168.30.1
 vinterface
INDEX  LOCAL ADDRESS  SUBNET           FLAGS      ID
-----------------------------------------------------------------
0      172.30.157.78  172.30.128.0/19  DISABLED
1      169.254.72.4   169.254.72.0/28  DISABLED
2      169.254.0.1    169.254.0.0/24   DISABLED
3      192.168.13.3   192.168.13.0/24  DR PIM
                                                  192.168.13.1
4      192.168.0.2    192.168.0.0/24   DISABLED
```

```
5      192.168.30.1   192.168.30.0/24  DR NO-NBR

 mroute
GROUP             SOURCE            RP ADDR           FLAGS
------------------------------------------------------------------------
239.0.1.0         192.168.20.2      192.168.30.1      SPT CACHE SG
239.0.1.1         192.168.20.2      192.168.30.1      SPT CACHE SG
239.0.1.2         192.168.20.2      192.168.30.1      SPT CACHE SG
239.0.1.3         192.168.20.2      192.168.30.1      SPT CACHE SG
239.0.1.4         192.168.20.2      192.168.30.1      SPT CACHE SG
239.0.1.5         192.168.20.2      192.168.30.1      SPT CACHE SG
239.0.1.6         192.168.20.2      192.168.30.1      SPT CACHE SG
```

Parameter	Description
`{ index }`	**Synopsis:** An integer Virtual interface index.
`local-address`	**Synopsis:** A string between 1 and 16 characters long Local address.
`subnet`	**Synopsis:** A string between 1 and 20 characters long Subnet.
`flags`	**Synopsis:** A string between 1 and 128 characters long Flags indicates virtual interface information. • DISABLED: The virtual interface is administratively disabled for PIM-SM. • DOWN: This virtual interface is down. • DR: Designated router. • NO-NBR: No neighbor on this virtual interface. • PIM: PIM neighbor. • DVMRP: DVMRP neighbor.
`id`	**Synopsis:** A string between 1 and 16 characters long Neighbor address.

3. At the command prompt, type **`show routing status pim-sm bsr`** and press **Enter**. The address of the BSR appears:

```
ruggedcom# show routing status pim-sm bsr
routing status pim-sm bsr 192.168.30.1
```

Parameter	Description
`bsr`	**Synopsis:** A string between 1 and 16 characters long Current BSR (bootstrap router) address.

4. At the command prompt, type **`show routing status pim-sm vinterface`** and press **Enter**. The PIM-SM virtual interface routing status information appears:

```
ruggedcom# show routing status pim-sm vinterface
```

```
INDEX  LOCAL ADDRESS  SUBNET           FLAGS      ID
-------------------------------------------------------------------
0      172.30.157.78  172.30.128.0/19  DISABLED
1      169.254.72.4   169.254.72.0/28  DISABLED
2      169.254.0.1    169.254.0.0/24   DISABLED
3      192.168.13.3   192.168.13.0/24  DR PIM
                                                  192.168.13.1
4      192.168.0.2    192.168.0.0/24   DISABLED
5      192.168.30.1   192.168.30.0/24  DR NO-NBR
```

Parameter	Description
`{ index }`	**Synopsis:** An integer Virtual interface index.
`local-address`	**Synopsis:** A string between 1 and 16 characters long Local address.
`subnet`	**Synopsis:** A string between 1 and 20 characters long Subnet.
`flags`	**Synopsis:** A string between 1 and 128 characters long Flags indicates virtual interface information. • DISABLED: The virtual interface is administratively disabled for PIM-SM. • DOWN: This virtual interface is down. • DR: Designated router. • NO-NBR: No neighbor on this virtual interface. • PIM: PIM neighbor. • DVMRP: DVMRP neighbor.
`id`	**Synopsis:** A string between 1 and 16 characters long Neighbor address.

5. At the command prompt, type **`show routing status pim-sm rp`** and press **Enter**. The PIM-SM rendezvous point routing status information appears:

```
show routing status pim-sm rp
ID                PREFIX                PRIORITY  HOLDTIME
-----------------------------------------------------------
192.168.30.1
                  239.0.0.0/16          100       125
169.254.0.1
                  232.0.0.0/8           1         65535
```

Parameter	Description
`id`	**Synopsis:** A string between 1 and 16 characters long RP address.
`{ prefix }`	**Synopsis:** A string between 1 and 20 characters long Group prefix.

Parameter	Description
`priority`	**Synopsis:** A string between 1 and 20 characters long Priority.
`holdtime`	**Synopsis:** A string between 1 and 20 characters long The RP holdtime.

6. At the command prompt, type **`show routing status pim-sm mroute`** and press **Enter**. The PIM-SM (S,G) routing status information appears:

```
ruggedcom# show routing status pim-sm mroute
GROUP             SOURCE            RP ADDR           FLAGS
------------------------------------------------------------------
239.0.1.0         192.168.20.2      192.168.30.1      SPT SG
239.0.1.1         192.168.20.2      192.168.30.1      SPT SG
239.0.1.2         192.168.20.2      192.168.30.1      SPT SG
239.0.1.3         192.168.20.2      192.168.30.1      SPT SG
239.0.1.4         192.168.20.2      192.168.30.1      SPT SG
239.0.1.5         192.168.20.2      192.168.30.1      SPT SG
239.0.1.6         192.168.20.2      192.168.30.1      SPT SG
239.0.1.7         192.168.20.2      192.168.30.1      SPT SG
239.0.1.8         192.168.20.2      192.168.30.1      SPT SG
239.0.1.9         192.168.20.2      192.168.30.1      SPT SG
239.0.1.10        192.168.20.2      192.168.30.1      SPT SG
239.0.1.11        192.168.20.2      192.168.30.1      SPT SG
239.0.1.12        192.168.20.2      192.168.30.1      SPT SG
239.0.1.13        192.168.20.2      192.168.30.1      SPT SG
239.0.1.14        192.168.20.2      192.168.30.1      SPT SG
239.0.1.15        192.168.20.2      192.168.30.1      SPT SG
239.0.1.16        192.168.20.2      192.168.30.1      SPT SG
239.0.1.18        192.168.20.2      192.168.30.1      SPT SG
239.0.1.19        192.168.20.2      192.168.30.1      SPT SG
239.0.1.20        192.168.20.2      192.168.30.1      SPT SG
239.0.1.21        192.168.20.2      192.168.30.1      SPT SG
239.0.1.22        192.168.20.2      192.168.30.1      SPT SG
239.0.1.23        192.168.20.2      192.168.30.1      SPT SG
239.0.1.24        192.168.20.2      192.168.30.1      SPT SG
239.0.1.25        192.168.20.2      192.168.30.1      SPT SG
```

Parameter	Description
`{ group }`	**Synopsis:** A string between 1 and 16 characters long Multicast group address.
`{ source }`	**Synopsis:** A string between 1 and 16 characters long Source IP address.
`rp-addr`	**Synopsis:** A string between 1 and 16 characters long RP (Rendezvous Point) address.
`flags`	**Synopsis:** A string between 1 and 128 characters long Flags. • SPT: IIF (incoming interface) toward source. • WC: (*,G) entry. • RP: IIF (incoming interface) toward RP.

Parameter	Description
	• CACHE: A mirror for the kernel cach. • ASSERT: Upstream is not that of source. • SG: (S,G) pure, not hanging off of (*,G). • PMBR: (*,*,RP) entry (for interop).

7. At the command prompt, type **`show routing status pim-sm ssmgroup`** and press **Enter**. The SSM Group routing status information appears:

```
ruggedcom# show routing status pim-sm ssmgroup
MCAST                    VINTERFACE
GROUP      SOURCE IP     INDEX
-------------------------------------
232.1.2.5
           192.168.11.4  1
```

Parameter	Description
`mcast-group`	**Synopsis:** A string between 1 and 16 characters long Multicast group address.
`{ source-ip }`	**Synopsis:** A string between 1 and 16 characters long Source IP address.
`vinterface-index`	**Synopsis:** An integer Virtual interface index.

8. At the command prompt, type **`show routing status pim-sm groute`** and press **Enter**. The PIM-SM (*,G) routing status information appears:

```
ruggedcom# show routing status pim-sm groute
GROUP             RP ADDR           FLAGS
-----------------------------------------
239.0.1.0         192.168.30.1      WC RP
239.0.1.1         192.168.30.1      WC RP
239.0.1.2         192.168.30.1      WC RP
239.0.1.3         192.168.30.1      WC RP
239.0.1.4         192.168.30.1      WC RP
239.0.1.5         192.168.30.1      WC RP
239.0.1.6         192.168.30.1      WC RP
239.0.1.7         192.168.30.1      WC RP
239.0.1.8         192.168.30.1      WC RP
239.0.1.9         192.168.30.1      WC RP
239.0.1.10        192.168.30.1      WC RP
239.0.1.11        192.168.30.1      WC RP
239.0.1.12        192.168.30.1      WC RP
239.0.1.13        192.168.30.1      WC RP
239.0.1.14        192.168.30.1      WC RP
239.0.1.15        192.168.30.1      WC RP
239.0.1.16        192.168.30.1      WC RP
239.0.1.17        192.168.30.1      WC RP
239.0.1.18        192.168.30.1      WC RP
239.0.1.19        192.168.30.1      WC RP
239.0.1.20        192.168.30.1      WC RP
239.0.1.21        192.168.30.1      WC RP
239.0.1.22        192.168.30.1      WC RP
239.0.1.23        192.168.30.1      WC RP
```

```
239.0.1.24        192.168.30.1      WC RP
```

Parameter	Description
`{ group }`	**Synopsis:** A string between 1 and 16 characters long Multicast group address.
`rp-addr`	**Synopsis:** A string between 1 and 16 characters long RP (Rendezvous Point) address.
`flags`	**Synopsis:** A string between 1 and 128 characters long Flags. • SPT: IIF (incoming interface) toward source. • WC: (*,G) entry. • RP: IIF (incoming interface) toward RP. • CACHE: A mirror for the kernel cach. • ASSERT: Upstream is not that of source. • SG: (S,G) pure, not hanging off of (*,G). • PMBR: (*,*,RP) entry (for interop).

13.14.3 Viewing the Status of Dynamic Multicast Routing

To view the status of dynamic multicast routing, type:

```
show routing status multicast
```

If multicast routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status multicast
                           IN           OUT
SOURCE          GROUP      INTERFACE    INTERFACE
-----------------------------------------------------
192.168.11.101  225.0.0.1  switch.0011  switch.0012 switch.0014
```

13.14.4 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 the CLI is in Configuration mode.
2. Enable PIM-SM by typing:

   ```
   routing multicast dynamic pim-sm enabled
   ```

3. Configure the following parameter(s) as required:

Parameter	Description
`default-preference { default-preference }`	**Synopsis:** An integer equal to or greater than 1 **Default:** 1024 Default preference value. Preferences are used by assert elections to determine upstream routers.
`default-metric { default-metric }`	**Synopsis:** An integer equal to or greater than 1 **Default:** 1024 Default metric value. Metric is the cost of sending data through interface.
`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 764).
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 764).
6. Define which multicast groups the device will handle. For more information, refer to "Adding a Multicast Group Prefix" (Page 768).
7. Type `commit` and press **Enter** to save the changes.

13.14.5 Setting the Device as a BSR Candidate

To set the device as a BSR candidate, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the device as a BSR candidate by typing:

   ```
   routing multicast dynamic pim-sm bsr-candidate local-address { address } priority { number }
   ```

   Where:

   - `{ address }` is the local address to be used in the Cand-BSR messages. If not specified, the largest local IP address will be used (excluding passive interfaces).
   - `{ priority }` sets the priority for the BSR. Larger values have higher priority.
3. Type `commit` and press **Enter** to save the changes.

13.14.6 Setting the Device as an RP Candidate

To set the device as an RP candidate, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the device as an RP candidate by typing:

   ```
   routing multicast dynamic pim-sm rp-candidate local-ad
   dress { address } timer { timer } priority { number }
   ```

   Where:

   - `{ address }` is the 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 }` is the number of seconds to wait between advertising and Cand-RP message.
   - `{ priority }` sets the priority for this CRP. Smaller values have higher priority.
3. Type `commit` and press **Enter** to save the changes.

13.14.7 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.

13.14.7.1 Viewing a List of PIM-SM Interfaces

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » multicast » dynamic » pim-sm*** and press **Enter**.
3. At the command prompt, type **`show full-configuration`** and press **Enter**.The PIM-SM interfaces information appears:

```
ruggedcom(config-pim-sm)# show full-configuration | tab

routing multicast dynamic pim-sm
 enabled
 bsr-candidate local-address 1.1.1.1
 bsr-candidate priority 1
 rp-candidate local-address 1.1.1.1
 rp-candidate priority 1
 no broken-cisco-checksum
 interface
                      IGMP
IFNAME       PASSIVE  VERSION
------------------------------
dummy0       true     v2
fe-3-1       false    v2
fe-3-2       false    v2
fe-3-5       true     v2
fe-cm-1      true     v2
switch.0001  false    v3
```

```
 group-prefix
PREFIX
--------------
228.1.3.1/32
228.1.3.2/32

!
```

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 765).

13.14.7.2 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » multicast » dynamic » PIM-SM » interface » interface-name***, where *interface-name* is the name of the interface to be enabled for PIM-SM.

   Note

   A maximum of 30 non-passive interfaces can be active for PIM-SM.

3. Configure the following parameter(s) as required:

Parameter	Description
`passive { passive }`	**Synopsis:** [true | false] **Default:** true Whether an interface is active or passive.
`igmp-version { igmp-version }`	**Synopsis:** [v2 | v3] **Default:** v2 The version of IGMP. Options include: • v2: IGMP version 2. • v3: IGMP version 3. Backwards compatible with v2.

4. Make sure the chosen interface is assigned an IP address. For more information, refer to "Managing IP Addresses for Routable Interfaces" (Page 267).
5. 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 368).

The same is required for any Layer 2 switches on the network.

6. Type `commit` and press **Enter** to save the changes.

13.14.8 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.

13.14.8.1 Viewing a List of Static RP Addresses

To view a list of static RP addresses, type:

```
show running-config routing multicast dynamic pim-sm rp-ad
dress
```

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing multicast dynamic pim-sm rp-address | tab
ADDRESS         GROUP        PRIORITY
----------------------------------------
172.30.145.254  225.0.2.6/8  -
192.168.0.10    225.0.0.1/8  -

!
```

If no addresses have been configured, add addresses as needed. For more information, refer to "Adding a Static RP Address" (Page 766).

13.14.8.2 Adding a Static RP Address

To add a static RP address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the RP address by typing:

   ```
   routing multicast dynamic pim-sm rp-address { static-ad
   dress } { group-address } priority { priority }
   ```

   Where:

   - `{ static-address }` is the IP address of the RP
   - `{ group-address }` is the multicast address of the group handled by the RP
   - `{ priority }` is the the RP's priority in the election process

Note

A higher value means a higher rendezvous point priority.

3. Type `commit` and press **Enter** to save the changes.

13.14.8.3 Deleting a Static RP Address

To delete a static RP address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen RP address by typing:

   ```
   no routing multicast dynamic pim-sm rp-address { stat
   ic-address }
   ```

   Where `{ static-address }` is the Static RP (Rendezvous Point) address
3. Type `commit` and press **Enter** to save the changes.

13.14.9 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).

13.14.9.1 Viewing a List of Multicast Group Prefixes

To view a list of multicast group prefixes, type:

```
show running-config routing multicast dynamic pim-sm group-
prefix
```

If prefixes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing multicast dynamic pim-sm group-prefix
routing multicast dynamic pim-sm
 group-prefix 225.1.2.0/24
 !
!
```

If no prefixes have been configured, add prefixes as needed. For more information, refer to "Adding a Multicast Group Prefix" (Page 768).

13.14.9.2 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. Make sure the CLI is in Configuration mode.
2. Add the multicast group prefix by typing:

   ```
   routing multicast dynamic pim-sm group-prefix { prefix }
   ```

   Where { prefix } is the prefix for the multicast group (e.g. 225.1.2.0/24).
3. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

13.14.9.3 Deleting a Multicast Group Prefix

To delete a multicast group prefix, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the multicast group prefix by typing:

   ```
   no routing multicast dynamic pim-sm group-prefix { pre
   fix }
   ```

   Where { prefix } is the chosen prefix.
3. Type `commit` and press **Enter** to save the changes.

13.14.10 Example: Configuring Protocol Independent Multicast

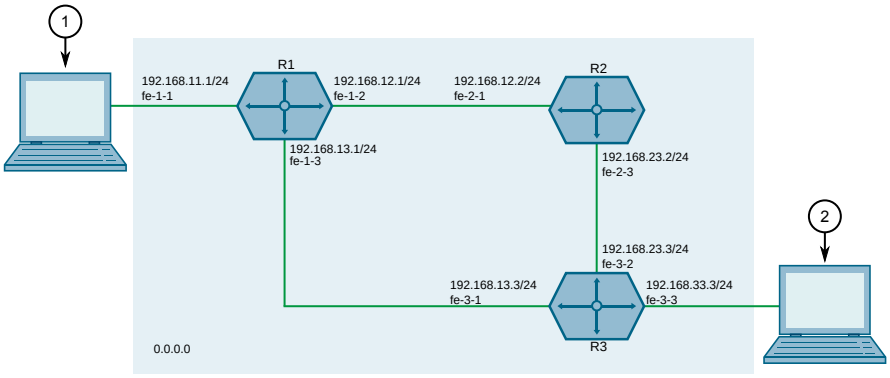
This section describes how to configure both PIM-SM and PIM-SSM using router ports in an OSPF network.

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 13.15 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 269).

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 269).

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 269).

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 669).
   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

Router	Area ID	IP Address/Prefix
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 762).
6. Enable PIM-SM on all multicast path interfaces. For more information, refer to "Enabling/Disabling a PIM-SM Interface" (Page 765).
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 269).
   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 766).
   c. On R1 and R3, add the RP address. For more information, refer to "Adding a Static RP Address" (Page 766).
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
 !
!
```

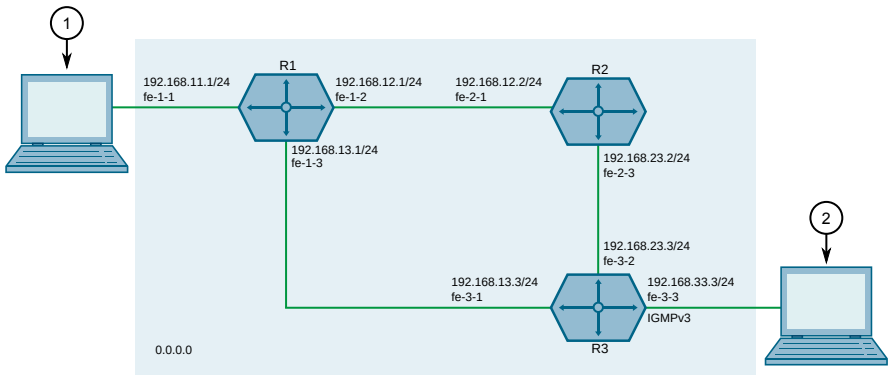
- **R3**

```
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 13.16 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 768).
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 765).
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 368).

b. On R1 and R3, verify the groups listed in step 3a (Page 772) are registered as SSM groups. For more information, refer to "Viewing the Status of PIM-SM" (Page 757).

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
 !
!
```

14 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.

14.1 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] 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.

14.1.1 VRRP Concepts

This section describes some of the concepts important to the implementation of the Virtual Router Redundancy Protocol (VRRP) in RUGGEDCOM ROX II.

14.1.1.1 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.

14.1.1.2 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.

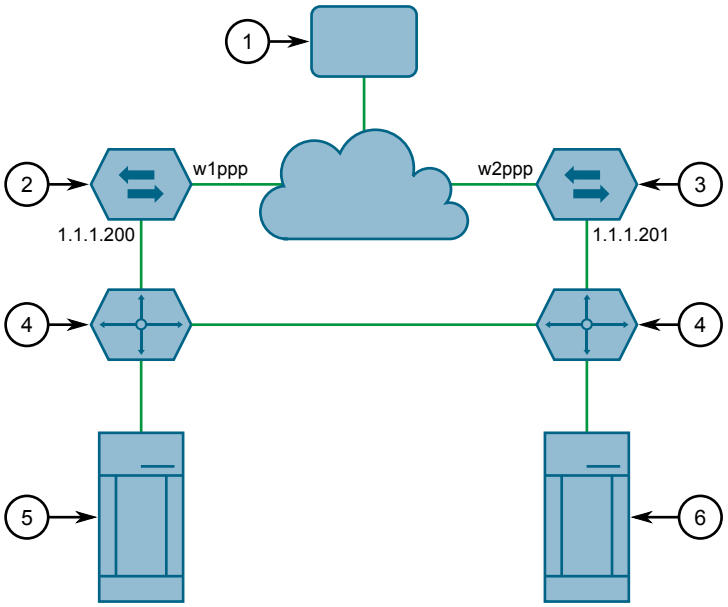
On RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512/RX1524/RX1536 devices with RUGGEDCOM ROX II v2.3 or higher installed, if the router with the highest priority is in a fault state, the backup VRRP Router can delay its transition to becoming the Master router. The length of the delay is user-defined.

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.



① Network
② Remote Router 1
③ Remote Router 2
④ Switch
⑤ Host 1
⑥ Host 2

Figure 14.1 VRRP Example

In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
• VRID 10 Gateway IP: 1.1.1.253 • VRID 10 Priority: 100 • VRID 10 Monitor Interface: w1ppp • VRID 11 Gateway IP: 1.1.1.252 • VRID 11 Priority: 50	• VRID 10 Gateway IP: 1.1.1.253 • VRID 10 Priority: 50 • VRID 11 Gateway IP: 1.1.1.252 • VRID 11 Priority: 100 • VRID 11 Monitor Interface: w2ppp

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.

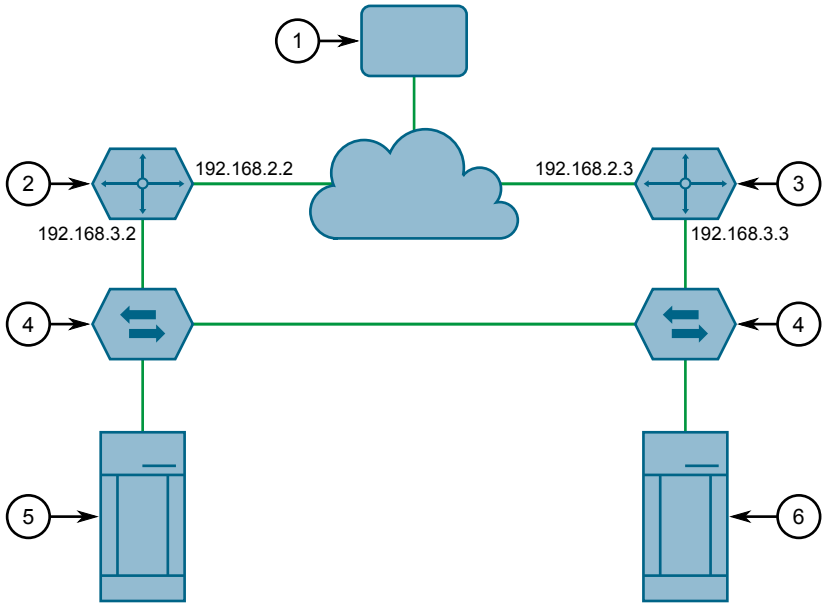
Note that both routers can always be reached by the hosts at their *real* IP addresses.

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 14.2 VRRP Group Example

In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
• VRID_20 Gateway IP: 192.168.2.10 • VRID_20 Priority: 100 • VRID_21 Gateway IP: 192.168.3.10 • VRID_21 Priority: 100	• VRID_20 Gateway IP: 192.168.2.10 • VRID_20 Priority: 50 • VRID_21 Gateway IP: 192.168.3.10 • VRID_21 Priority: 50

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.

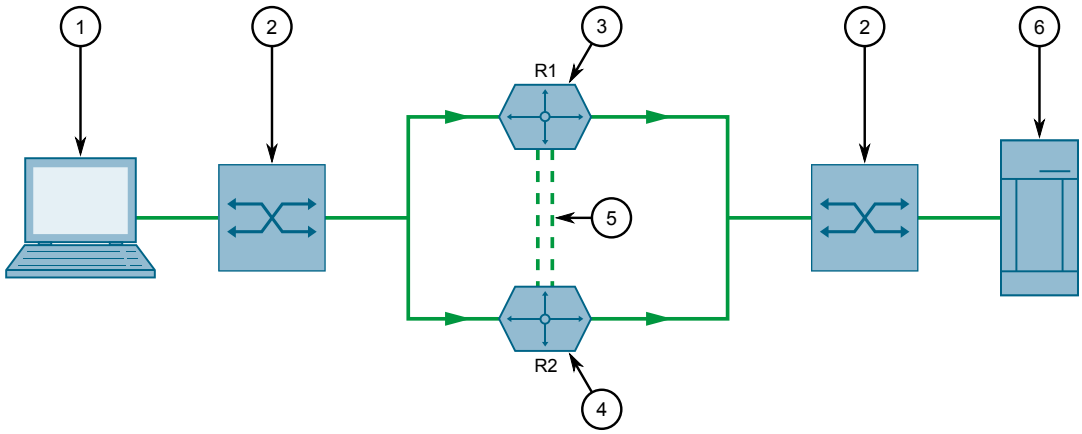
The router issues a set of gratuitous ARPs when moving between Master and Backup roles. These unsolicited ARPs teach the hosts and switches in the network of the current MAC address and port associated with the gateway. The router will issue a second set of ARPs after the time specified by the Gratuitous ARP delay.

14.1.1.3 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 14.3 Connection Synchronization Example

14.1.2 Viewing the Status of VRRP

To view the status of VRRP, type:

```
show services vrrp status
```

A table or list similar to the following example appears:

```
ruggedcom# show services vrrp status
                                                                    MONITOR
                                                        INTERFACE   INTERFACE
NAME  STATE   PRIORITY  TIME CHANGE                     STATE       STATE
-------------------------------------------------------------------------------
v1    master  100       Sat Feb  2 06:30:41 EST 2013  fe-cm-1 is Up
```

This following information is provided:

Parameter	Description
`{ name }`	**Synopsis:** A string The VRRP instance name.
`state`	**Synopsis:** A string The VRRP instance state.
`priority`	**Synopsis:** A string The VRRP instance priority.
`time-change`	**Synopsis:** A string The time of change to the current state.
`interface-state`	**Synopsis:** A string The VRRP interface state.
`monitor-interface-state`	**Synopsis:** A string Monitors the interface state.

14.1.3 Enabling/Disabling VRRP

To enable or disable VRRP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable VRRP by typing:

   Enabling VRRP

   ```
   services vrrp enabled
   ```

   Disabling VRRP

   ```
   no services vrrp enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

14.1.4 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.

14.1.4.1 Viewing a List of VRRP Trackers

To view a list of VRRP trackers, type:

```
show running-config services vrrp trackers
```

If trackers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp trackers
services
 vrrp
  trackers tracker tracker1
   network   10.0.0.0/8
   interface dummy0
   interval  1
  !
 !
!
```

If no VRRP trackers have been configured, add trackers as needed. For more information, refer to "Adding a VRRP Tracker" (Page 781).

14.1.4.2 Adding a VRRP Tracker

To add a VRRP tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tracker by typing:

   ```
   services vrrp trackers { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP tracker
3. Configure the following parameter(s) as required:

Parameter	Description
`type { type }`	**Synopsis:** [route] **Default:** route The type of condition for the tracker to check.
`network { network }`	**Synopsis:** 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.

Parameter	Description
`interface { interface }`	**Synopsis:** A string The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
`interval { interval }`	**Synopsis:** An integer between 1 and 120 The number of seconds between tracker queries.
`weight { weight }`	**Synopsis:** 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 { rise }`	**Synopsis:** An integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
`fall { fall }`	**Synopsis:** An integer between 1 and 65535 The number of unsuccessful tracker queries before changing the router priority.

4. Type `commit` and press **Enter** to save the changes.

14.1.4.3 Deleting a VRRP Tracker

To delete a VRRP tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tracker by typing:

   ```
   no services vrrp trackers { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP tracker
3. Type `commit` and press **Enter** to save the changes.

14.1.5 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.

14.1.5.1 Viewing a List of VRRP Groups

To view a list of VRRP groups, type:

```
show running-config services vrrp group
```

If groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp group
services
 vrrp
  group group1
  !
 !
!
```

If no VRRP groups have been configured, add groups as needed. For more information, refer to "Adding a VRRP Group" (Page 783).

14.1.5.2 Adding a VRRP Group

To add a VRRP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the group by typing:

   ```
   services vrrp group { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP group
3. Type `commit` and press **Enter** to save the changes.

14.1.5.3 Deleting a VRRP Group

To delete a VRRP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the group by typing:

   ```
   no services vrrp group { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP group
3. Type `commit` and press **Enter** to save the changes.

14.1.6 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.

14.1.6.1 Viewing a List of VRRP Instances

To view a list of VRRP instances, type:

```
show running-config services vrrp instance
```

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance
services
 vrrp
  instance vid20
   interface switch.0001
   vrid      10
   priority  100
   group     group1
   monitor fe-cm-1
   !
   track-script tracker1
   !
   vrip 192.168.0.10/24
   !
  !
 !
!
```

If no VRRP instances have been configured, add instances as needed. For more information, refer to "Adding a VRRP Instance" (Page 784).

14.1.6.2 Adding a VRRP Instance

To add a VRRP instance, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a VRRP group has been configured. For more information, refer to "Adding a VRRP Group" (Page 783).
3. Add the instance by typing:

   ```
   services vrrp instance { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance. The name must not include spaces.
4. Configure the following parameter(s) as required:

⚠ 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 246).

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

Parameter	Description
`vrrp-version { vrrp-version }`	**Synopsis:** An integer between 2 and 3 **Default:** 2 Configure VRRP version for this instance.
`interface { interface }`	**Synopsis:** 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.
`vrid { vrid }`	**Synopsis:** An integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID.
`priority { priority }`	**Synopsis:** 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.
`advert-interval { advert-interval }`	**Synopsis:** An integer between 1 and 255 **Default:** 1 VRRP2 advertisement interval, in seconds.
`advert-interval-millisecond { advert-interval-millisecond }`	**Synopsis:** An integer between 20 and 3000 **Default:** 1000 VRRP3 advertisement interval in millisecond, must be multiple of 10.

Parameter	Description
`garp-delay { garp-delay }`	**Synopsis:** An integer between 1 and 255 **Default:** 5 Gratuitous ARP delay, in seconds. Sets the delay after the router changes state state before a second set of gratuitous ARPs are sent.
`nopreempt`	When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
`preempt-delay { preempt-delay }`	**Synopsis:** An integer between 0 and 1000 **Default:** 0 The time, in seconds, after startup until preemption.
`fault-to-master-delay { fault-to-master-delay }`	**Synopsis:** An integer between 0 and 1000 **Default:** 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).
`group { group }`	**Synopsis:** A string between 1 and 64 characters long Binds this VRRP instance to a VRRP group.

5. [Optional] Add one or more VRRP monitors. For more information, refer to "Adding a VRRP Monitor" (Page 787).
6. [Optional] Add one or more track scripts. For more information, refer to "Adding a Track Script" (Page 789).
7. Add one or more virtual IP addresses. For more information, refer to "Adding a Virtual IP Address" (Page 790).
8. Type `commit` and press **Enter** to save the changes.

14.1.6.3 Deleting a VRRP Instance

To delete a VRRP instance, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the instance by typing:

   ```
   no services vrrp instance { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
3. Type `commit` and press **Enter** to save the changes.

14.1.7 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.

14.1.7.1 Viewing a List of VRRP Monitors

To view a list of VRRP monitors, type:

```
show running-config services vrrp instance { name } monitor
```

Where:

- `{ name }` is the name of the VRRP instance

If monitors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance monitor
services
 vrrp
  instance vid20
   monitor fe-cm-1
   !
  !
 !
!
```

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to "Adding a VRRP Monitor" (Page 787).

14.1.7.2 Adding a VRRP Monitor

To add a VRRP monitor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the instance by typing:

   ```
   services vrrp instance { name } monitor { interface }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
   - `{ interface }` is the name of the extra interface to monitor
3. Configure the following parameter(s) as required:

Parameter	Description
`weight { weight }`	**Synopsis:** 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.

4. Type `commit` and press **Enter** to save the changes.

14.1.7.3 Deleting a VRRP Monitor

To delete a VRRP monitor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the monitor by typing:

   ```
   no services vrrp instance { name } monitor { interface }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
   - `{ interface }` is the name of the extra interface to monitor
3. Type `commit` and press **Enter** to save the changes.

14.1.8 Managing Track Scripts

Track scripts are used to associate VRRP trackers with VRRP instances.

14.1.8.1 Viewing a List of Track Scripts

To view a list of track scripts, type:

```
show running-config services vrrp instance { name } monitor
```

Where:

- `{ name }` is the name of the VRRP instance

If track scripts have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance track-script
services
 vrrp
  instance vid20
   track-script tracker1
   !
  !
 !
!
```

If no track scripts have been configured, add track scripts as needed. For more information, refer to "Adding a Track Script" (Page 789).

14.1.8.2 Adding a Track Script

To add a track script, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the track script by typing:

   ```
   services vrrp instance { name } track-script { tracker }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
   - `{ tracker }` is the name of the tracker to use to monitor the VRRP instance
3. Configure the following parameter(s) as required:

Parameter	Description
`weight { weight }`	**Synopsis:** 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.

4. Type `commit` and press **Enter** to save the changes.

14.1.8.3 Deleting a Track Script

To delete a track script, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the track script by typing:

   ```
   no services vrrp instance { name } track-script { track
   er }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
   - `{ tracker }` is the name of the tracker to use to monitor the VRRP instance
3. Type `commit` and press **Enter** to save the changes.

14.1.9 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.

14.1.9.1 Viewing a List of Virtual IP Addresses

To view a list of virtual IP addresses, type:

```
show running-config services vrrp instance { name } vrip
```

Where:

- `{ name }` is the name of the VRRP instance

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance vid20 vrip
services
 vrrp
  instance vid20
   vrip 192.168.0.10/24
   !
  !
 !
!
```

If no virtual IP addresses have been configured, add addresses as needed. For more information, refer to "Adding a Virtual IP Address" (Page 790).

14.1.9.2 Adding a Virtual IP Address

To add a virtual IP address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the instance by typing:

   ```
   services vrrp instance { name } vrip { address }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
   - `{ address }` is the address and subnet
3. Type `commit` and press **Enter** to save the changes.

14.1.9.3 Deleting a Virtual IP Address

To delete a virtual IP address, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the virtual IP address by typing:

   ```
   no services vrrp instance { name } vrip { address }
   ```

   Where:

   - `{ name }` is the name of the VRRP instance
   - `{ address }` is the virtual IP address and netmask

3. Type `commit` and press **Enter** to save the changes.

14.1.10 Managing Connection Synchronization

This section describes how to configure connection synchronization between two VRRP-enabled routers.

14.1.10.1 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 235).

1. Configure a firewall with stateful firewall rules to control inbound and outbound traffic. For more information, refer to "Adding a Firewall" (Page 239).
2. Make sure the VRRP service is enabled. For more information, refer to "Enabling/Disabling VRRP" (Page 780).
3. Configure VRRP instances and groups. For more information, refer to "Adding a VRRP Instance" (Page 784) and "Adding a VRRP Group" (Page 783).
4. Define one or more dedicated links for each VRRP group. For more information, refer to "Adding a Dedicated Link" (Page 792).
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 793).
6. Enable the configuration synchronization service. For more information, refer to "Enabling/Disabling Connection Synchronization" (Page 792).

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 794).

14.1.10.2 Enabling/Disabling Connection Synchronization

To enable or disable connection synchronization, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable connection synchronization by typing:

   Enabling

   ```
   services conn-sync enabled
   ```

   Disabling

   ```
   no services conn-sync enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

14.1.10.3 Viewing a List of Dedicated Links

To view a list of dedicated links, type:

```
show running-config services conn-sync dedicated-link | tab
```

If dedicated links have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services conn-sync dedicated-link | tab
                                                    SEND    RECV
NAME  INTERFACE  IP         MCAST IP    GROUP  BUFFER  BUFFER
-------------------------------------------------------------------
3     fe-2-3     100.0.5.1  225.0.0.51  3781   1220    1220
4     fe-2-4     100.1.5.1  225.0.0.52  3782   1220    1220

 !
!
```

If no dedicated links have been configured, add dedicated links as needed. For more information, refer to "Adding a Dedicated Link" (Page 792).

14.1.10.4 Adding a Dedicated Link

To add a dedicated link, do the following:

1. Make sure the CLI is in Configuration mode.

   Note

   RUGGEDCOM ROX II supports up to four dedicated links.

2. Add a dedicated link by typing:

   ```
   services conn-sync dedicated-link { name }
   ```

   Where { name } is the name of the dedicated link.

3. Configure the following parameter(s) as required:

Parameter	Description
`interface { interface }`	**Synopsis:** A string between 1 and 15 characters long The interface name of the dedicated link.
`ip { ip }`	**Synopsis:** 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.
`mcast-ip { mcast-ip }`	**Synopsis:** A string between 7 and 15 characters long or A string between 7 and 39 characters long **Default:** 225.0.0.50 The destination IPv4 or IPv6 multicast address of the dedicated link.
`group { group }`	**Synopsis:** An integer between 1 and 65535 **Default:** 3780 The multicast group ID of the cluster.
`send-buffer { send-buffer }`	**Synopsis:** An integer between 64 and 2560 **Default:** 1220 The sending socket buffer size in kB.
`recv-buffer { recv-buffer }`	**Synopsis:** An integer between 64 and 2560 **Default:** 1220 The receiving socket buffer size in kB.

4. Type `commit` and press **Enter** to save the changes.

14.1.10.5 Deleting a Dedicated Link

To delete a dedicated link, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the dedicated link by typing:

   ```
   no services conn-sync dedicated-link { name }
   ```

   Where { name } is the name of the dedicated link.
3. Type `commit` and press **Enter** to save the changes.

14.1.10.6 Selecting a Default Dedicated Link

To select a default a dedicated link, do the following:

1. Make sure the CLI is in Configuration mode.

2. Set the default dedicated link by typing:

   ```
   services conn-sync default-dedicated-link { link }
   ```

   Where { link } is the name of the default dedicated link.
3. Type `commit` and press **Enter** to save the changes.

14.1.10.7 Viewing the Status of Each Dedicated Link

To view the status of all dedicated links, do the following:

1. Make sure the CLI is in Configuration mode.
2. To view the status of all dedicated links, type the following:

   ```
   show services conn-sync status
   ```

   A list similar to the following example appears:

```
ruggedcom# show services conn-sync status
status fe-2-3
 state           NO-CARRIER
 role            ACTIVE
 byte sent       3614860
 byte received   0
 packet sent     114224
 packet received 0
 error sent      0
 error received  0
status fe-2-4
 state           NO-CARRIER
 role            BACKUP
 byte sent       0
 byte received   0
 packet sent     0
 packet received 0
 error sent      0
 error received  0
```

The list provides the following information:

Parameter	Description
`{ name }`	**Synopsis:** A string The conn-sync dedicated link interface name.
`state`	**Synopsis:** A string The conn-sync dedicated link status.
`role`	**Synopsis:** A string The conn-sync dedicated link role.
`byte-sent`	**Synopsis:** An integer The number of bytes sent on conn-sync dedicated link.

Parameter	Description
byte-received	**Synopsis:** An integer The number of bytes received on conn-sync dedicated link.
packet-sent	**Synopsis:** An integer The number of packets sent on conn-sync dedicated link.
packet-received	**Synopsis:** An integer The number of packets received on conn-sync dedicated link.
error-sent	**Synopsis:** An integer The number of errors sent on conn-sync dedicated link.
error-received	**Synopsis:** An integer The number of errors received on conn-sync dedicated link.

14.2 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 711).

14.2.1 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 713).
2. Enable the VRRP service for each VRF definition. For more information, refer to "Adding VRRP Service to a VRF" (Page 797).
3. [Optional] Add VRRP trackers as needed. For more information, refer to "Adding a VRRP Tracker for a VRF" (Page 799).
4. [Optional] Add VRRP groups as needed. For more information, refer to "Adding a VRRP Group for a VRF" (Page 800).
5. [Optional] Add VRRP monitors as needed. For more information, refer to "Adding a VRRP Monitor to a VRF" (Page 804).
6. [Optional] Add track scripts as needed. For more information, refer to "Adding a VRRP Track Script to a VRF" (Page 806).
7. Add a virtual IP address for the VRF. For more information, refer to "Adding a Virtual IP Address to a VRF" (Page 808).
8. Verify the network configuration.

14.2.2 Viewing the VRRP Status for a VRF

To view the VRRP status for a VRF, type:

```
show services vrrp vrf { name } status
```

Where:

- `{ name }` is the name of the VRF

IIf VRRP instances have been configured, a table or list similar to the following example appears:

```
 show services vrrp vrf vrf1 status
                                                                    MONITOR
                                                          INTERFACE INTERFACE
NAME      STATE   PRIORITY  TIME CHANGE                 STATE     STATE
-------------------------------------------------------------------------------
vrf-ins1  backup  130       Thu Jan 24 11:08:54 2019    fe-1-1 is Up
```

This table or list provides the following information:

Parameter	Description
`{ name }`	**Synopsis:** A string The VRRP instance name.
`state`	**Synopsis:** A string The VRRP instance state.
`priority`	**Synopsis:** A string The VRRP instance priority.
`time-change`	**Synopsis:** A string The time of change to the current state.
`interface-state`	**Synopsis:** A string The VRRP interface state.
`monitor-interface-state`	**Synopsis:** A string Monitors the interface state.

14.2.3 Configuring VRRP Service for a VRF

This section describes how to view, add and delete VRRP for a VRF.

14.2.3.1 Viewing a List of VRFs Configured with VRRP Service

To view a list of VRFs configured with VRRP service, type:

```
show running-config services vrrp vrf
```

If a VRF has been configured with VRRP service, a table or list similar to the following example appears:

```
show running-config services vrrp vrf
services
 vrrp
  vrf vrf1
   enabled
   no router-id
   group Grp-1
   !
   trackers tracker net-6
    network  6.6.6.4/30
    interval 1
   !
   instance vrf-ins1
    vrrp-version                3
    interface                   fe-1-1
    vrid                        101
    priority                    150
    advert-interval-millisecond 20
    group                       Grp-1
    vrip 100.100.100.101/24
    !
   !
```

If no VRF has been configured with VRRP service, add as needed. For more information, refer to "Adding VRRP Service to a VRF" (Page 797).

14.2.3.2 Adding VRRP Service to a VRF

To add VRRP service to a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the definition by typing:

   ```
   services vrrp vrf { name }
   ```

   Where:

   - `{ name }` is the name of the VRF. The name must be unique and not exceed 32 characters or contain spaces. The first character must also not be a special character. Only the following special characters are permitted in the remainder of the name: hyphen (-), underscore (_), colon (:), and period (.).
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables or disables the VRRP service.
`router-id { router-id }`	**Synopsis:** A string The router ID for VRRP logs.

4. Type `commit` and press **Enter** to save the changes.

14.2.3.3 Deleting VRRP Service from a VRF

To delete VRRP service from a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the definition key by typing:

   ```
   no services vrrp vrf { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP for VRF.
3. Type `commit` and press **Enter** to save the changes.

14.2.4 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.

14.2.4.1 Viewing a List of VRRP Trackers for a VRF

To view a list of VRRP trackers for a VRF, type:

```
show running-config services vrrp vrf trackers
```

If trackers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp vrf trackers
services
 vrrp
  vrf vrf1
   trackers tracker net-6
    network  6.6.6.4/30
    interval 1
   !
  !
 !
```

If no VRRP trackers have been configured, add trackers as needed. For more information, refer to "Adding a VRRP Tracker for a VRF" (Page 799).

14.2.4.2 Adding a VRRP Tracker for a VRF

To add a VRRP tracker for a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tracker by typing:

   ```
   services vrrp vrf trackers { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP tracker
3. Configure the following parameter(s) as required:

Parameter	Description
`type { type }`	**Synopsis:** [route] **Default:** route The type of condition for the tracker to check.
`network { network }`	**Synopsis:** 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 { interface }`	**Synopsis:** A string The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
`interval { interval }`	**Synopsis:** An integer between 1 and 120 The number of seconds between tracker queries.
`weight { weight }`	**Synopsis:** 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 { rise }`	**Synopsis:** An integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
`fall { fall }`	**Synopsis:** An integer between 1 and 65535 The number of unsuccessful tracker queries before changing the router priority.

4. Type `commit` and press **Enter** to save the changes.

14.2.4.3 Deleting a VRRP Tracker for a VRF

To delete a VRRP tracker for a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tracker by typing:

   ```
   no services vrrp vrf trackers { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP tracker
3. Type `commit` and press **Enter** to save the changes.

14.2.5 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.

14.2.5.1 Viewing a List of VRRP Groups for a VRF

To view a list of VRRP groups, type:

```
show running-config services vrrp vrf group
```

If groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp vrf group
services
 vrrp
  vrf vrf1
   group Grp-1
   !
  !
 !
```

If no VRRP groups have been configured, add groups as needed. For more information, refer to "Adding a VRRP Group" (Page 783).

14.2.5.2 Adding a VRRP Group for a VRF

To add a VRRP group for a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the group by typing:

   ```
   services vrrp vrf group { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP group

3. Configure the following parameter(s) as required:

Parameter	Description
`name { name }`	**Synopsis:** A string between 1 and 64 characters long The VRRP group name.

4. Type `commit` and press **Enter** to save the changes.

14.2.5.3 Deleting a VRRP Group

To delete a VRRP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the group by typing:

   ```
   no services vrrp vrf group { name }
   ```

   Where:

   - `{ name }` is the name of the VRRP group

3. Type `commit` and press **Enter** to save the changes.

14.2.6 Managing VRRP Instances for a VRF

VRRP instances can be configured for one or more VRF definitions. This is done by by enabling VRRP for a VRF and then configuring the required VRRP parameters.

14.2.6.1 Viewing a List of VRRP Instances for a VRF

To view a list of VRF instances defined for OSPF, type:

```
show running-config services vrrp vrf instance
```

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp vrf instance
services
 vrrp
  vrf vrf1
   instance vrf-ins1
    vrrp-version                3
    interface                   fe-1-1
    vrid                        101
    priority                    220
    advert-interval-millisecond 500
    group                       Grp-1
    vrip 100.100.100.101/24
    !
   !
```

```
!
```

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 802).

14.2.6.2 Adding a VRRP Instance for a VRF

To add a VRRP instance for a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the group by typing:

   ```
   services vrrp vrf { name } instance
   ```

   Where:

   - `{ name }` is the name of the VRF
3. Configure the following parameter(s) as required:

⚠ 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 246).

Parameter	Description
`vrrp-version { vrrp-version }`	**Synopsis:** An integer between 2 and 3 **Default:** 2 Configure VRRP version for this instance.
`interface { interface }`	**Synopsis:** 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.
`vrid { vrid }`	**Synopsis:** An integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID.
`priority { priority }`	**Synopsis:** 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.
`advert-interval { advert-interval }`	**Synopsis:** An integer between 1 and 255 **Default:** 1 VRRP2 advertisement interval, in seconds.

Parameter	Description
`advert-interval-millisecond { advert-interval-millisecond }`	**Synopsis:** An integer between 20 and 3000 **Default:** 1000 VRRP3 advertisement interval in millisecond, must be multiple of 10.
`garp-delay { garp-delay }`	**Synopsis:** An integer between 1 and 255 **Default:** 5 Gratuitous ARP delay, in seconds. Sets the delay after the router changes state state before a second set of gratuitous ARPs are sent.
`nopreempt`	When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
`preempt-delay { preempt-delay }`	**Synopsis:** An integer between 0 and 1000 **Default:** 0 The time, in seconds, after startup until preemption.
`fault-to-master-delay { fault-to-master-delay }`	**Synopsis:** An integer between 0 and 1000 **Default:** 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).
`group { group }`	**Synopsis:** A string between 1 and 64 characters long Binds this VRRP instance to a VRRP group.

4. Type `commit` and press **Enter** to save the changes.

14.2.6.3 Deleting a VRRP Instance for a VRF

To delete a VRF instance for a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the definition key by typing:

   ```
   no services vrrp vrf { name } instance
   ```

   Where:

   - `{ name }` is the name of the VRF
3. Type `commit` and press **Enter** to save the changes.

14.2.7 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.

14.2.7.1 Viewing a List of VRRP Monitors for a VRF

To view a list of VRRP monitors, type:

```
show running-config services vrrp vrf { vrf name } instance
{ name } monitor
```

Where:

- `{ vrf name }` is the name of the VRF
- `{ name }` is the name of the VRRP instance

If monitors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp vrf instance vrf-ins1 monitor
services
 vrrp
  vrf vrf1
   instance vrf-ins1
    monitor fe-1-1
    !
   !
  !
 !
!
```

If no monitors have been configured, add monitors as needed. For more information, refer to "Adding a VRRP Monitor to a VRF" (Page 804).

14.2.7.2 Adding a VRRP Monitor to a VRF

To add a VRRP monitor to a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the instance by typing:

   ```
   services vrrp vrf { vrf name } instance { name } monitor
   { interface }
   ```

   Where:

   - `{ vrf name }` is the name of the VRF
   - `{ name }` is the name of the VRRP instance
   - `{ interface }` is the name of the extra interface to monitor
3. Configure the following parameter(s) as required:

Parameter	Description
`weight { weight }`	**Synopsis:** 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.

4. Type `commit` and press **Enter** to save the changes.

14.2.7.3 Deleting a VRRP Monitor from a VRF

To delete a VRRP monitor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the monitor by typing:

   ```
   no services vrrp vrf { vrf name } instance { name } moni
   tor { interface }
   ```

   Where:

   - `{ vrf name }` is the name of the VRF
   - `{ name }` is the name of the VRRP instance
   - `{ interface }` is the name of the extra interface to delete
3. Type `commit` and press **Enter** to save the changes.

14.2.8 Managing VRRP Track Scripts for a VRF

Track scripts are used to associate VRRP trackers with VRRP instances.

14.2.8.1 Viewing a List of VRRP Track Scripts for a VRF

To view a list of track scripts, type:

```
show running-config services vrrp vrf instance { name }
track-script
```

Where:

- `{ name }` is the name of the VRRP instance

If track scripts have been configured, a table or list similar to the following example appears:

```
show running-config services vrrp vrf instance vrf-ins1  track-script
services
 vrrp
```

```
   vrf vrf1
    instance vrf-ins1
     track-script net-6
     !
    !
   !
  !
 !
```

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 806).

14.2.8.2 Adding a VRRP Track Script to a VRF

To add a track script, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the track script by typing:

   ```
   services vrrp vrf { vrf name } instance { name } track-
   script { tracker }
   ```

   Where:

   - `{ vrf name }` is the name of the VRF
   - `{ name }` is the name of the VRRP instance
   - `{ tracker }` is the name of the tracker to use to monitor the VRRP instance
3. Configure the following parameter(s) as required:

Parameter	Description
`weight { weight }`	**Synopsis:** 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.

4. Type `commit` and press **Enter** to save the changes.

14.2.8.3 Deleting a VRRP Track Script from a VRF

To delete a track script, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the track script by typing:

   ```
   no services vrrp vrf { vrf name } instance { name } track-
   script { tracker }
   ```

Where:

- `{ vrf name }` is the name of the VRF
- `{ name }` is the name of the VRRP instance
- `{ tracker }` is the name of the tracker to use to monitor the VRRP instance

3. Type `commit` and press **Enter** to save the changes.

14.2.9 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.

14.2.9.1 Viewing a List of Virtual IP Addresses

To view a list of virtual IP addresses, type:

```
show running-config services vrrp vrf { vrf name } instance
{ name } vrip
```

Where:

- `{ vrf name }` is the name of the VRF
- `{ name }` is the name of the VRRP instance

If VRIPs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp vrf vrf1 instance vrf-ins1 vrip
services
 vrrp
  vrf vrf1
   instance vrf-ins1
    vrip 100.100.100.101/24
    !
   !
  !
 !
```

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 808).

14.2.9.2 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. Make sure the CLI is in Configuration mode.
2. Add the instance by typing:

   ```
   services vrrp vrf { vrf name } instance { name } vrip
   { address }
   ```

   Where:

   - `{ vrf name }` is the name of the VRF
   - `{ name }` is the name of the VRRP instance
   - `{ address }` is the address and subnet
3. Type `commit` and press **Enter** to save the changes.

14.2.9.3 Deleting a Virtual IP Address from a VRF

To delete a virtual IP address from a VRF, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the virtual IP address by typing:

   ```
   no services vrrp vrf { vrf name } instance { name } vrip
   { address }
   ```

   Where:

   - `{ vrf name }` is the name of the VRF
   - `{ name }` is the name of the VRRP instance
   - `{ address }` is the address and subnet
3. Type `commit` and press **Enter** to save the changes.

14.2.10 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

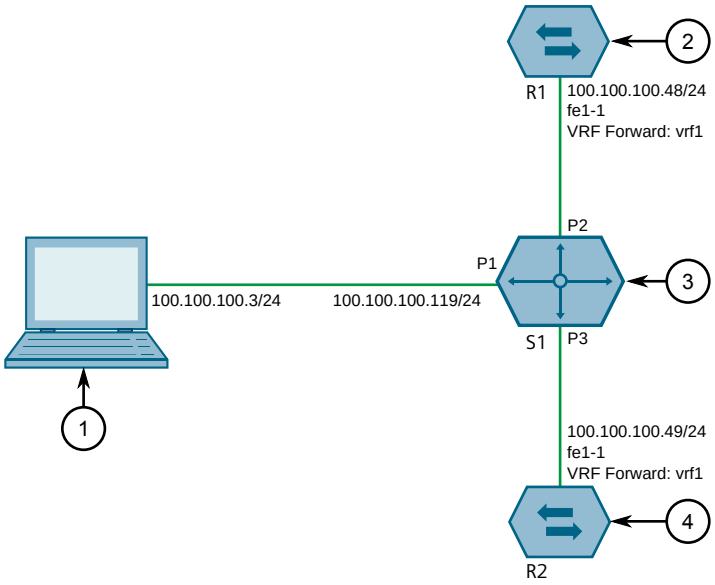
RUGGEDCOM ROX II supports VRRP within VRF for IPv4 addresses only.

⚠ NOTICE

Connection synchronization is not supported for VRRPs within a VRF. For more information about connection synchronization, refer to "Connection Synchronization" (Page 779).

⚠ 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 14.4 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 386).

b. Assign IP address *100.100.100.119* to VLAN 100. For more information, refer to "Adding an IPv4 Address" (Page 269).

c. Assign VLAN 100 to ports 1, 2 and 3. For more information, refer to "Configuring a Switched Ethernet Port" (Page 335).

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 715).

   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 717).

   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 810) to forward traffic to vrf1. For more information, refer to "Configuring a VRF Interface" (Page 714).

   e. Enable VRRP Service for VRF. For more information, refer to "Adding VRRP Service to a VRF" (Page 797).

   f. Configure a VRF instance with the folowing parameters:

Interface	Virtual Router ID	Priority
fe-1-1	101	150

   For more information, refer to "Adding a VRRP Instance for a VRF" (Page 802).

   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 808).

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 715).

   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 717).

   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 810) to forward traffic to vrf1. For more information, refer to "Configuring a VRF Interface" (Page 714).

   e. Enable VRRP Service for VRF. For more information, refer to "Adding VRRP Service to a VRF" (Page 797).

   f. Configure a VRF instance with the folowing parameters:

Interface	VRID	Priority
fe-1-1	101	130

For more information, refer to "Adding a VRRP Instance for a VRF" (Page 802).

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 808).

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
                                                                    MONITOR
                                                    INTERFACE       INTERFACE
NAME      STATE  PRIORITY  TIME CHANGE              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
                                                                    MONITOR
                                                    INTERFACE       INTERFACE
NAME      STATE  PRIORITY  TIME CHANGE              STATE           STATE
-------------------------------------------------------------------------------
vrf-ins1  backup  130       Fri Jan 25 13:43:52 2019  fe-1-1 is Up
```

14.3 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 be Ethernet, Cellular Modem, T1/E1, or DDS.

Link failover can back up to multiple remote locations, managing multiple main-to-backup link relationships. When the backup link is a modem, many profiles of dialed numbers can exist, each serving as a distinct backup link.

Link failover can back up a permanent, high-speed WAN link to a permanent, low-speed WAN link. Use this function when OSPF cannot be employed, such as on public links.

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.

14.3.1 Viewing the Link Failover Log

To view the link failover log, do the following:

1. Make sure the CLI is in Configuration mode.
2. Display the log by typing:

   ```
   services link-failover log
   ```

   A table or list similar to the following appears:

```
ruggedcom(config)# services link-failover switch.0001 log
link-backup-log /var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd initializing.
/var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd configured and started.
/var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-cm-1 is up
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: creating thread to monitor main=switch.0001
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: setting new_backup_record
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: setting new_backup_record done!
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: dumping backup record:
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:   main_interface = switch.0001
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_test_host = 10.10.10.10
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     start_delay = 180
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_path_down_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_path_up_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_path_up_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_timeout = 2
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_interval = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_retry_count = 3
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_interface = fe-1-1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       backup gateway = 192.168.1.2
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       ondemand = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       distance = 1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       transfer default route = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_interface = te1-2-1c01ppp
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       ondemand = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       distance = 1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       transfer default route = yes
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-1-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_down: interface fe-1-1 is down
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-1-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_down: interface fe-1-1 is down
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-cm-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface switch.0001 is
 up
/var/log/syslog:Jan 25 09:47:11 R1-RX1512 linkd[4183]: linkd_interface_down: interface switch.0001 is
 down
/var/log/syslog:Jan 25 09:47:14 R1-RX1512 linkd[4183]: linkd_interface_up: interface switch.0001 is
 up
/var/log/syslog:Jan 25 09:49:52 R1-RX1512 linkd[4183]: Start monitoring link backup set:
 "switch.0001"
```

14.3.2 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:

```
show services link-failover status
```

A table or list similar to the following appears:

```
ruggedcom# show services link-failover status
```

```
             MAIN    BACKUP  MAIN                                                    BACKUP
             LINK    LINK    PING  TIME OF LAST STATE                                INTERFACE
MAIN         STATUS  STATUS  TEST  CHANGE                    LINK BACKUP STATE     IN USE
-------------------------------------------------------------------------------------------
switch.0001  up      down    ok    Fri Jan 25 09:49:52 2013  Main path is active  fe-1-1
```

The table or list provides the following information:

Parameter	Description
`main-link-status`	**Synopsis:** A string The main link status.
`backup-link-status`	**Synopsis:** A string The backup link status.
`main-ping-test`	**Synopsis:** A string The results of pinging the target using the main interface.
`time-of-last-state-change`	**Synopsis:** A string The time of the last state change.
`link-backup-state`	**Synopsis:** A string The backup link state.
`backup-interface-in-use`	**Synopsis:** A string The name of the backup interface that is being used.

14.3.3 Managing Link Failover Parameters

This section describes how to manage parameter settings for link failover.

14.3.3.1 Viewing a List of Link Failover Parameters

To view a list of link failover parameters, type:

```
show running-config services link-failover
```

If parameters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services link-failover
services
 link-failover switch.0001
  enabled
  backup fe-1-1
   transfer-default-route
   backup-gateway         192.168.1.2
  !
  backup te1-2-1c01ppp
   priority               second
   transfer-default-route
  !
```

```
   target 10.10.10.10
   !
  !
 !
```

If no parameters have been configured, add parameters as needed. For more information, refer to "Adding a Link Failover Parameter" (Page 814).

14.3.3.2 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. Make sure the CLI is in Configuration mode.
2. Add the parameter by typing:

   ```
   services link-failover { interface }
   ```

   Where:

   - `{ interface }` is the name of the interface
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables this link backup.
`ping-timeout { ping-timeout }`	**Synopsis:** An integer between 1 and 65536 **Default:** 2 The time interval, in seconds, before immediately retrying a ping.
`ping-interval { ping-interval }`	**Synopsis:** An integer between 0 and 65536 **Default:** 60 The time interval, in seconds, between ping tests.
`ping-retry { ping-retry }`	**Synopsis:** An integer between 0 and 65536 **Default:** 3 The number of ping retries before constructing a path failure.
`start-delay { start-delay }`	**Synopsis:** An integer between 0 and 65536 **Default:** 180 The delay time, in seconds, when first starting link failover.

Parameter	Description
`main-down-timeout { main-down-timeout }`	**Synopsis:** An integer between 0 and 65536 **Default:** 60 The delay time, in seconds, that the main trunk is down before starting the backup trunk.
`main-up-timeout { main-up-timeout }`	**Synopsis:** An integer between 0 and 65536 **Default:** 60 The delay time, in seconds, to confirm that the main trunk is up (returned to service) before stopping the backup trunk.

4. Type `commit` and press **Enter** to save the changes.

14.3.3.3 Deleting a Link Failover Parameter

To delete a link failover parameter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the parameter by typing:

   ```
   no services link-failover { interface }
   ```

   Where:

   - `{ interface }` is the name of the interface
3. Type `commit` and press **Enter** to save the changes.

14.3.4 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.

14.3.4.1 Viewing a List of Link Failover Backup Interfaces

To view a list of link failover backup interfaces, type:

```
show running-config services link-failover { interface }
backup
```

Where:

- `{ interface }` is the name of the interface

If backup interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services link-failover switch.0001 backup
```

```
services
 link-failover switch.0001
  backup fe-1-1
   transfer-default-route
   backup-gateway         192.168.1.2
  !
  backup te1-2-1c01ppp
   priority               second
   transfer-default-route
  !
 !
!
```

If no backup interfaces have been configured, add backup interfaces as needed. For more information, refer to "Adding a Link Failover Backup Interface" (Page 816).

14.3.4.2 Adding a Link Failover Backup Interface

To set a link failover backup interface, do the following:

⚠ NOTICE

Configuration hazard – risk of connection loss.

If a RUGGEDCOM APE module is installed, either avoid configuring switch.0001 as a link failover backup interface or configure a different VLAN for the APE module. By default, APE modules utilize VLAN 1 (switch.0001) and always keep the interface in the UP state. This would interfere with the link failover mechanism.

To configure a different VLAN for the APE module, change the PVID for the associated switched Ethernet port. For information, refer to "Configuring a Switched Ethernet Port" (Page 335).

1. Make sure the CLI is in Configuration mode.
2. Add the backup interface by typing:

   ```
   services link-failover { interface } backup { backup-in
   terface }
   ```

   Where:

   - `{ interface }` is the name of the interface
   - `{ backup-interface }` is the name of the secondary, backup interface
3. 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 { priority }`	**Synopsis:** [third | second | first] **Default:** first The priority which is applied to the backup interface when switching.
`transfer-default-route`	The transfer default gateway on the switching main and backup interface. The default route on the device must have a **distance** greater than one.
`backup-gateway { back up-gateway }`	**Synopsis:** A string up to 15 characters long The IP address of the backup gateway.
`on-demand`	**Synopsis:** [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.

4. Type `commit` and press **Enter** to save the changes.

14.3.4.3 Deleting a Link Failover Backup Interface

To delete a link failover backup interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the backup interface by typing:

   ```
   no services link-failover { interface } backup { back up-interface }
   ```

   Where:

   - `{ interface }` is the name of the interface
   - `{ backup-interface }` is the name of the secondary, backup interface
3. Type `commit` and press **Enter** to save the changes.

14.3.5 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.

14.3.5.1 Viewing a List of Link Failover Ping Targets

To view a list of link failover ping targets, type:

```
show running-config services link-failover { interface } tar
get
```

Where:

- `{ interface }` is the name of the interface

If ping targets have been configured, a table or list similar to the following example appears:

```
R1-RX1512# show running-config services link-failover switch.0001 target
services
 link-failover switch.0001
  target 10.10.10.10
  !
 !
!
```

If no ping targets have been configured, add targets as needed. For more information, refer to "Adding a Link Failover Ping Target" (Page 818).

14.3.5.2 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. Make sure the CLI is in Configuration mode.
2. Add the ping target by typing:

   ```
   services link-failover { interface } target { address }
   ```

   Where:

   - `{ interface }` is the name of the interface
   - `{ address }` is the IP address of the target host to verify the main path
3. Type `commit` and press **Enter** to save the changes.

14.3.5.3 Deleting a Link Failover Ping target

To delete a link failover ping target, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the backup interface by typing:

   ```
   no services link-failover { interface } target { address }
   ```

   Where:

   - `{ interface }` is the name of the interface
   - `{ address }` is the IP address of the target host to verify the main path
3. Type `commit` and press **Enter** to save the changes.

14.3.6 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 812).

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 820).

Canceling the test returns the interfaces to their pre-test condition.

---

1. Make sure the CLI is in Configuration mode.
2. Start the test by typing:

   ```
   services link-failover { interface } start-test start-
   test-delay { delay } test-duration { duration }
   ```

   Where:

   - `{ interface }` is the name of the interface
   - `{ delay }` is the time (in seconds) to wait before running the test
   - `{ duration }` is the maximum time (in minutes) to run the test before restoring service to the main trunk

14.3.7 Canceling a Link Failover Test

To cancel a link failover test, type:

```
services link-failover { interface } cancel-test
```

Where:

- `{ interface }` is the name of the interface

14.4 Managing Spanning Tree Protocol

This section describes how to manage the Spanning Tree Protocol (STP).

14.4.1 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 802.12D-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.

14.4.1.1 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.

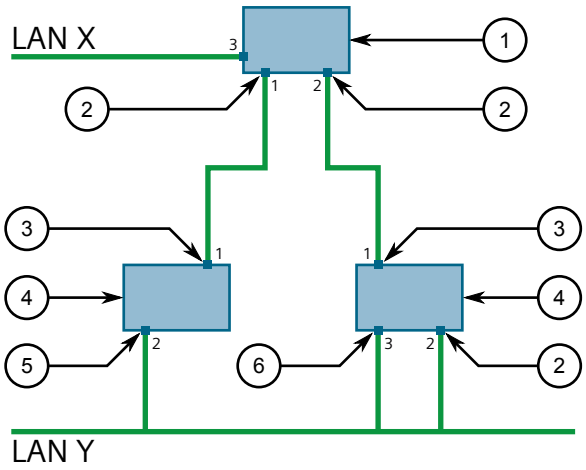
⚠ NOTICE

Purely for purposes of management, RUGGEDCOM ROX II introduces two more states: *Disabled* and *Link Down*. The *Disabled* state refers to links for which RSTP has been disabled. The *Link Down* 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 14.5 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.

14.4.1.2 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.

14.4.1.3 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.

14.4.1.4 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.

14.4.1.5 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 ¼ 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.

14.4.1.6 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.

14.4.1.7 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

14.4.2 RSTP Applications

This section describes various applications of RSTP.

14.4.2.1 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 14.6, "Example - Structured Wiring Configuration" (Page 826) would leave all the ports of bridges 555 through 888 connected to the network.

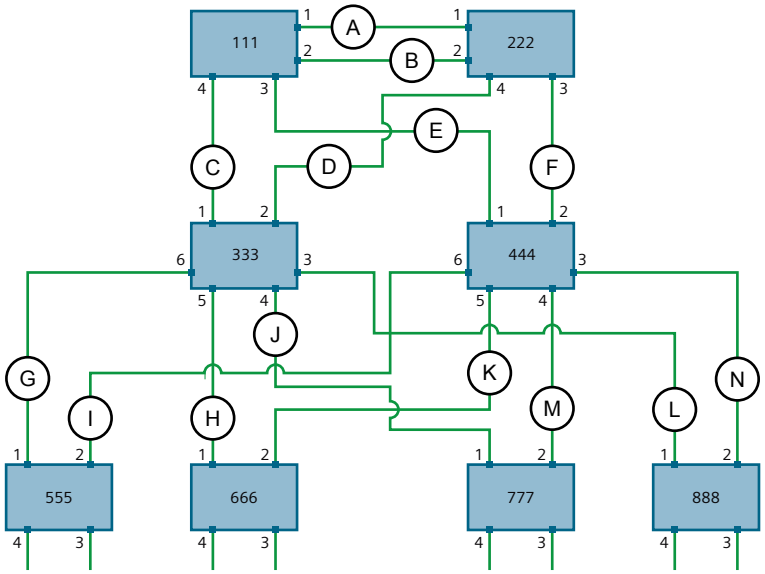


Figure 14.6 Example - Structured Wiring Configuration

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 of 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.

14.4.2.2 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 14.7, "Example - Ring Backbone Configuration" (Page 827). 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.

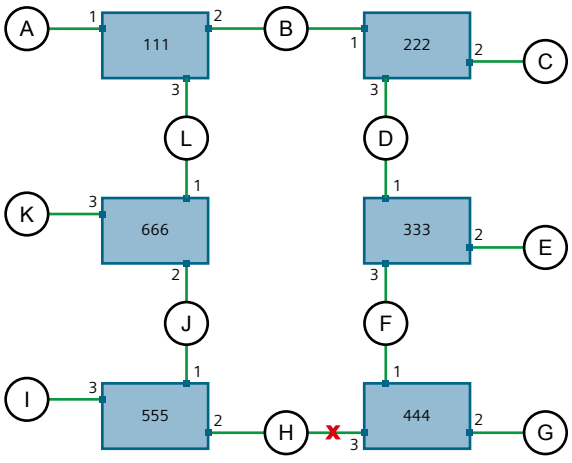


Figure 14.7 Example - Ring Backbone Configuration

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]".

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.

14.4.2.3 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.

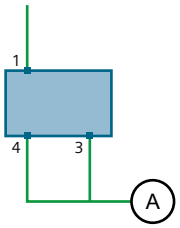


Figure 14.8 Example - Port Redundancy

14.4.3 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.

14.4.3.1 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.

14.4.3.2 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.
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	• 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. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.
MSTI Port Roles	For each MSTI on a bridge: • 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. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root. 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.
Boundary Ports	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. A Boundary Port may be: • The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port). • 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. 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

Role	Description
	MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.

14.4.3.3 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.

14.4.3.4 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 833).
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 841).
3. Create static VLANs and map them to the MSTIs. For more information, refer to "Adding a Static VLAN" (Page 386).
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 842).
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 833).

14.4.4 Configuring STP Globally

To configure global settings for the Spanning Tree Protocol (STP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » spanning-tree***.
3. Configure the basic STP settings by configuring the following parameter(s):

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true 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.

Parameter	Description
`version { version }`	**Synopsis:** [stp | rstp | mstp] **Default:** rstp The version (either only STP or Rapid STP or Multiple STP) of the Spanning Tree Protocol (STP) to support.
`hello-time { hello-time }`	**Synopsis:** An integer between 1 and 10 **Default:** 2 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 : maxAgeTime >= 2 * (helloTime + 1.0 seconds))
`max-age { max-age }`	**Synopsis:** An integer between 6 and 40 **Default:** 20 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 : maxAgeTime >= 2 * (helloTime + 1.0 seconds))
`tx-hold-count { tx-hold-count }`	**Synopsis:** An integer between 0 and 100 **Default:** 0 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.
`forward-delay { forward-delay }`	**Synopsis:** An integer between 4 and 30 **Default:** 15 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.
`max-hops { max-hops }`	**Synopsis:** An integer between 6 and 40 **Default:** 20 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 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.

Parameter	Description
`mst-region-name { mst-region-name }`	**Synopsis:** 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 { mst-revision-level }`	**Synopsis:** An integer between 0 and 65535 **Default:** 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.

4. Configure the eRSTP settings by configuring the following parameter(s):

Parameter	Description
`max-net-diameter-multiplier { max-net-diameter-multiplier }`	**Synopsis:** [1 | 4] **Default:** 4 The Max Network Diameter as a multiplier of the MaxAgeTime value.
`bpdu-guard { bpdu-guard }`	**Synopsis:** [specify | noshutdown | untilreset] **Default:** 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. • NO SHUTDOWN: BPDU Guard is disabled. • UNTIL RESET: The port will remain shut down until the port reset command is issued by the user. • SPECIFY: A timeout period is specified for the port using the BPDU Timeout parameter.
`bpdu-timeout { bpdu-timeout }`	**Synopsis:** An integer between 1 and 86400 The time for which a port is shutdown. Only applicable when BPDU Guard Mode is set to **specify**.
`fast-root-failover { fast-root-failover }`	**Synopsis:** [on | off | on-with-standard-root] **Default:** on The Fast Root Failover algorithm. Options include: • 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.

Parameter	Description
	• 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. • 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.
`dot1w-interop { dot1w-interop }`	**Synopsis:** [true | false] **Default:** true Enables/disables IEEE 802.1w Interoperability
`cost-style { cost-style }`	**Synopsis:** [stp | rstp] **Default:** 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).

5. Configure the RSTP instance settings by configuring the following parameter(s):

Parameter	Description
`bridge-priority { bridge-priority }`	**Synopsis:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Default:** 32768 The priority assigned to the RSTP/Common Bridge Instance.

6. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 841).
7. Type `commit` and press **Enter** to save the changes.

14.4.5 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. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For switched Ethernet ports:**
     interface » switch » { interface } » spanning-tree, where { interface } is the name given to the switched Ethernet port.

- **For Ethernet trunk interfaces:**
  interface » trunks » { id } » spanning-tree, where { id } is the ID given to the interface.

3. Configure the following parameter(s):

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/disables STP/RSTP on the interface.
`admin-edge { admin-edge }`	**Synopsis:** [forceTrue | forceFalse | auto] **Default:** auto 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 **Edgeness** of the port will be switched off and the standard RSTP rules will apply (until the next link outage).
`admin-point-to-point { admin-point-to-point }`	**Synopsis:** [forceTrue | forceFalse | auto] **Default:** auto 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).
`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.

Parameter	Description
`rstp-priority { rstp-priority }`	**Synopsis:** [0 | 16 | 32 | 64 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 224 | 240] **Default:** 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 { stp-cost }`	**Synopsis:** [auto-cost] or An integer between 0 and 65535 **Default:** 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 { rstp-cost }`	**Synopsis:** [auto-cost] or An integer between 0 and 2147483647 **Default:** 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.

4. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 841).
5. Type `commit` and press **Enter** to save the changes.

14.4.6 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 829).

14.4.6.1 Viewing Statistics for Multiple Spanning Tree Instances

To view statistics related to Multiple Spanning Tree Instances (MSTIs), type:

```
show switch spanning-tree msti-status
```

A table or list similar to the following example appears:

```
ruggedcom# show switch spanning-tree msti-status | tab
                                                                                ROOT  ROOT  ROOT  TOTAL
INSTANCE          ROOT                          BRIDGE                        PORT  PORT  PATH  TOP
ID        STATUS  PRIORITY  ROOT MAC            PRIORITY  BRIDGE MAC          SLOT  PORT  COST  CHANGES
--------------------------------------------------------------------------------------------------------
1         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
2         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
3         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
4         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
5         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
6         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
7         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
8         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
9         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
10        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
11        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
12        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
13        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
14        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
15        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
16        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
```

The table or list provides the following information:

Parameter	Description
`{ instance-id }`	**Synopsis:** An integer between 1 and 16 The bridge identifier of this bridge.
`status`	**Synopsis:** [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`	**Synopsis:** An integer The bridge identifier of the root bridge.
`root-mac`	**Synopsis:** A string up to 17 characters long The bridge identifier of the root bridge.
`bridge-priority`	**Synopsis:** An integer The bridge identifier of this bridge.
`bridge-mac`	**Synopsis:** A string up to 17 characters long The bridge identifier of this bridge.

Parameter	Description
root-port-slot	**Synopsis:** [--- | 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	**Synopsis:** 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	**Synopsis:** 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 configured, 1Gbps 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.
total-top-changes	**Synopsis:** 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.

14.4.6.2 Viewing a List of Multiple Spanning Tree Instances

To view a list of Multiple Spanning Tree Instances (MSTIs), type:

```
show running-config switch spanning-tree mstp-instance
```

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch spanning-tree mstp-instance | tab
INSTANCE  BRIDGE
ID        PRIORITY
--------------------
1         32768
2         57344

!
```

If no MSTIs have been configured, add instances as needed. For more information, refer to "Adding a Multiple Spanning Tree Instance" (Page 841).

14.4.6.3 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. Make sure the CLI is in Configuration mode.

⚠ 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.

2. Add the Multiple Spanning Tree Instance by typing:

```
switch spanning-tree mstp-instance { id }
```

Where:

- `{ id }` is the ID for the Multiple Spanning Tree Instance

3. Configure the following parameter(s) as required:

Parameter	Description
`bridge-priority { bridge-priority }`	**Synopsis:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Default:** 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 can establish the path of traffic flows in normal and abnormal conditions.

4. Map one or more static VLANs and map them to the MSTI. For more information, refer to "Adding a Static VLAN" (Page 386).
5. Type `commit` and press **Enter** to save the changes.

14.4.6.4 Deleting a Multiple Spanning Tree Instance

To delete a Multiple Spanning Tree Instance (MSTI), do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the multiple spanning tree instance by typing:

   ```
   no switch spanning-tree mstp-instance { ID }
   ```

   Where:

   - `{ ID }` is the ID of the multiple spanning tree instance
3. Type `commit` and press **Enter** to save the changes.

14.4.7 Managing Multiple Spanning Tree Instances Per-Port

This section describes how to configure and manage Multiple Spanning Tree Instances (MSTIs) for individual ports.

14.4.7.1 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, type:

```
show switch spanning-tree port-msti-id
```

A table similar to the following example appears:

```
ruggedcom# show switch spanning-tree port-msti-id
                                                DESIG
INSTANCE                  STP       STP         BRIDGE
ID        SLOT    PORT    STATE     ROLE  COST  PRIORITY  DESIG BRIDGE MAC
-------------------------------------------------------------------------------
1
          swport  1       disabled  ----  0     0         00:00:00:00:00:00
          swport  2       disabled  ----  0     0         00:00:00:00:00:00
          swport  3       disabled  ----  0     0         00:00:00:00:00:00
          swport  4       disabled  ----  0     0         00:00:00:00:00:00
          swport  5       disabled  ----  0     0         00:00:00:00:00:00
          swport  6       disabled  ----  0     0         00:00:00:00:00:00
2
          swport  1       disabled  ----  0     0         00:00:00:00:00:00
          swport  2       disabled  ----  0     0         00:00:00:00:00:00
          swport  3       disabled  ----  0     0         00:00:00:00:00:00
          swport  4       disabled  ----  0     0         00:00:00:00:00:00
          swport  5       disabled  ----  0     0         00:00:00:00:00:00
          swport  6       disabled  ----  0     0         00:00:00:00:00:00
.
.
.
```

This table provides the following information:

Parameter	Description
`instance-id`	**Synopsis:** An integer between 1 and 16 The Multiple Spanning Tree Protocol (MSTP) Instance ID.

Parameter	Description
`{ slot }`	**Synopsis:** [sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport | trnk] The slot of the module that contains this port.
`{ port }`	**Synopsis:** An integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
`stp-state`	**Synopsis:** [disabled | blocking | listening | learning | forwarding | linkDown | discarding] The status of this interface in the spanning tree: • Disabled: The Spanning Tree Protocol (STP) is disabled on this port. • Link Down: STP is enabled on this port but the link is down. • Discarding: The link is not used in the STP topology but is standing by. • Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • Forwarding: The port is forwarding traffic.
`stp-role`	**Synopsis:** [---- | root | designated | alternate | backup | master] The role of this port in the spanning tree: • Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to. • Root: The single port on the bridge, which provides connectivity towards the root bridge. • 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. • Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • 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).
`cost`	**Synopsis:** 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 configured, 1Gbps 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.

Parameter	Description
`desig-bridge-priority`	**Synopsis:** An integer The bridge identifier of this bridge.
`desig-bridge-mac`	**Synopsis:** A string up to 17 characters long The bridge identifier of this bridge.

14.4.7.2 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, type:

- **For switched Ethernet ports:**

  ```
  show running-config interface switch { slot } { port }
  spanning-tree msti
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module

- **For Ethernet trunk interfaces:**

  ```
  show running-config interface trunk { id } spanning-tree
  msti
  ```

  Where:

  - `{ id }` is the ID given to the interface

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface trunks 1 spanning-tree msti | tab
INSTANCE  MSTP
ID        PRIORITY  STP COST   RSTP COST
-----------------------------------------
1         128       auto-cost  auto-cost
2         128       auto-cost  auto-cost

 !
!
```

```
show running-config interface trunk { id } spanning-tree msti
```

Where:

- `{ id }` is the ID given to the interface

If MSTIs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface trunks 1 spanning-tree msti | tab
INSTANCE  MSTP
ID        PRIORITY  STP COST   RSTP COST
-----------------------------------------
1         128       auto-cost  auto-cost
2         128       auto-cost  auto-cost

 !
!
```

If no MSTIs have been configured, add them as needed. For more information, refer to "Adding a Port-Specific Multiple Spanning Tree Instance" (Page 845).

14.4.7.3 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. Make sure the CLI is in Configuration mode.

   ⚠ 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.

2. Add the MSTI by typing:
   - **For switched Ethernet ports:**

     `interface switch { slot } { port } spanning-tree msti { id }`

     Where:
     - `{ slot }` is the name of the module location
     - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - `{ id }` is the ID for the Multiple Spanning Tree Instance
   - **For Ethernet trunk interfaces:**

     `interface trunks { id } spanning-tree msti { mstp-id }`

     Where:
     - `{ id }` is the ID given to the interface
     - `{ mstp-id }` is the ID for the Multiple Spanning Tree Instance
3. Configure the following parameter(s) as required:

Parameter	Description
`mstp-priority { mstp-priority }`	**Synopsis:** [0 | 16 | 32 | 64 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 224 | 240] **Default:** 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 { stp-cost }`	**Synopsis:** [auto-cost] or An integer between 0 and 65535 **Default:** auto-cost 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.
`rstp-cost { rstp-cost }`	**Synopsis:** [auto-cost] or An integer between 0 and 2147483647 **Default:** auto-cost 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.

4. Map one or more static VLANs and map them to the MSTI. For more information, refer to "Adding a Static VLAN" (Page 386).
5. Type `commit` and press **Enter** to save the changes.

14.4.7.4 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. Make sure the CLI is in Configuration mode.
2. Delete the MSTI by typing:
   - **For switched Ethernet ports:**

     ```
     no interface switch { slot } { port } spanning-tree
     msti { id }
     ```

     Where:

     - `{ slot }` is the name of the module location

- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ id }` is the ID for the Multiple Spanning Tree Instance

- **For Ethernet trunk interfaces:**

  ```
  no interface trunks { id } spanning-tree msti { mstp-id }
  ```

  Where:

  - `{ id }` is the ID given to the interface
  - `{ mstp-id }` is the ID for the Multiple Spanning Tree Instance

3. Type `commit` and press **Enter** to save the changes.

14.4.8 Viewing the Status of RSTP

To view the status of the RSTP network, type:

```
show switch spanning-tree rstp-status
```

A list similar to the following appears:

```
ruggedcom# show switch spanning-tree rstp-status
rstp-status
 status                   notDesignatedForAnyLAN
 bridge priority          32768
 bridge mac               00:0a:dc:f6:c6:ff
 root priority            32768
 root mac                 00:0a:dc:00:71:57
 regional root priority   32768
 regional root mac        00:0a:dc:f6:c6:ff
 root port slot           lm1
 root port port           1
 root path cost           38
 regional root path cost  0
 configured hello time    2
 learned hello time       2
 configured forward delay 15
 learned forward delay    15
 configured max age       20
 learned max age          20
 total top changes        5
```

This list provides the following information:

Parameter	Description
`status`	**Synopsis:** [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`	**Synopsis:** An integer The bridge identifier of this bridge.

Parameter	Description
bridge-mac	**Synopsis:** A string up to 17 characters long The bridge identifier of this bridge.
root-priority	**Synopsis:** An integer The priority value of the root bridge.
root-mac	**Synopsis:** A string up to 17 characters long The MAC address of the root bridge.
regional-root-priority	**Synopsis:** 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	**Synopsis:** 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	**Synopsis:** [--- | 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	**Synopsis:** 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	**Synopsis:** 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 configured. 1Gbps 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	**Synopsis:** 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	**Synopsis:** An integer The configured hello time from the Bridge RSTP Parameters menu.
learned-hello-time	**Synopsis:** An integer The actual hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.

Parameter	Description
configured-forward-delay	**Synopsis:** An integer The configured forward delay time from the Bridge RSTP Parameters menu.
learned-forward-delay	**Synopsis:** 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	**Synopsis:** An integer The configured maximum age time from the Bridge RSTP Parameters menu.
learned-max-age	**Synopsis:** 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-top-changes	**Synopsis:** 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.

14.4.9 Viewing RSTP Per-Port Statistics

To view Rapid Spanning Tree Protocol (RSTP) statistics for each port, type:

```
show switch spanning-tree port-rstp-stats
```

A table or list similar to the following example appears:

```
ruggedcom# show switch spanning-tree port-rstp-stats
port-rstp-stats lm1 1
 stp state            forwarding
 stp role             root
 cost                 19
 desg bridge priority 32768
 desg bridge mac      00:0a:dc:78:fc:40
 oper edge            false
 rx rsts              556
 tx rsts              3
 rx configs           0
 tx configs           0
 rx tcns              0
 tx tcns              0
```

The following information is provided:

Parameter	Description
`{ slot }`	**Synopsis:** [sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport | trnk] The slot of the module that contains this port.
`{ port }`	**Synopsis:** An integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
`stp-state`	**Synopsis:** [disabled | blocking | listening | learning | forwarding | linkDown | discarding] Describes the status of this interface in the spanning tree: • Disabled: Spanning Tree Protocol (STP) is disabled on this port. • Link Down: STP is enabled on this port but the link is down. • Discarding: The link is not used in the STP topology but is standing by. • Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • Forwarding : The port is forwarding traffic.
`stp-role`	**Synopsis:** [---- | root | designated | alternate | backup | master] The role of this port in the spanning tree: • Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to. • Root: The single port on the bridge, which provides connectivity towards the root bridge. • 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. • Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • 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 (MSTI) towards the Common Spanning Tree (CST) root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
`cost`	**Synopsis:** An integer The cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.

Parameter	Description
desg-bridge-priority	**Synopsis:** An integer between 0 and 65535 Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.
desg-bridge-mac	**Synopsis:** A string up to 17 characters long Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.
oper-edge	**Synopsis:** [true | false] Whether or not the port is operating as an edge port.
rx-rsts	**Synopsis:** An integer The number of Rapid Spanning Tree Protocol (RSTP) configuration messages received on this port.
tx-rsts	**Synopsis:** An integer The number of Rapid Spanning Tree Protocol (RSTP) configuration messages transmitted on this port.
rx-configs	**Synopsis:** An integer The number of Spanning Tree Protocol (STP) configuration messages received on this port.
tx-configs	**Synopsis:** An integer The number of Spanning Tree Protocol (STP) configuration messages transmitted on this port.
rx-tcns	**Synopsis:** An integer The number of configuration change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems.
tx-tcns	**Synopsis:** An integer The number of configuration messages transmitted from this port.

14.4.10 Clearing Spanning Tree Protocol Statistics

To clear all Spanning Tree Protocol statistics, type:

```
switch spanning-tree clear-stp-stats
```

14.5 Managing the Media Redundancy Protocol (MRP)

RUGGEDCOM ROX II supports the Media Redundancy Protocol (MRP), a network redundancy protocol for mission-critical applications.

14.5.1 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).

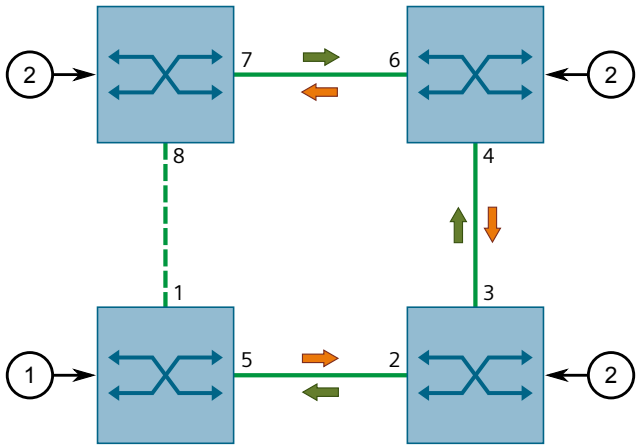
MRP is standardized by the International Electrotechnical Commission as IEC 62439-2.

14.5.1.1 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.



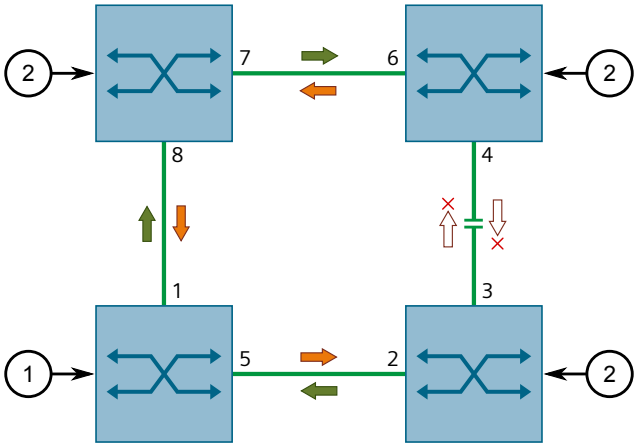
① MRM
② MRC

Figure 14.9 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 14.10 MRP Ring-Open State

Note

Frames will be lost when transitioning between ring states.

14.5.1.2 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.

14.5.1.3 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.

14.5.1.4 Requirements and Restrictions

Note the following requiremens 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.

14.5.2 Configuring MRP Globally

To configure the Media Redundancy Protocol globally, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » media-redundancy***.
3. Configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false Enables MRP globally.
`auto-generate-uuid { auto-generate-uuid }`	**Synopsis:** [true | false] **Default:** true Enables or disables the automatic generation of the MRP Universal Unique Identifier (UUID).

4. Type `commit` and press **Enter** to save the changes.

14.5.3 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 1043).

These traps can be enabled or disabled as needed.

To enable/disable these SNMP traps, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable SNMP traps for the desired MRP instance by typing one of the following commands:

   Enable

   ```
   switch media-redundancy mrp-instance { instance-id } ring-alarms
   ```

   Where { instance-id } is a number between 1 and 4.

   Disable

   ```
   no switch media-redundancy mrp-instance { instance-id } ring-alarms
   ```

   Where { instance-id } is a number between 1 and 4.
3. Type `commit` and press **Enter** to save the changes.

14.5.4 Viewing the List of MRP Instances

To view the status of MRP instances, type:

```
show running-config switch media-redundancy mrp-instance
```

If MRP instances have been configured, a table or list similar to the following example appears:

```
switch media-redundancy
 mrp-instance 1
  ring-ports primary-slot lm1
  ring-ports primary-port 5
  ring-ports secondary-slot lm1
  ring-ports secondary-port 6
 !
!
```

If no MRP instances have been configured, add them. For more information, refer to "Adding an MRP Instance" (Page 856).

14.5.5 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 335).

For more information about open and closed MRP rings, refer to "MRP Operation" (Page 852).

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 174).

1. Make sure the CLI is in Configuration mode.
2. Add the MRP instance by typing:

   ```
   switch media-redundancy mrp-instance { instance-id }
   ```

   Where { instance-id } is a number between 1 and 4.
3. Configure the following parameters to define the MRP instance:

Parameter	Description
`name { name }`	**Synopsis:** A string between 1 and 24 characters long **Default:** default-mrpdomain The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name.
`role { role }`	**Synopsis:** [Disabled | Client | Manager | ManagerAuto] **Default:** Client The role assigned to this MRP instance.

Parameter	Description
	• Disabled – No role is assigned. The MRP instance is disabled. • Client – The device operates as a Media Redundancy Client (MRC). • Manager – The device operates as a Media Redundancy Manager (MRM). • ManagerAuto – The MRP instance automatically determines the role of the device.
`priority { priority }`	**Synopsis:** A string up to 4 characters long **Default:** 8000 The priority assigned to the MRP instance. This is used when negotiating with other MRP devices to determine which is the MRP Manager. • 0000 - Highest priority (Manager) • 1000-7000 -High priority (Manager) • 8000 - Default priority (Manager) • 9000-E000 - Low priority (ManagerAuto) • F000 - Lowest priority (ManagerAuto)
`domain-id { domain-id }`	**Synopsis:** A string up to 32 characters long **Default:** FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF 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. If the Auto Generate UUID parameter is disabled, the domain ID can be modified.
`ring-alarms { ring-alarms }`	**Synopsis:** [true | false] **Default:** true 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.

4. Enter `ring-ports` and then configure the following parameters to select the primary and secondary ring ports:

Parameter	Description
`primary-slot { primary-slot }`	**Synopsis:** [sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport] MRP ring primary slot number.
`primary-port { primary-port }`	**Synopsis:** An integer between 1 and 16 MRP ring primary port number.

Parameter	Description
`secondary-slot { secondary-slot }`	**Synopsis:** [sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport] MRP ring secondary slot number.
`secondary-port { secondary-port }`	**Synopsis:** An integer between 1 and 16 MRP ring secondary port number.

5. Type `commit` and press **Enter** to save the changes.

14.5.6 Deleting an MRP Instance

To delete an MRP instance, do the following:

1. Make sure the CLI is in Configuration mode.
2. 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 128).
3. Delete the desired MRP instance by typing:

   ```
   no switch media-redundancy mrp-instance { instance-id }
   ```

   Where { instance-id } is a number between 1 and 4.
4. Type `commit` and press **Enter** to save the changes.

14.5.7 Viewing the Status of MRP Instances

To view the status of MRP instances, type:

```
show switch media-redundancy mrp-status
```

If MRP instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show switch media-redundancy mrp-status
mrp-status 1
 name            default-mrpdomain
 role            manager
 ring status     closed
 prm port        lm1-2
 prm port state  FORWARD
 sec port        lm1-5
 sec port state  BLOCKED
 multi mrm err   false
 one side rx err false
```

The following information is provided per instance:

Parameter	Description
`{ instance-id }`	**Synopsis:** An integer between 1 and 4 The Media Redundancy Protocol (MRP) instance
`name`	**Synopsis:** A string The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name.
`role`	**Synopsis:** [disable | client | manager | managerAuto] The role assigned to this MRP instance. • Disabled – No role is assigned. The MRP instance is disabled. • Client – The device operates as a Media Redundancy Client (MRC). • Manager – The device operates as a Media Redundancy Manager (MRM). • ManagerAuto – The MRP instance automatically determines the role of the device.
`ring-status`	**Synopsis:** [unknown | open | closed] The status of the MRP ring. • Unknown - The status of the ring is unknown. This is displayed when the device is an MRC • Open - The MRP ring is open. Both ring ports are forwarding packets. • Closed - The MRP ring is closed. One ring port is forwarding packets, while the other is blocking packets.
`prm-port`	**Synopsis:** A string The MRP primary port of the MRP ring port.
`prm-port-state`	**Synopsis:** [OFF | DOWN | BLOCKED | FORWARD | UNKNOWN] The status of the primary ring port. Possible values include: • OFF - MRP is not running • DOWN - The MRP ring port is down • BLOCKED - The MRP ring port is blocking packets • FORWARD - The MRP ring port is forwarding packets • UNKNOWN - The MRP ring port is Unknown
`sec-port`	**Synopsis:** A string The MRP secondary port of the MRP ring port.
`sec-port-state`	**Synopsis:** [OFF | DOWN | BLOCKED | FORWARD | UNKNOWN] The status of the secondary ring port. Possible values include: • OFF - MRP is not running • DOWN - The MRP ring port is down • BLOCKED - The MRP ring port is blocking packets

Parameter	Description
	• FORWARD - The MRP ring port is forwarding packets • UNKNOWN - The MRP ring port is Unknown
`multi-mrm-err`	**Synopsis:** [true | false] Error indicated by an MRM when more than one MRM are active in the MRP ring.
`one-side-rx-err`	**Synopsis:** [true | false] Error indicated by an MRM when the test frames of an MRM has been seen, but only on one ring port.

If no MRP instances have been configured, add them. For more information, refer to "Adding an MRP Instance" (Page 856).

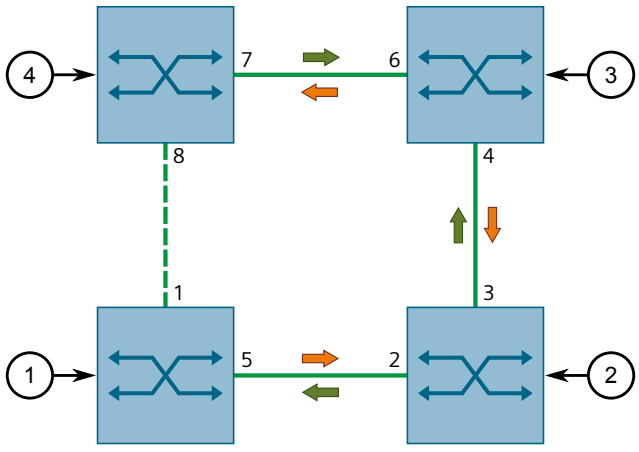
14.5.8 Example: Configuring an MRP Ring

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.



① MRM
② MRC 1
③ MRC 2
④ MRC 3

Figure 14.11 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 833).

   For more information about disabling RSTP per port, refer to "Configuring a Switched Ethernet Port" (Page 335).

2. Enable MRP on the MRM and all MRCs.

   For more information, refer to "Configuring MRP Globally" (Page 854).

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 856).

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 856).

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 856).

15 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.

15.1 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 802.1AB 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.

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

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.

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.

15.1.1 Configuring LLDP

To configure the Link Layer Discovery Protocol (LLDP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » net-discovery » lldp*** and configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables LLDP, making the device an LLDP agent.
`tx-interval { tx-interval }`	**Synopsis:** An integer between 5 and 32768 **Default:** 30 The time in seconds (s) between each subsequent transmission of an LLDP frame.
`tx-hold { tx-hold }`	**Synopsis:** An integer between 2 and 10 **Default:** 4 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. The TTL value is equal to the value of the **Transmission Hold (tx-hold)** parameter multiplied by the value of the **Transmission Interval (tx-interval)** parameter.
`reinit-delay { reinit-delay }`	**Synopsis:** An integer between 1 and 10 **Default:** 2 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.

Parameter	Description
`tx-delay { tx-delay }`	**Synopsis:** An integer between 1 and 8192 **Default:** 2 The time in seconds (s) the LLDP agent will wait before transmitting a new LLDP frame after the configuration of the device is changed. The value of the **Transmission Delay (tx-parameter)** should be no more than one quarter of the value of the **Transmission Interval (tx-interval)** parameter.
`notification-interval { notification-interval }`	**Synopsis:** An integer between 5 and 3600 **Default:** 5 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.

3. Type `commit` and press **Enter** to save the changes.

15.1.2 Viewing Global Statistics

To view global statistics for LLDP, type:

```
show switch net-discovery lldp global-statistics
```

A table or list similar to the following appears:

```
ruggedcom# show switch net-discovery lldp global-statistics
global-statistics
 inserts          21
 deletes          20
 drops            0
 ageouts          8
 last change time 3D14m19s
```

The table or list displays the following information:

Parameter	Description
`inserts`	**Synopsis:** An integer between 0 and 4294967295 The total number of new hosts added to the LLDP Neighbor Information Table.
`deletes`	**Synopsis:** An integer between 0 and 4294967295 The total number of hosts deleted from the LLDP Neighbor Information Table.
`drops`	**Synopsis:** An integer between 0 and 4294967295 The total number of hosts detected that could not be added to the LLDP Neighbor Information Table.

Parameter	Description
ageouts	**Synopsis:** An integer between 0 and 4294967295 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.
last-change-time	**Synopsis:** A string 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 8601 format (e.g. P1Y1M2W3DT2H3M30S represents 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30 seconds).

15.1.3 Viewing Global Statistics and Advertised System Information

To view the system information that is advertised to neighbors, type:

```
show switch net-discovery lldp local-system
```

A table or list similar to the following appears:

```
ruggedcom#  show switch net-discovery lldp local-system
local-system
 local chassis subtype     macAddress
 local chassis id          00:0a:dc:ff:9a:00
 local system name         R12.localdomain
 local system desc         RX5000-R-MNT-HI-HI-SM61-CM01-L3SEC-16TX01-XX-XX-
XX-4FG50-XX
 local system caps         bridge,router
 local system caps enabled bridge,router
```

The table or list displays the following information:

Parameter	Description
local-chassis-subtype	**Synopsis:** [chassisComponent | interfaceAlias | portComponent | macAddress | networkAddress | interfaceName | local] The source of the **Local Chassis ID (local-chassis-id)** parameter. Options include: • chassisComponent - The **Local Chassis ID (local-chassis-id)** corresponds with the alias for a chassis component (entPhysicalAlias) in the ENTITY-MIB file • interfaceAlias - The **Local Chassis ID (local-chassis-id)** corresponds with the alias for an interface (ifAlias) in the IF-MIB file • portComponent - The **Local Chassis ID (local-chassis-id)** corresponds with the alias for a port or backplane component (entPhysicalAlias) in the ENTITY-MIB file • macAddress - The **Local Chassis ID (local-chassis-id)** is a MAC address associated with the device • networkAddress - The **Local Chassis ID (local-chassis-id)** is an IP address associated with the device

Parameter	Description
	• interfaceName - The **Local Chassis ID (local-chassis-id)** corresponds with the default name for an interface (ifName) in the IF-MIB file • local - The **Local Chassis ID (local-chassis-id)** is a locally defined value
`local-chassis-id`	**Synopsis:** A string up to 17 characters long The type-length-value (TLV) used to identify the device to LLDP neighbors. The value of the **Local Chassis ID (local-chassis-id)** parameter is categorized by the **Local Chassis Subtype (local-chassis-subtype)** parameter.
`local-system-name`	**Synopsis:** A string up to 255 characters long An administratively assigned name, often the fully qualified domain name (FQDN), for the device. The **Local System Name (local-system-name)** parameter corresponds with the sysName object in the SNMPv2-MIB.
`local-system-desc`	**Synopsis:** A string up to 255 characters long The default system description of the device, which includes the full name and version ID of its hardware, operating system, and networking software. The **Local System Description (local-system-desc)** parameter corresponds with the sysDescr object in the SNMPv2-MIB.
`local-system-caps`	**Synopsis:** [other | repeater | bridge | wlanAccessPoint | router | telephone | docsisCableDevice | stationOnly] The network functions the device can serve. Options include: • other - The device can serve other, unspecified functions • repeater - The device can receive and regenerate IP packets within a single network • bridge - The device can join two or more networks into a single network • wlanAccessPoint - The device can forward network traffic to/from a WLAN • router - The device can forward IP packets from one wired network to another • telephone - The device can forward IP packets to/from a telephone network • docsisCableDevice - The device can forward IP packets to a Cable TV system • stationOnly - The device can only receive network traffic
`local-system-caps-enabled`	**Synopsis:** [other | repeater | bridge | wlanAccessPoint | router | telephone | docsisCableDevice | stationOnly] The network functions the device currently serves. Options include: • other - The device serves other, unspecified functions

Parameter	Description
	• repeater - The device receives and regenerates IP packets within a single network • bridge - The device joins two or more networks into a single network • wlanAccessPoint - The device forwards network traffic to/from a WLAN • router - The device forwards IP packets from one wired network to another • telephone - The device forwards IP packets to/from a telephone network • docsisCableDevice - The device forwards IP packets to a Cable TV system • stationOnly - The device only receives network traffic

15.1.4 Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, type:

```
show switch net-discovery lldp port-lldp-neighbors
```

A table or list similar to the following appears:

```
ruggedcom# show switch net-discovery lldp port-lldp-neighbors
port-lldp-neighbors lm1 1
 chassis id              ""
 port id                 ""
 system name             ""
 system desc             ""
 port desc               ""
 man address             ""
 man address if id       0
 system caps             ""
 system caps enabled     ""
 chassis subtype         macAddress
 port subtype            interfaceName
 man address subtype     other
 man address if subtype unknown
 last update             0s
```

The table or list displays the following information:

Parameter	Description
`chassis-id`	**Synopsis:** A string up to 17 characters long The type-length-value (TLV) used to identify the LLDP neighbor. The value of the **Chassis ID (chassis-id)** parameter is categorized by the **Chassis Subtype (chassis-subtype)** parameter.
`port-id`	**Synopsis:** A string up to 17 characters long The remote port from which the LLDP neighbor sends LLDP frames to the device.

Parameter	Description
	The value of the **Port ID (port-id)** parameter is categorized by the **Port Subtype (port-subtype)** parameter.
`system-name`	**Synopsis:** A string up to 255 characters long An administratively assigned name, often the fully qualified domain name (FQDN), for the LLDP neighbor. The **System Name (system-name)** parameter corresponds with the sysName object in the SNMPv2-MIB associated with the LLDP neighbor.
`system-desc`	**Synopsis:** A string up to 255 characters long The default system description of the LLDP neighbor, which includes the full name and version ID of its hardware, operating system, and networking software. The **System Description (system-desc)** parameter corresponds with the sysDescr object in the SNMPv2-MIB associated with the LLDP neighbor.
`port-desc`	**Synopsis:** A string up to 255 characters long 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. The **Port Description (port-desc)** parameter corresponds with the ifDescr object in the IF-MIB associated with the LLDP neighbor.
`man-address`	**Synopsis:** A string up to 31 characters long An address associated with the LLDP neighbor that can be used to access information about the neighbor host. The value of the **Management Address (man-address)** parameter is categorized by the **Management Address Subtype (man-address-subtype)** parameter.
`man-address-if-id`	**Synopsis:** An integer The interface with which the **Management Address (man-address)** of the LLDP neighbor is associated. The value of the **Management Address Interface ID (man-address-if-id)** parameter is categorized by the **Management Address Interface Subtype (man-address-if-subtype)** parameter.
`system-caps`	**Synopsis:** [other | repeater | bridge | wlanAccessPoint | router | telephone | docsisCableDevice | stationOnly] The network functions the LLDP neighbor can serve. Possible values include: • other - The neighbor host can serve other, unspecified functions • repeater - The neighbor host can receive and regenerate IP packets within a single network • bridge - The neighbor host can join two or more networks into a single network • wlanAccessPoint - The neighbor host can forward network traffic to/from a WLAN

Parameter	Description
	• router - The neighbor host can forward IP packets from one wired network to another • telephone - The neighbor host can forward IP packets to/from a telephone network • docsisCableDevice - The neighbor host can forward IP packets to a Cable TV system • stationOnly - The neighbor host can only receive network traffic The network functions that the LLDP neighbor currently serves are specified by the **System Capabilities Enabled (system-caps-enabled)** parameter.
`system-caps-enabled`	**Synopsis:** [other | repeater | bridge | wlanAccessPoint | router | telephone | docsisCableDevice | stationOnly] The network functions that the LLDP neighbor currently serves. Possible values include: • other - The neighbor host serves other, unspecified functions • repeater - The neighbor host receives and regenerates IP packets within a single network • bridge - The neighbor host joins two or more networks into a single network • wlanAccessPoint - The neighbor host forwards network traffic to/from a WLAN • router - The neighbor host forwards IP packets from one wired network to another • telephone - The neighbor host forwards IP packets to/from a telephone network • docsisCableDevice - The neighbor host forwards IP packets to a Cable TV system • stationOnly - The neighbor host only receives network traffic 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 **System Capabilities (system-caps)** parameter.
`chassis-subtype`	**Synopsis:** [chassisComponent | interfaceAlias | portComponent | macAddress | networkAddress | interfaceName | local] The source of the **Chassis ID (chassis-id)** parameter as advertised by LLDP neighbor. Possible values include: • chassisComponent - The **Chassis ID (chassis-id)** corresponds with the alias for a chassis component (entPhysicalAlias) in the ENTITY-MIB file • interfaceAlias - The **Chassis ID (chassis-id)** corresponds with the alias for an interface (ifAlias) in the IF-MIB file • portComponent - The **Chassis ID (chassis-id)** corresponds with the alias for a port or backplane component (entPhysicalAlias) in the ENTITY-MIB file • macAddress - The **Chassis ID (chassis-id)** is a MAC address associated with the LLDP neighbor • networkAddress - The **Chassis ID (chassis-id)** is an IP address associated with the LLDP neighbor

Parameter	Description
	• interfaceName - The **Chassis ID (chassis-id)** corresponds with the default name for an interface (ifName) in the IF-MIB file • local - The **Chassis ID (chassis-id)** is a value defined locally by the LLDP neighbor
`port-subtype`	**Synopsis:** [interfaceAlias | portComponent | macAddress | networkAddress | interfaceName | agentCircuitId | local] The source of the **Port ID (port-id)** parameter as advertised by LLDP neighbor. Possible values include: • interfaceAlias - The **Port ID (port-id)** corresponds with the alias for an interface (ifAlias) in the IF-MIB file • portComponent - The **Port ID (port-id)** corresponds with the alias for a port component (entPhysicalAlias) in the ENTITY-MIB file • macAddress - The **Port ID (port-id)** is a MAC address associated with a remote port • networkAddress - The **Port ID (port-id)** is an IP address associated with a remote port • interfaceName - The **Port ID (port-id)** corresponds with the default name for a port (ifName) in the IF-MIB file • agentCircuitId - The **Port ID (port-id)** corresponds with the Circuit ID for a port as defined by the DHCP agent • local - The **Port ID (port-id)** is a value defined locally by the LLDP neighbor
`man-address-subtype`	**Synopsis:** [other | ipV4 | ipV6 | nsap | hdlc | bbn1822 | all802 | e163 | e164 | f69 | x121 | ipx | appleTalk | decnetIV | banyanVines | e164withNsap | dns | distinguishedName | asNumber | xtpOverIpv4 | xtpOverIpv6 | xtpNativeModeXTP | fibreChannelWWPN | fibreChannelWWNN | gwid | afi | reserved] The source of the **Management Address (man-address)** parameter as advertised by LLDP neighbor. Possible values include: • other - The **Management Address (man-address)** is another, unspecified type of address • ipv4 - The **Management Address (man-address)** is an IPv4 address • ipv6 - The **Management Address (man-address)** is an IPv6 address • nsap - The **Management Address (man-address)** is an Network Service Access Point (NSAP) address • hdlc - The **Management Address (man-address)** is a High-level Link Control (HDLC) address • bbn1822 - The **Management Address (man-address)** is a numeric host address to be used in IMP-host exchanges • all802 - The **Management Address (man-address)** is an IEEE 802 address • e163 - The **Management Address (man-address)** is an E.163 telephone number • e164 - The **Management Address (man-address)** is an E.164 telephone number

Parameter	Description
	• f69 - The **Management Address (man-address)** is an F.69 telex number • x121 - The **Management Address (man-address)** is an X.121 address • ipx - The **Management Address (man-address)** is an IPX address • appleTalk - The **Management Address (man-address)** is an AppleTalk address • decnetIV - The **Management Address (man-address)** is a DECnet Phase IV address • banyanVines - The **Management Address (man-address)** is a VINES network address • e164withNsap - The **Management Address (man-address)** is a Network Service Access Point (NSAP)-encoded E.164 telephone number • dns - The **Management Address (man-address)** is a Domain Name Server (DNS) server • distinguishedName - The **Management Address (man-address)** is a Distinguished Name (DN) address • asNumber - The **Management Address (man-address)** is an Autonomous System Number (ASN) • xtpOverIpv4 - The **Management Address (man-address)** is an IPv4 address that uses Xpress Transport Protocol (XTP) instead of TCP • xtpOverIpv6 - The **Management Address (man-address)** is an IPv6 address that uses Xpress Transport Protocol (XTP) instead of TCP • xtpNativeModeXTP - The **Management Address (man-address)** is an Xpress Transport Protocol (XTP) address segment • fibreChannelWWPN - The **Management Address (man-address)** is an World Wide Port Name (WWPN) • fibreChannelWWNN - The **Management Address (man-address)** is an World Wide Node Name (WWNN) • gwid - The **Management Address (man-address)** is a Gateway Identifier (GWID) • afi - The **Management Address (man-address)** is an Authority and Format Identifier (AFI) • reserved - The **Management Address (man-address)** is a reserved IPv4 or IPv6 address
`man-address-if-subtype`	**Synopsis:** [unknown | ifIndex | systemPortNumber] The source of the **Management Address Interface ID (man-address-if-id)** parameter as advertised by the LLDP neighbor. Possible values include: • unknown - The **Management Address Interface ID (man-address-if-id)** is not known • ifIndex - The **Management Address Interface ID (man-address-if-id)** corresponds with the indexed name for an interface (ifIndex) in the IF-MIB file

Parameter	Description
	• systemPortNumber - The **Management Address Interface ID (man-address-if-id)** corresponds with a locally defined port number
`last-update`	**Synopsis:** A string 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).

15.1.5 Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, type:

```
show switch net-discovery lldp port-lldp-stats
```

A table or list similar to the following appears:

```
ruggedcom# show switch net-discovery lldp port-lldp-stats
             FRM  ERR  FRM   FRM            TLVS  TLVS
SLOT  PORT   DRP  FRM  IN    OUT   AGEOUTS  DROP  UNKNOWN
-------------------------------------------------------------
lm1   1      0    0    0     0     0        0     0
lm1   2      0    0    8583  8577  8        0     0
lm1   3      0    0    0     0     0        0     0
lm1   4      0    0    0     0     0        0     0
lm1   5      0    0    0     0     0        0     0
lm1   6      0    0    0     0     0        0     0
lm1   7      0    0    0     0     0        0     0
lm1   8      0    0    8934  8934  0        0     0
lm1   9      0    0    0     0     0        0     0
lm1   10     0    0    0     0     0        0     0
lm1   11     0    0    0     0     0        0     0
lm1   12     0    0    0     0     0        0     0
lm1   13     0    0    0     0     0        0     0
lm1   14     0    0    0     0     0        0     0
lm1   15     0    0    0     0     0        0     0
lm1   16     0    0    0     0     0        0     0
lm5   1      0    0    0     0     0        0     0
lm5   2      0    0    0     0     0        0     0
lm5   3      0    0    0     0     0        0     0
lm5   4      0    0    0     0     0        0     0
cm    1      0    0    8915  8900  0        0     0
```

The table or list displays the following information:

Parameter	Description
`{ slot }`	**Synopsis:** [--- | pm1 | pm2 | main | sm | lm1 | lm2 | lm3 | lm4 | lm5 | lm6 | swport | eth | serport | celport | wlanport | cm | em | trnk] The slot number of the module that contains the port specified by the **Port (port)** parameter.

Parameter	Description
`{ port }`	**Synopsis:** An integer between 1 and 16 The port number as indicated on the front plate silkscreen of the module. The port is contained in the slot module specified by the **Slot (slot)** parameter.
`frm-drp`	**Synopsis:** An integer between 0 and 4294967295 The total number of incoming LLDP frames dropped by the port.
`err-frm`	**Synopsis:** An integer between 0 and 4294967295 The total number of incoming LLDP frames received on the port with detectable errors.
`frm-in`	**Synopsis:** An integer between 0 and 4294967295 The total number of incoming LLDP frames received on the port.
`frm-out`	**Synopsis:** An integer between 0 and 4294967295 The total number of outgoing LLDP frames broadcast on the port.
`ageouts`	**Synopsis:** 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-drop`	**Synopsis:** An integer between 0 and 4294967295 The total number of TLVs discarded from LLDP frames received on the port.
`tlvs-unknown`	**Synopsis:** An integer between 0 and 4294967295 The total number of unrecognized TLVs in LLDP frames received on the port.

15.2 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 973).

For a list of supported SNMP traps, refer to "Standard SNMP Traps" (Page 1041) and "Proprietary SNMP Traps" (Page 1043).

15.2.1 Enabling and Configuring SNMP Sessions

To enable and configure SNMP sessions, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » snmp*** and configure the following parameter(s) as required:

⚠ NOTICE

To generate all SNMP traffic for a specific interface, make sure the IP address for the desired interface is set for both the **Listen IP** and **Source IP for Traps** parameters.

⚠ NOTICE

The **auth-failure-trap-notify** parameter is used to notify users of authentication failures when the **authen-traps-enabled** is enabled. For more information about SNMP notifications, refer to "Standard SNMP Traps" (Page 1041) and "Proprietary SNMP Traps" (Page 1043).

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false Enables SNMP, making the device an SNMP agent.
`listen-ip { listen-ip }`	**Synopsis:** A string **Default:** 0.0.0.0 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.
`port { port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 161 The default port on which the SNMP agent will listen for SNMP requests. The port corresponds with the IP address specified by the **Listen IP (listen-ip)** parameter.
`extra-ip-ports { extra-ip-ports }`	**Synopsis:** A string 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). If the **Listen IP (listen-ip)** parameter is set to a value other than 0.0.0.0, the port specified by the **Listen Port (port** parameter must not be associated with any additional addresses.
`max-sessions { max-sessions }`	**Synopsis:** An integer **Default:** 30 The maximum number of concurrent SNMP sessions.
`snmp-engine-id { snmp-engine-id }`	**Synopsis:** A string 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. The value of **Local SNMP Engine ID (snmp-engine-id).** must correspond with the value of **User SNMP Engine ID (id)**.
`source-ip { source-ip }`	**Synopsis:** A string The source IP address for all notifications sent from the SNMP agent. The address may or may not belong to the device.
`auth-failure-trap-notify { auth-failure-trap-notify }`	**Synopsis:** [none | snmpv1_trap | snmpv2_trap | snmpv2_inform | snmpv3_trap | snmpv3_inform] **Default:** none The security model and notification type of the authenticationFailure notification, which the agent sends out when authentication fails. Options include:

Parameter	Description
	• none - The authenticationFailure notification is delivered to all management targets • snmpv1_trap - The authenticationFailure notification is delivered to management targets configured to receive SNMPv1 trap notifications • snmpv2_trap - The authenticationFailure notification is delivered to management targets configured to receive SNMPv2 trap notifications • snmpv2_inform - The authenticationFailure notification is delivered to management targets configured to receive SNMPv2 **inform** notifications • snmpv3_trap - The authenticationFailure notification is delivered to management targets configured to receive SNMPv3 **trap** notifications • snmpv3_inform - The authenticationFailure notification is delivered to management targets configured to receive SNMPv3 **inform** notifications
`authen-traps-enabled { authen-traps-enabled }`	**Synopsis:** [true | false] **Default:** false Enables/disables the SNMP to send generic authentication traps.
`rox-authentication-trap-enabled { rox-authentication-trap-enabled }`	**Synopsis:** [true | false] **Default:** false Enables/disables the SNMP to send detailed traps related to user authentication and password management.
`dscp { dscp }`	**Synopsis:** An integer between 0 and 63 **Default:** 0 The priority level for traffic sent by the SNMP agent. Values must correspond with Differentiated Services Code Points (DSCPs), as described in RFC 2475.

3. Type `commit` and press **Enter** to save the changes.

15.2.2 Viewing Statistics for SNMP

To view the statistics collected for SNMP, type:

```
show admin snmp statistics
```

If statistics are available, a table or list similar to the following example appears:

```
ruggedcom# show admin snmp statistics
statistics
 unsupported sec levels 1
 not in time windows    1
 unknown user names     1
 unknown engine ids     4
 wrong digests          1
```

```
  decryption errors      1
```

The table or list provides the following information:

Parameter	Description
unsupported-sec-levels	**Synopsis:** An integer The total number of incoming SNMP packets dropped because they requested an unknown or unavailable security level.
not-in-time-windows	**Synopsis:** An integer The total number of incoming SNMP packets dropped because they were received after the authoritative SNMP engine's time out period expired.
unknown-user-names	**Synopsis:** An integer The total number of incoming SNMP packets dropped because they referenced an unknown user.
unknown-engine-ids	**Synopsis:** An integer The total number of incoming SNMP packets dropped because they referenced an unknown SNMP Engine ID.
wrong-digests	**Synopsis:** An integer The total number of incoming SNMP packets dropped because they contained an unexpected digest value (i.e. authentication key).
decryption-errors	**Synopsis:** An integer The total number of incoming SNMP packets dropped because they could not be decrypted.

15.2.3 Discovering SNMP Engine IDs

To discover an ID of a remote SNMP protocol engine, do the following:

1. At the prompt, type the following command:

   ```
   admin snmp snmp-discover
   ```

2. When prompted, type the IP address of the remote SNMP protocol engine.

   ```
   ruggedcom# admin snmp snmp-discover
   Value for 'address' (<string, min: 7 chars, max: 15 chars>): { ip-address }
   ```

Once discovered, the ID is displayed. For example:

```
snmp-discover-return-string 80:00:3A:9C:03:94:B8:C5:FF:F6:00
```

15.2.4 Managing SNMP Communities

This section describes how to manage SNMP communities.

15.2.4.1 Viewing a List of SNMP Communities

To view a list of SNMP communities configured on the device, type:

```
show running-config admin snmp snmp-community { name }
```

If communities have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin snmp snmp-community | tab
COMMUNITY  USER
NAME       NAME
------------------
private    oper
public     guest

 !
!
```

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 879).

15.2.4.2 Adding an SNMP Community

To add an SNMP community, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP community by typing:

   ```
   admin snmp snmp-community { name }
   ```

   Where:

   - `{ name }` is the name of the community
3. Configure the following parameter(s) as required:

Parameter	Description
`user-name { user-name }`	**Synopsis:** A string between 1 and 128 characters long The user name associated with the community string.

4. Type `commit` and press **Enter** to save the changes.

15.2.4.3 Deleting an SNMP Community

To delete an SNMP community, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP community by typing:

   ```
   no admin snmp snmp-community { name }
   ```

   Where:

   - `{ name }` is the name of the community
3. Type `commit` and press **Enter** to save the changes.

15.2.5 Managing SNMP Target Addresses

This section describes how to manage SNMP target addresses.

15.2.5.1 Viewing a List of SNMP Target Addresses

To view a list of SNMP target addresses configured on the device, type:

```
show running-config admin snmp snmp-target-address
```

If target addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin snmp snmp-target-address | tab
                              TARGET         TRAP  SECURITY  USER   SECURITY
TARGET NAME          ENABLED  ADDRESS        PORT  MODEL     NAME   LEVEL
-------------------------------------------------------------------------------
127.0.0.1 v1         true     127.0.0.1      162   v1        oper   noAuthNoPriv
127.0.0.1 v2         true     127.0.0.1      162   v2c       oper   noAuthNoPriv
127.0.0.1 v3.guest   true     127.0.0.1      162   v3        admin  noAuthNoPriv
127.0.0.1 v3.inform  true     127.0.0.1      162   v3        admin  authPriv
127.0.0.1 v3.trap    true     127.0.0.1      162   v3        admin  authNoPriv
target               true     192.168.0.111  162   v2c       admin  noAuthNoPriv

 !
!
```

If no SNMP target addresses have been configured, add target addresses as needed. For more information, refer to "Adding an SNMP Target Address" (Page 880).

15.2.5.2 Adding an SNMP Target Address

To add an SNMP target address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » snmp » snmp-target-address*** and configure the following parameter(s) as required:

Parameter	Description
`{ target-name }`	**Synopsis:** A string between 1 and 32 characters long The unique name for the SNMP target.
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables/disables the SNMP agent to send traps to the SNMP target.
`target-address { target-address }`	**Synopsis:** A string The IPv4 or IPv6 address for the SNMP target.
`trap-port { trap-port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 162 The UDP port on which the target will receive notifications. The trap port corresponds with the IP address specified by **Target Address (target-address).**
`security-model { security-model }`	**Synopsis:** [v1 | v2c | v3] **Default:** v2c The recognized security model of SNMP packets sent from the target. Options include: • snmpv1 - Packets sent from the target use the SNMPv1 community-based security model. • snmpv2c - Packets sent from the target use the SNMPv2c community-based security model • snmpv3 - Packets sent from the target use the SNMPv3 user-based security model
`user-name { user-name }`	**Synopsis:** A string between 1 and 128 characters long The recognized user name. Only this user name is permitted to exchange SNMP packets with the target.
`security-level { security-level }`	**Synopsis:** [noAuthNoPriv | authNoPriv | authPriv] **Default:** noAuthNoPriv The security level of SNMPv3 packets sent to or from the target. Options include: • authPriv - Users must be authenticated with a password in order to receive SNMPv3 packets sent from the target • authNoPriv - Users must be authenticated in order to receive SNMPv3 packets sent from the target. No password is required. • noAuthnoPriv - Users do not need to be authenticated to receive SNMPv3 packets sent from the target. No password is required. **Security Model (security-model)** must be set to **snmpv3**.

Parameter	Description
`control-community { control-community }`	**Synopsis:** A string between 1 and 32 characters long Incoming SNMP requests from the specified community will be blocked. Values must correspond with preconfigured SNMPv1/v2c community names.
`tag-list { tag-list }`	**Synopsis:** [snmpv1_trap | snmpv2_trap | snmpv2_inform | snmpv3_trap | snmpv3_inform] **Default:** snmpv2_trap The types of notifications the target may receive. Options include: • snmpv1_trap - The target will receive **trap** notifications from SNMPv1 agents • snmpv2_trap - The target will receive **trap** notifications from SNMPv2c agents • snmpv2_inform - The target will receive and acknowledge **inform** notifications from SNMPv2c agents • snmpv3_trap - The target will receive **trap** notifications from SNMPv3 agents • snmpv3_inform - The target will receive and acknowledge **inform** notifications from SNMPv3 agents **Note** Multiple options can be selected.
`inform-timeout { inform-timeout }`	**Synopsis:** An integer between 0 and 2147483647 **Default:** 6000 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. The maximum number of attempts is defined by **Maximum Retries (inform-retries)**.
`inform-retries { inform-retries }`	**Synopsis:** An integer between 0 and 255 **Default:** 3 The maximum number of times the agent will resend an unacknowledged inform notification. After this value is exceeded the SNMP session fails.
`target-engine-id { target-engine-id }`	**Synopsis:** A string 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.

3. Type `commit` and press **Enter** to save the changes.

15.2.5.3 Deleting an SNMP Target Address

To delete an SNMP target address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP target address by typing:

   ```
   no admin snmp snmp-target-address { target-name }
   ```

   Where:

   - `{ target-name }` is a descriptive name for the target (e.g. *Corporate NMS*)
3. Type `commit` and press **Enter** to save the changes.

15.2.6 Managing SNMP Users

This section describes how to manage SNMP users.

15.2.6.1 Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, type:

```
show running-config admin snmp snmp-user
```

If users have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin snmp snmp-user | tab
                                  USER   AUTH
USER ENGINE ID                    NAME   PROTOCOL  AUTH KEY
------------------------------------------------------------------------------
80:00:3a:9c:03:00:0a:dc:ff:9a:00  oper   sha1      $4$kNxlPIYMx2xJhYYI0d4IDw==
80:00:3a:9c:03:00:0a:dc:ff:9a:00  admin  none      -
80:00:3a:9c:03:00:0a:dc:ff:9a:00  guest  md5       $4$kNxlPIYMx2xJhYYI0d4IDw==

 !
!
```

If no SNMP users have been configured, add users as needed. For more information, refer to "Adding an SNMP User" (Page 883).

15.2.6.2 Adding an SNMP User

To add an SNMP user, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP user by typing:

   ```
   admin snmp snmp-user { id } { name }
   ```

   Where:

- `{ id }` is the ID for the user
- `{ name }` is the name of the user

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

Use only strong passwords when configuring SNMP users that consist of at least:

- One lower case character
- One upper case character
- One number
- One special character (i.e. !@#$%^&*()_+-={}[];:',<.>/?\|`~)

Avoid weak passwords (e.g. *password1*, *123456789*, *abcdefgh*) or repeated characters (e.g. *abcabc*).

3. Configure the following parameter(s) as required:

Parameter	Description
`auth-protocol { auth-protocol }`	**Synopsis:** [none | md5 | sha1] **Default:** none The authentication method used for exchanges between the user and the SNMP engine. Options include: • none - Exchanges are not authenticated • md5 - The server uses the MD5 algorithm to authenticate exchanges • sha1 - The server uses the SHA-1 hash function to authenticate exchanges When md5 or sha1 is selected, **Authentication Key (auth-key)** must be defined.
`auth-key { auth-key }`	**Synopsis:** A string at least 8 characters long The passphrase required to authenticate messages from the SNMP engine. The passphrase must be at least 8 characters long. **Authentication Protocol (auth-protocol)** must be set to either md5 or sha1.
`privacy-protocol { privacy-protocol }`	**Synopsis:** [none | des3cbc | aescfb128] **Default:** none The data encryption and decryption method for exchanges between the user and the SNMP engine. Options include: • none - Exchanges are not encrypted and decrypted • des3cbc - The server uses the 3DES-CBC algorithm to encrypt and decrypt exchanges • aescfb128 - The server uses the AES-CFB algorithm to encrypt and decrypt exchanges

Parameter	Description
	When des3cbc or aescfb128 is selected, **Privacy Key (privacy-key)** must be defined.
`privacy-key { privacy-key }`	**Synopsis:** A string The privacy passphrase required to encrypt message to and decrypt messages from the SNMP engine. The passphrase must be at least 8 characters long. **Privacy Protocol (privacy-protocol)** must be set to either des3cbc or aescfb128.

4. Type `commit` and press **Enter** to save the changes.

15.2.6.3 Deleting an SNMP User

To delete an SNMP user, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP user by typing:

   ```
   no admin snmp snmp-user { id } { name }
   ```

   Where:

   - `{ id }` is the ID for the user
   - `{ name }` is the name of the user
3. Type `commit` and press **Enter** to save the changes.

15.2.7 Managing SNMP Security Model Mapping

This section describes how to manage the mapping of SNMP security models.

15.2.7.1 Viewing a List of SNMP Security Models

To view a list of SNMP security models configured on the device, type:

```
show running-config admin snmp snmp-security-to-group
```

If target addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin snmp snmp-security-to-group | tab
SECURITY  USER
MODEL     NAME   GROUP
-----------------------------
v1        oper   all-rights
v1        guest  all-rights
v2c       oper   all-rights
v2c       admin  testgroup
```

```
v2c       guest  all-rights
v3        admin  initial

 !
!
```

If no SNMP security models have been configured, add security models as needed. For more information, refer to "Adding an SNMP Security Model" (Page 886).

15.2.7.2 Adding an SNMP Security Model

To add an SNMP security model, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP security model by typing:

   ```
   admin snmp snmp-security-to-group { model } { name }
   { group | { group } }
   ```

   Where:

   - `{ model }` is the security model. Options include **range**, **v1**, **v2c** and **v3**.
   - `{ name }` is the name of the associated user profile. Options include **admin**, **guest** and **oper**.
   - `{ group }` is the name of the associated SNMP group. If a group is not defined, the user is granted all access rights by default.
3. Type `commit` and press **Enter** to save the changes.

15.2.7.3 Deleting an SNMP Security Model

To delete an SNMP security model, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP security model by typing:

   ```
   no admin snmp snmp-security-to-group { model } { name }
   ```

   Where:

   - `{ model }` is the security model
   - `{ name }` is the name of the associated user profile
3. Type `commit` and press **Enter** to save the changes.

15.2.8 Managing SNMP Group Access

This section describes how to manage access for SNMP groups.

15.2.8.1 Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, type:

```
show running-config admin snmp snmp-access
```

If groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config admin snmp snmp-access | tab
            SECURITY  SECURITY      READ VIEW   WRITE VIEW  NOTIFY
GROUP       MODEL     LEVEL         NAME        NAME        VIEW NAME
-------------------------------------------------------------------------
initial     any       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib
initial     any       authNoPriv    all-of-mib  all-of-mib  all-of-mib
initial     any       authPriv      all-of-mib  all-of-mib  all-of-mib
testgroup   v2c       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib
all-rights  any       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib

 !
!
```

If no SNMP groups have been configured, add groups as needed. For more information, refer to "Adding an SNMP Group" (Page 887).

15.2.8.2 Adding an SNMP Group

To add an SNMP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP group by typing:

   ```
   admin snmp snmp-access { group } { model } { level }
   ```

   Where:

   - `{ group }` is the name of the group.
   - `{ model }` is the security model for the group. Options include: **any**, **v1**, **v2c**, or **v3**.
   - `{ level }` is the security level for the group. Options include:
     - **authPriv** – Communication with authentication and privacy.
     - **authNoPriv** – Communication with authentication and without privacy.
     - **noAuthnoPriv** – Communication without authentication and privacy.
3. Configure the following parameter(s) as required:

Parameter	Description
`read-view-name { read-view-name }`	**Synopsis:** [no-view | v1-mib | restricted | all-of-mib] **Default:** all-of-mib The read view to which members of the SNMP group have access. Options include: • all-of-mib - Group members can view all objects in the MIB

Parameter	Description
	• restricted - Group members can view only the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtrees in the MIB • v1-mib - Group members can view only SNMPv1 objects in the MIB • no-view - Group members cannot view any object in the MIB
`write-view-name { write-view-name }`	**Synopsis:** [no-view | v1-mib | restricted | all-of-mib] **Default:** all-of-mib The write view to which members of the SNMP group have access. Options include: • all-of-mib - Group members can make changes to all objects in the MIB • restricted - Group members can make changes to only the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtrees in the MIB • v1-mib - Group members can make changes to only SNMPv1 objects in the MIB • no-view - Group members cannot make changes to any object in the MIB
`notify-view-name { notify-view-name }`	**Synopsis:** [no-view | v1-mib | restricted | all-of-mib] **Default:** all-of-mib The notify view to which members of the SNMP group have access. Options include: • all-of-mib - Group members receive notifications from all objects in the MIB • restricted - Group members receive notifications from only the system, snmp, snmpEngine, snmpMPDStats, and usmStats subtrees in the MIB • v1-mib - Group members receive notifications from only SNMPv1 objects in the MIB • no-view - Group members do not receive any notifications from the MIB

4. Type `commit` and press **Enter** to save the changes.

15.2.8.3 Deleting an SNMP Group

To delete an SNMP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP group by typing:

   ```
   no admin snmp snmp-access { group } { model } { level }
   ```

   Where:

- `{ group }` is the name of the group
- `{ model }` is the security model for the group
- `{ level }` is the security level for the group

3. Type `commit` and press **Enter** to save the changes.

15.3 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 ".

15.3.1 Enabling and Configuring NETCONF Sessions

To enable and configure NETCONF sessions, do the following:

1. Make sure the CLI is in Configuration mode.

⚠ 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. Navigate to ***admin » netconf*** and configure the following parameter(s) as required:

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** true Enables NETCONF on the device, allowing it to receive and respond to NETCONF requests.
`listen-ip { listen-ip }`	**Synopsis:** A string **Default:** 0.0.0.0 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.
`port { port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 830 The default port on which the device will listen for NETCONF requests. The port corresponds with the IP address specified by the **Listen IP (listen-ip)** parameter.
`extra-ip-ports { extra-ip-ports }`	**Synopsis:** A string 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]). If the **Listen IP (listen-ip)** parameter is set to a value other than "0.0.0.0," the port specified by the **Listen Port (port)** parameter must not be associated with any additional addresses.
`max-sessions { max-sessions }`	**Synopsis:** An integer **Default:** 10 The maximum number of concurrent NETCONF sessions.
`idle-timeout { idle-timeout }`	**Synopsis:** A string **Default:** PT0S 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 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. Type `commit` and press **Enter** to save 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 99).
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 99).

15.3.2 Viewing NETCONF Statistics

To view NETCONF related statistics, type:

```
show admin netconf
```

A table or list similar to the following example appears:

```
ruggedcom# show admin netconf
netconf
 statistics
  in bad hellos     0
  in sessions       0
  dropped sessions  0
  in rpcs           0
  in bad rpcs       0
  out rpc errors    0
  out notifications 0
```

The following information is provided:

Parameter	Description
`in-bad-hellos`	**Synopsis:** 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`	**Synopsis:** An integer The total number of NETCONF sessions initiated on the device.
`dropped-sessions`	**Synopsis:** An integer The total number of NETCONF sessions dropped on the device.
`in-rpcs`	**Synopsis:** An integer The total number of NETCONF requests (i.e. rpc messages) received.
`in-bad-rpcs`	**Synopsis:** An integer The total number of NETCONF requests (i.e. rpc messages) dropped because they contained non-conformant XML.
`out-rpc-errors`	**Synopsis:** 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`	**Synopsis:** An integer The total number of notification messages sent.

15.4 Managing IPv4 Neighbors

RUGGEDCOM ROX II supports Address Resolution Protocol (ARP) tables for individual Layer 3 interfaces.

15.4.1 IPv4 Neighbor Concepts

An IPv4 neighbor is any host on the same local area network connected to the device via Ethernet cables or network swiches. 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 reqeust 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.

15.4.2 Viewing IPv4 Neighbors

An ARP table (or cache) of IPv4 neighbor information is available for a Layer 3 interface if IPv4 neighbors are discovered.

IPv4 Neighbor Information

The ARP table details the following for each entry:

Parameter	Description
`{ neigh-ipaddress }`	**Synopsis:** A string The IP address of the neighbor.

Parameter	Description
neigh-macaddress	**Synopsis:** A string The MAC address of the neighbor.
neigh-state	**Synopsis:** A string The state of the neighbor. Possible values include: • **permanent** – The entry is valid and permanent. Entries in this state must be cleared by a user. • **noarp** – The entry is valid, but no attempt to validate the entry will be made. It can be removed when its lifetime has expired. • **reachable** – The entry is valid until the reachability timeout expires. • **stale** – The entry is valid, but suspicious. • **incomplete** – The entry is not yet validated/resolved. • **delay** – Validation of the entry is delayed. • **probe** – The neighbor is being probed. • **failed** – The maximum number of probes has been exceeded and neighbor verification has failed.

Viewing the State of All IPv4 Neighbors

To view the state of all IPv4 neighbors for all Layer 3 interfaces, type:

```
show ip ipv4 neighbors
```

For example:

```
ruggedcom# show ip ipv4 neighbors
             NEIGH                              NEIGH
IFNAME       IPADDRESS       NEIGH MACADDRESS   STATE
-------------------------------------------------------------
dummy0
fe-cm-1
             172.30.141.141  none               incomplete
             172.30.141.164  00:0a:cd:27:e2:80  stale
             172.30.128.12   00:1a:64:23:9b:d8  stale
             192.168.1.111   00:1b:21:a2:fe:4d  stale
             172.30.128.1    94:b8:c5:34:ac:3f  reachable
             172.30.128.8    00:1a:64:d4:4d:1e  stale
             172.30.141.49   00:13:46:30:2f:b5  stale
switch.0001
```

Viewing the State of IPv4 Neighbors for Specific Interfaces

To view the state of IPv4 neighbors for a specific Layer 3 interface, type:

```
show ip { interface } ipv4 neighbors
```

Where { interface } is the name of the Layer 3 interface.

For example:

```
ruggedcom# show ip fe-cm-1 ipv4 neighbors
NEIGH                              NEIGH
IPADDRESS       NEIGH MACADDRESS   STATE
-------------------------------------------
172.30.141.164  00:0a:cd:27:e2:80  stale
172.30.128.12   00:1a:64:23:9b:d8  stale
192.168.1.111   00:1b:21:a2:fe:4d  stale
172.30.128.1    94:b8:c5:34:ac:3f  reachable
172.30.128.8    00:1a:64:d4:4d:1e  stale
172.30.141.49   00:13:46:30:2f:b5  stale
```

Viewing the State of a Specific IPv4 Neighbor

To view the state of a specific IPv4 neighbor in an ARP table, type:

```
show ip { interface } ipv4 neighbors status { neighbor }
```

Where:

- { interface } is the name of the Layer 3 interface
- { neighbor } is the IP address of the IPv4 neighbor

For example:

```
ruggedcom# show ip fe-cm-1 ipv4 neighbors status 172.30.128.1
NEIGH                           NEIGH
IPADDRESS     NEIGH MACADDRESS  STATE
------------------------------------------
172.30.128.1  94:b8:c5:34:ac:3f  reachable
```

15.4.3 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, type:

```
ip { interface } ipv4 neighbors status { neighbor } clear
```

Where:

- { interface } is the name of the Layer 3 interface
- { neighbor } is the IP address of the IPv4 neighbor

16 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.

16.1 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.

16.1.1 Configuring Port Mirroring

To configure port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » 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 configuing 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 383).

3. Configure port mirroring for a specific port by typing:

```
switch port-mirroring enabled target-slot { slot } tar
get-port { port } egress-src { egress } ingress-src
{ ingress }
```

Where:

- `{ slot }` is the name of the module location
- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk)
- `{ egress }` is the port number for the outgoing port
- `{ ingress }` is the port number for the the incoming port

4. Add egress and ingress source ports. For more information, refer to "Adding an Egress Source Port" (Page 897) and "Adding an Ingress Source Port" (Page 898).
5. Type `commit` and press **Enter** to save the changes.

16.1.2 Managing Egress Source Ports

This section describes how to configure and manage egress source ports for port mirroring.

16.1.2.1 Viewing a List of Egress Source Ports

To view a list of egress source port for port mirroring, type:

```
show running-config switch port-mirroring egress-src
```

If egress source ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch port-mirroring egress-src
switch port-mirroring
 egress-src lm1 1
 !
!
```

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 897).

16.1.2.2 Adding an Egress Source Port

To add an egress source port for port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the egress source port by typing:

   ```
   switch port-mirroring egress-src { slot } { port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list ofports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

16.1.2.3 Deleting an Egress Source Port

To delete an egress source port for port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no switch port-mirroring egress-src { slot } { port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

16.1.3 Managing Ingress Source Ports

This section describes how to configure and manage ingress source ports for port mirroring.

16.1.3.1 Viewing a List of Ingress Source Ports

To view a list of ingress source port for port mirroring, type:

```
show running-config switch port-mirroring ingress-src
```

If ingress source ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch port-mirroring ingress-src
switch port-mirroring
 ingress-src lm1 1
 !
!
```

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 898).

16.1.3.2 Adding an Ingress Source Port

To add an ingress source port for port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the ingress source port by typing:

   ```
   switch port-mirroring ingress-src { slot } { port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

16.1.3.3 Deleting an Ingress Source Port

To delete an ingress source port for port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no switch port-mirroring ingress-src { slot } { port }
   ```

   Where:

   - `{ slot }` is the name of the module location
   - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type `commit` and press **Enter** to save the changes.

16.2 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 235).

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.

16.2.1 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. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
`enabled`	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 **enabled** TC configuration will be included. When a work configuration is committed, the **enabled** TC configuration will be included in the work configuration. **A TC configuration needs a firewall configuration to operate**.
`mode-choice { mode-choice }`	**Synopsis:** [basic | advanced] **Default:** 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 901).
   b. Add traffic control priorities. For more information, refer to "Adding a Traffic Control Priority" (Page 904).
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 906).
   b. Add traffic control devices. For more information, refer to "Adding a Traffic Control Device" (Page 909).
   c. Add traffic control rules. For more information, refer to "Adding a Traffic Control Rule" (Page 911).
5. Type `commit` and press **Enter** to save the changes.

16.2.2 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 899).

16.2.2.1 Viewing a List of Traffic Control Interfaces

To view a list of traffic control interfaces, type:

```
show running-config qos traffic-control basic-configuration
tcinterfaces
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control basic-configuration tcinter
faces
qos
 traffic-control
  basic-configuration
   tcinterfaces te1-2-1c01ppp
    type         external
    inbandwidth  1500
    in-unit      kilobits
    outbandwidth 1500
    out-unit     kilobits
    description  "TC on T1 Link"
   !
  !
 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a Traffic Control Interface" (Page 901).

16.2.2.2 Adding a Traffic Control Interface

To add a new traffic control interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the interface by typing:

   ```
   qos traffic-control basic-configuration tcinterfaces { in
   terface }
   ```

   Where:

   - { interface } is the name of the traffic control interface

3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 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.
`type { type }`	**Synopsis:** [internal | external | none] **Default:** none (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.
`inbandwidth { inband width }`	**Synopsis:** An integer (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.
`in-unit { in-unit }`	**Synopsis:** [none | kilobits | megabits] **Default:** none The unit for inbandwidth, per second.
`outbandwidth { out bandwidth }`	**Synopsis:** An integer The outgoing bandwidth for this interface. Specify only the number here. The unit (kilobits, megabits) is specified in the out-unit.
`out-unit { out-unit }`	**Synopsis:** [kilobits | megabits] **Default:** megabits The unit for outgoing bandwidth, per second.
`description { descrip tion }`	**Synopsis:** A string A description for this configuration item.

4. Type `commit` and press **Enter** to save the changes.

16.2.2.3 Deleting a Traffic Control Interface

To delete a traffic control interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the traffic control interface by typing:

   ```
   no qos traffic-control basic-configuration tcinterfaces
   { interface }
   ```

   Where:

   - `{ interface }` is the name of the traffic control interface

3. Type `commit` and press **Enter** to save the changes.

16.2.3 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 899).

16.2.3.1 Viewing a List of Traffic Control Priorities

To view a list of traffic control priorities, type:

```
show running-config qos traffic-control basic-configuration
tcpriorities
```

If priorities have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control basic-configuration tcpriori
ties
qos
 traffic-control
  basic-configuration
   tcpriorities high
    band        high
    protocol    tcp
    port        80
    description "High priority traffic"
   !
   tcpriorities medium
    protocol    udp
    port        1500
    description "Medium priority traffic"
   !
   tcpriorities low
    band        low
    protocol    icmp
    description "Low priority traffic"
   !
  !
 !
!
```

If no priorities have been configured, add priorities as needed. For more information, refer to "Adding a Traffic Control Priority" (Page 904).

16.2.3.2 Adding a Traffic Control Priority

To add a new traffic control priority, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static MAC address by typing:

   ```
   qos traffic-control basic-configuration tcpriority
   { name }
   ```

   Where:

   - `{ name }` is the name of the traffic control priority entry
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`band { band }`	**Synopsis:** [high | medium | low] **Default:** medium Priority (band) : high, medium, low... **High band includes:** • Minimize Delay (md) (0x10), • md + Minimize Monetary Cost (mmc) (0x12), • md + Maximize Reliability (mr) (0x14), • mmc+md+mr (0x16). **Medium band includes:** • 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). **Low band includes:** • mmc (0x02), • mt (0x08), • mmc+mt (0x0a), • mr+mt (0x0c),

Parameter	Description
	• mmc+mr+mt (0x0e).
`protocol { protocol }`	**Synopsis:** A string or [tcp | udp | icmp | all] (choice) A targeted protocol.
`port { port }`	**Synopsis:** A string (choice) Source port - can be specified **only if** protocol is TCP, UDP, DCCP, SCTP or UDPlite
`address { address }`	**Synopsis:** A string (choice) The source address. This can be specified **only if** the protocol, port and interface are not defined.
`interface { inter face }`	**Synopsis:** A string between 1 and 15 characters long (choice) The source interface. This can be specified **only if** the protocol, port and address are not defined. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
`description { descrip tion }`	**Synopsis:** A string (optional) A description for this configuration.

4. Type `commit` and press **Enter** to save the changes.

16.2.3.3 Deleting a Traffic Control Priority

To delete a traffic control priority, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control priority by typing:

   ```
   no qos traffic-control basic-configuration tcpriority
   { name }
   ```

   Where:

   - `{ name }` is the name of the traffic control priority entry
3. Type `commit` and press **Enter** to save the changes.

16.2.4 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].

16.2.4.1 Viewing a List of Traffic Control Classes

To view a list of traffic control classes, type:

```
show running-config qos traffic-control advanced-configura
tion tcclasses
```

If classes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcclass
es
qos
 traffic-control
  advanced-configuration
   tcclasses TCP
    interface     te1-2-1c01ppp
    mark          1
    min-bandwidth full/2
    max-bandwidth full
    priority      1
   !
  !
 !
!
```

If no classes have been configured, add classes as needed. For more information, refer to "Adding a Traffic Control Class" (Page 906).

16.2.4.2 Adding a Traffic Control Class

To add a new traffic control class, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static MAC address by typing:

   ```
   qos traffic-control advanced-configuration tcclasses
   { name }
   ```

   Where:

   - `{ name }` is the name of the traffic control class entry
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`interface { interface }`	**Synopsis:** A string The interface to which this class applies. Each interface must be listed only once. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
`mark { mark }`	**Synopsis:** An integer between 1 and 255 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.
`min-bandwidth { min-bandwidth }`	**Synopsis:** A string 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. A calculated expression is based on a fraction of the 'full' bandwidth, such as: 1. 'full/3' for a third of the bandwidth and 2. 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any minbw-unit.
`minbw-unit { minbw-unit }`	**Synopsis:** [none | kilobits | megabits] **Default:** none (per second) Only if the minimum bandwidth is a single numerical value
`max-bandwidth { max-bandwidth }`	**Synopsis:** A string 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. A calculated expression is based on a fraction of the 'full' bandwidth, such as: 1. 'full/3' for a third of the bandwidth and 2. 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any maxbw-unit.

Parameter	Description
`maxbw-unit { maxbw-unit }`	**Synopsis:** [none | kilobits | megabits] **Default:** none (per second) only if max-bandwidth is a **single numerical value**
`priority { priority }`	**Synopsis:** An integer between 0 and 7 **Default:** 0 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).
`description { description }`	**Synopsis:** A string A description for this configuration item.

4. Type `commit` and press **Enter** to save the changes.

16.2.4.3 Deleting a Traffic Control Class

To delete a traffic control class, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control class by typing:

   ```
   no qos traffic-control advanced-configuration tcclasses
   { name }
   ```

   Where:

   - `{ name }` is the name of the traffic control class entry
3. Type `commit` and press **Enter** to save the changes.

16.2.5 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 899).

16.2.5.1 Viewing a List of Traffic Control Devices

To view a list of traffic control devices, type:

```
show running-config qos traffic-control advanced-configura
tion tcdevices
```

If devices have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcde
vices
qos
 traffic-control
  advanced-configuration
   tcdevices te1-2-1c01ppp
    inbandwidth  1500
    in-unit      kilobits
    outbandwidth 1500
    out-unit     kilobits
   !
  !
 !
!
```

If no devices have been configured, add devices as needed. For more information, refer to "Adding a Traffic Control Device" (Page 909).

16.2.5.2 Adding a Traffic Control Device

To add a new traffic control device, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the traffic control device by typing:

   ```
   qos traffic-control advanced-configuration tcdevices
   { name }
   ```

   Where:

   - `{ name }` is the name of the interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.

Parameter	Description
`inbandwidth { inband width }`	**Synopsis:** An integer **Default:** 0 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.
`in-unit { in-unit }`	**Synopsis:** [none | kilobits | megabits] **Default:** none Unit for inbandwidth, per second.
`outbandwidth { out bandwidth }`	**Synopsis:** An integer Maximum outgoing bandwidth... This is the maximum speed that can be handled. Additional packets will be dropped. This is the bandwidth that can be refrred-to as 'full' when defining classes.
`out-unit { out-unit }`	**Synopsis:** [kilobits | megabits] **Default:** megabits Unit for outgoing bandwidth, per second.
`description { descrip tion }`	**Synopsis:** A string A description for this configuration item.

4. Type `commit` and press **Enter** to save the changes.

16.2.5.3 Deleting a Traffic Control Device

To delete a traffic control device, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control device by typing:

   ```
   no qos traffic-control advanced-configuration tcdevices
   { name }
   ```

   Where:

   - `{ name }` is the name of the interface to which traffic shaping will apply.
3. Type `commit` and press **Enter** to save the changes.

16.2.6 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 899).

16.2.6.1 Viewing a List of Traffic Control Rules

To view a list of traffic control rules, type:

```
show running-config qos traffic-control advanced-configura
tion tcrules
```

If rules have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcrules
qos
 traffic-control
  advanced-configuration
   tcrules rule1
    mark-choice set
     mark 1
    !
    source       all
    destination  all
    protocol     tcp
    source-ports 80
   !
  !
 !
!
```

If no rules have been configured, add rules as needed. For more information, refer to "Adding a Traffic Control Rule" (Page 911).

16.2.6.2 Adding a Traffic Control Rule

To add a new traffic control rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the traffic control rule by typing:

   ```
   qos traffic-control advanced-configuration tcrule { name }
   ```

   Where:

   - `{ name }` is the name of the traffic control rule entry.
3. Configure the following parameter(s) as required:

Parameter	Description
`iptype { iptype }`	**Synopsis:** [ipv4 | ipv6 | ipv4ipv6] **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
`source { source }`	**Synopsis:** 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 { destination }`	**Synopsis:** A string IF name, comma-separated list of hosts or IPs, or 'all'.
`protocol { protocol }`	**Synopsis:** A string or [tcp | udp | icmp | all] **Default:** all The protocol to match.
`destination-ports { destination-ports }`	**Synopsis:** A string (Optional) A comma-separated list of port names, port numbers or port ranges.
`source-ports { source-ports }`	**Synopsis:** A string (Optional) A comma- separated list of port names, port numbers or port ranges.
`test { test }`	**Synopsis:** A string Defines the test criteria for an existing packet or connection mark. The rule will match only if the test returns true. Define the test as follows: [!]{ value }[/ { mask }][:C] ! - Reverses the test value - The value of the packet or connection mark mask - A mask to be applied to the mark before testing :C - Designates a connection mark. If not present, the test is applied by default to a packet mark. Example: !0:C
`length { length }`	**Synopsis:** A string (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 **64** Greater or equal to 65

Parameter	Description
	65: Lesser or equal to 65 **:65** In-between 64 and 768 **64:768**
`tos { tos }`	**Synopsis:** A string or [minimize-delay | maximize-throughput | maximize-reliability | minimize-cost | normal-service] (Optional) Type of Service . A pre-defined ToS value or a numerical value. The numerical value is hexadecimal. Ex.: 0x38
`description { description }`	**Synopsis:** A string A description for this configuration item.

4. Type `commit` and press **Enter** to save the changes.

16.2.6.3 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. Make sure the CLI is in Configuration mode.
2. Select the Set option by typing:

   ```
   qos traffic-control advanced-configuration tcrules
   { name } mark-choice set
   ```

   Where:

   - `{ name }` is the name of the traffic control rule
3. Configure the following parameter(s):

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 { object }`	**Synopsis:** [packet | connection] **Default:** packet Sets the mark on either a packet or a connection.
`mark { mark }`	**Synopsis:** A string A mark that corresponds to a class mark (decimal value).
`mask { mask }`	**Synopsis:** A string (optional) A mask to determine which mark bits will be set.
`chain-options { chain-options }`	**Synopsis:** [forward | postrouting | prerouting] **Default:** forward A chain where the set operation will take place.

4. Type `commit` and press **Enter** to save the changes.

Configuring a Modify Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Modify option by typing:

```
qos traffic-control advanced-configuration tcrules
{ name } mark-choice modify
```

Where:

- `{ name }` is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
`logic-op { logic-op }`	**Synopsis:** [and | or] A logical operation to perform on the current mark: AND/OR.
`mark-value { mark-value }`	**Synopsis:** A string A mark to perform the operation with (decimal value).
`modify-chain { modify-chain }`	**Synopsis:** [forward | postrouting | prerouting] **Default:** forward A chain in which the operation will take place.

4. Type `commit` and press **Enter** to save the changes.

Configuring a Save Mark

1. Make sure the CLI is in Configuration mode.
2. Configure the Save option by typing:

   ```
   qos traffic-control advanced-configuration tcrules
   { name } mark-choice save
   ```

   Where:

   - `{ name }` is the name of the traffic control rule
3. Configure the following parameter(s):

Parameter	Description
`value-mask { value-mask }`	**Synopsis:** A string Mask to process the mark with
`op-chain { op-chain }`	**Synopsis:** [forward | prerouting] **Default:** forward A chain in which the operation will take place.

4. Type `commit` and press **Enter** to save the changes.

Configuring a Restore Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Restore option by typing:

   ```
   qos traffic-control advanced-configuration tcrules
   { name } mark-choice restore
   ```

   Where:

   - `{ name }` is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
`value-mask { value-mask }`	**Synopsis:** A string A mask to process the mark with.
`op-chain { op-chain }`	**Synopsis:** [forward | prerouting] **Default:** forward A chain in which the operation will take place.

4. Type `commit` and press **Enter** to save the changes.

Configuring a Continue Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Continue option by typing:

   ```
   qos traffic-control advanced-configuration tcrules
   { name } mark-choice continue
   ```

   Where:

   - `{ name }` is the name of the traffic control rule
3. Configure the following parameter(s):

Parameter	Description
`continue-chain { continue-chain }`	**Synopsis:** [forward | prerouting] **Default:** forward A chain in which the operation will take place.

4. Type `commit` and press **Enter** to save the changes.

Configuring a DSCP Mark

1. Make sure the CLI is in Configuration mode.
2. Select the DSCP Marking option by typing:

   ```
   qos traffic-control advanced-configuration tcrules
   { name } mark-choice dscpmarking
   ```

   Where:

   - `{ name }` is the name of the traffic control rule
3. Configure the following parameter(s):

Parameter	Description
`dscp-mark { dscp-mark }`	**Synopsis:** [BE | AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 | AF41 | AF42 | AF43 | CS1 | CS2 | CS3 | CS4 | CS5 | CS6 | CS7 | EF] A DSCP class value chosen amongst the given list.
`dscpchain { dscpchain }`	**Synopsis:** [forward | postrouting | prerouting] **Default:** forward A chain where the DSCP marking will take place.

4. Type `commit` and press **Enter** to save the changes.

16.2.6.4 Deleting aTraffic Control Rule

To delete a traffic control rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control rule by typing:

   ```
   no qos traffic-control advanced-configuration tcrule
   { name }
   ```

   Where:

   - `{ name }` is the name of the traffic control rule entry
3. Type `commit` and press **Enter** to save the changes.

16.2.7 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.

16.2.7.1 Viewing a List of QoS Maps for VLANs

To view a list of QoS maps for a VLAN connection, type:

- **For Switched Ethernet Ports**

  ```
  show running-config switch { vlans } { all-vlans } { id }
  qosmap
  ```

Where:

- `{ id }` is the ID given to the VLAN

- **For Routable Ethernet Ports**

  ```
  show running-config interface eth { slot } { port } vlan
  { id } qosmap
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN

- **For Virtual Switches**

  ```
  show running-config interface virtualswitch { id } vlan
  { vlan-id } qosmap
  ```

  Where:

  - `{ id }` is the ID of the virtual switch
  - `{ vlan-id }` is the ID given to the VLAN

- **For WAN Interfaces**

  ```
  show running-config interface wan { interface } { proto
  col } channel { number } connection hdlc-eth vlan { id }
  qosmap
  ```

  Where:

  - `{ interface }` is the WAN interface
  - `{ protocol }` is either T1 or E1
  - `{ number }` is the channel number
  - `{ id }` is the ID of the VLAN

If QoS maps have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface virtualswitch vlan 100 qosmap
interface
 virtualswitch 1
  vlan 100
   qosmap 2
    ingress 10
   !
  !
 !
!
```

If no QoS maps have been configured, add maps as needed. For more information, refer to "Adding a QoS Map" (Page 919).

16.2.7.2 Adding a QoS Map

To add a QoS map for a VLAN connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the QoS map by typing:
   - **For Switched Ethernet Ports**

     ```
     switch { vlans } { all-vlans } { id } qosmap { priori
     ty }
     ```

     Where:
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
   - **For Routable-Only Ethernet Ports**

     ```
     interface eth { slot } { port } vlan { id } qosmap
     { priority }
     ```

     Where:
     - `{ slot }` is the name of the module location
     - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
   - **For Virtual Switches**

     ```
     interface virtualswitch { id } vlan { vlan-id } qosmap
     { priority }
     ```

     Where:
     - `{ id }` is the ID of the virtual switch
     - `{ vlan-id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
   - **For WAN Interfaces**

     ```
     interface wan { interface } { protocol } channel { num
     ber } connection hdlc-eth vlan { id } qosmap { priori
     ty }
     ```

     Where:
     - `{ interface }` is the WAN interface
     - `{ protocol }` is either T1 or E1
     - `{ number }` is the channel number
     - `{ id }` is the ID of the VLAN
     - `{ priority }` is the priority assigned to the QoS map

3. Configure the following parameter(s) as required:

Parameter	Description
`ingress { ingress }`	**Synopsis:** An integer between 0 and 255 Map the ingress to a mark.

4. Type `commit` and press **Enter** to save the changes.

16.2.7.3 Deleting a QoS Map

To delete a QoS map for a VLAN connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the QoS map for the VLAN connection by typing:
   - **For Switched Ethernet Ports**

     ```
     no switch { vlans } { all-vlans } { id } qosmap { pri
     ority }
     ```

     Where:
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
   - **For Routable Ethernet Ports**

     ```
     no interface eth { slot } { port } vlan { id } qosmap
     { priority }
     ```

     Where:
     - `{ slot }` is the name of the module location
     - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
   - **For Virtual Switches**

     ```
     no interface virtualswitch { id } vlan { vlan-id }
     qosmap { priority }
     ```

     Where:
     - `{ id }` is the ID of the virtual switch
     - `{ vlan-id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map

- **For WAN Interfaces**

  ```
  no interface wan { interface } { protocol } chan
  nel { number } connection hdlc-eth vlan { id } qosmap
  { priority }
  ```

  Where:

  - `{ interface }` is the WAN interface
  - `{ protocol }` is either T1 or E1
  - `{ number }` is the channel number
  - `{ id }` is the ID of the VLAN
  - `{ priority }` is the priority assigned to the QoS map

3. Type `commit` and press **Enter** to save the changes.

16.2.8 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.

16.2.8.1 Viewing a List of Egress Marks

To view a list of egress marks for a QoS map, type:

- **For Switched Ethernet Ports**

  ```
  show running-config interface switch { vlans } { all-
  vlans } { id } qosmap { priority } egress
  ```

  Where:

  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map

- **For Routable-Only Ethernet Ports**

  ```
  show running-config interface eth { slot } { port } vlan
  { id } qosmap { priority } egress
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map

- **For Virtual Switches**

  ```
  show running-config interface virtualswitch { id } vlan
  { vlan-id } qosmap { priority } egress
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map

- **For WAN Interfaces**

  ```
  show running-config interface wan { slot } { port } vlan
  { id } qosmap { priority } egress
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map

If egress marks have been configured, a table or list similar to the following example appears:

```
show running-config interface virtualswitch vs1 vlan 100 qosmap 2 egress
interface
 virtualswitch vs1
  vlan 100
   qosmap 2
    egress 11
    !
   !
  !
 !
!
```

If no egress marks have been configured, add egress marks as needed. For more information, refer to "Adding an Egress Mark" (Page 922).

16.2.8.2 Adding an Egress Mark

To add an egress mark for a QoS Map, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the QoS map by typing:
   - **For Switched Ethernet Ports**

     ```
     switch { vlans } { all-vlans } { id } qosmap { priori
     ty } egress { mark }
     ```

Where:

- `{ id }` is the ID given to the VLAN
- `{ priority }` is the priority assigned to the QoS map
- `{ mark }` is the value of the egress mark

- **For Routable-Only Ethernet Ports**

  ```
  interface eth { slot } { port } vlan { id } qosmap
  { priority } egress { mark }
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map
  - `{ mark }` is the value of the egress mark

- **For Virtual Switches**

  ```
  interface virtualswitch { id } vlan { vlan-id } qosmap
  { priority } egress { mark }
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map
  - `{ mark }` is the value of the egress mark

- **For WAN Interfaces**

  ```
  interface wan { slot } { port } vlan { id } qosmap
  { priority } egress { mark }
  ```

  Where:

  - `{ slot }` is the name of the module location
  - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
  - `{ id }` is the ID given to the VLAN
  - `{ priority }` is the priority assigned to the QoS map
  - `{ mark }` is the value of the egress mark

3. Type `commit` and press **Enter** to save the changes.

16.2.8.3 Deleting an Egress Mark

To delete an egress mark for a QoS map, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the QoS map for the VLAN connection by typing:
   - **For Switched Ethernet Ports**

     ```
     no switch { vlans } { all-vlans } { id } qosmap { pri
     ority } egress { mark }
     ```

     Where:
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
     - `{ mark }` is the value of the egress mark
   - **For Routable-Only Ethernet Ports**

     ```
     no interface eth { slot } { port } vlan { id } qosmap
     { priority } egress { mark }
     ```

     Where:
     - `{ slot }` is the name of the module location
     - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
     - `{ mark }` is the value of the egress mark
   - **For Virtual Switches**

     ```
     no interface virtualswitch { id } vlan { vlan-id }
     qosmap { priority } egress { mark }
     ```

     Where:
     - `{ slot }` is the name of the module location
     - `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - `{ id }` is the ID given to the VLAN
     - `{ priority }` is the priority assigned to the QoS map
     - `{ mark }` is the value of the egress mark
   - **For WAN Interfaces**

     ```
     no interface wan { slot } { port } vlan { id } qosmap
     { priority } egress { mark }
     ```

     Where:
     - `{ slot }` is the name of the module location

- `{ port }` is the port number (or a list of ports, if aggregated in a port trunk) for the module
- `{ id }` is the ID given to the VLAN
- `{ priority }` is the priority assigned to the QoS map
- `{ mark }` is the value of the egress mark

3. Type `commit` and press **Enter** to save the changes.

16.2.9 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 905).

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 899).

To view the QoS statistics, type:

```
show qos statistics
```

A table or list similar to the following example appears:

```
ruggedcom# show qos statistics | tab
           MIN        MAX
CLASSNAME  BANDWIDTH  BANDWIDTH  SENTBYTES  SENTPACKETS  DROPPEDPACKETS  RATE       AVERAGE
-------------------------------------------------------------------------------------------
High       1200Kbit   1500Kbit   4956594    9953         0               446104bit  112pps
Default    300000bit  1500Kbit   3029832    6084         3869            270088bit  68pps
```

The following information is provided:

Parameter	Description
`min-bandwidth`	**Synopsis:** A string The minimum guaranteed bandwidth. This is based on the device's defined characteristics.
`max-bandwidth`	**Synopsis:** A string The maximum guaranteed bandwidth in absence of any higher prioritized traffic. This is based on the device's defined characteristics.

Parameter	Description
`sentbytes`	**Synopsis:** A string The number of bytes that were sent through this class.
`sentpackets`	**Synopsis:** A string The number of packets that were sent through this class.
`droppedpackets`	**Synopsis:** A string The number of packets that were dropped in this class.
`rate`	**Synopsis:** A string Based on a 10-second average.
`average`	**Synopsis:** A string Based on a 10-second average.

16.3 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.

16.3.1 Configuring Classes of Service

To configure Classes of Service, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the CoS weighting by typing:

   ```
   switch classes-of-service cos-weighting { weighting }
   ```

   Where:

   - `{ weighting }` is the weighting algorithm for transmitting different priority CoS frames. During traffic bursts, frames queued in the switch pending transmission on a port may have different CoS priorities.
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 928) or "Adding a DSCP-to-CoS Mapping Entry" (Page 929).
4. Type `commit` and press **Enter** to save the changes.

16.3.2 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.

16.3.2.1 Viewing a List of Priority-to-CoS Mapping Entries

To view a list of priority-to-CoS mapping entries, type:

```
show running-config switch class-of-service priority-to-cos
```

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch class-of-service priority-to-cos | tab
PRIORITY  COS
------------------
0         normal
1         normal
2         normal
3         medium
4         medium
5         medium
6         high
7         high

!
```

If no entries have been configured, add entries as needed. For more information, refer to "Adding a Priority-to-CoS Mapping Entry" (Page 928).

16.3.2.2 Adding a Priority-to-CoS Mapping Entry

To add a priority-to-CoS mapping entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the entry by typing:

   ```
   switch class-of-service priority-to-cos { priority }
   ```

   Where:

   - `{ priority }` is the value of the IEEE 802.1p priority
3. Configure the following parameter(s) as required:

Parameter	Description
`cos { cos }`	**Synopsis:** [N/A | normal | medium | high | crit] **Default:** normal The Class of Service (CoS) assigned to received tagged frames with the specified IEEE 802.1p priority value.

4. Type `commit` and press **Enter** to save the changes.

16.3.2.3 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. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:

   ```
   no switch class-of-service priority-to-cos { priority }
   ```

   Where:

   - `{ priority }` is the value of the IEEE 802.1p priority
3. Type `commit` and press **Enter** to save the changes.

16.3.3 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.

16.3.3.1 Viewing a List of DSCP-to-CoS Mapping Entries

To view a list of priorities, type:

```
show running-config switch class-of-service dscp-to-cos
```

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch class-of-service dscp-to-cos | tab
DSCP  COS
--------------
1     normal
3     high
4     medium
6     normal
7     normal

!
```

If no entries have been configured, add entries as needed. For more information, refer to "Adding a DSCP-to-CoS Mapping Entry" (Page 929).

16.3.3.2 Adding a DSCP-to-CoS Mapping Entry

To add a DSCP-to-CoS mapping entry, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the entry by typing:

   ```
   switch class-of-service dscp-to-cos { dscp }
   ```

   Where:

   - `{ dscp }` is the value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header

3. Configure the following parameter(s) as required:

Parameter	Description
`cos { cos }`	**Synopsis:** [N/A | normal | medium | high | crit] **Default:** normal The Class of Service (CoS) assigned to the received frames with the specified DSCP.

4. 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 335) and/or "Adding an Ethernet Trunk Interface" (Page 351).
5. Type `commit` and press **Enter** to save the changes.

16.3.3.3 Deleting a DSCP-to-CoS Mapping Entry

To delete a DSCP-to-CoS mapping entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:

   ```
   no switch class-of-service dscp-to-cos { dscp }
   ```

   Where:

   - `{ dscp }` is the value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header

3. Type `commit` and press **Enter** to save the changes.

16.4 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 934).

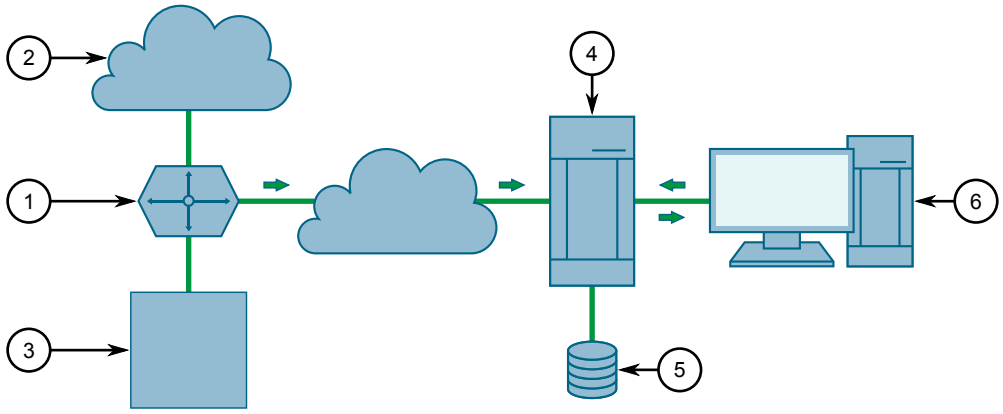
16.4.1 Understanding NetFlow Data Export

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 16.1 NetFlow

Note

RUGGEDCOM ROX II supports NetFlow version 5.

16.4.1.1 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.

16.4.2 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**.

   ⚠ NOTICE

   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 393).

3. Enable the NetFlow service. For more information, refer to "Enabling/Disabling NetFlow" (Page 933).
4. [Optional] Set the engine ID that is assigned to each flow record. For more information, refer to "Setting the NetFlow Engine ID" (Page 933).
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 934).
6. [Optional] Control how RUGGEDCOM ROX II manages active and inactive flows. For more information, refer to "Controlling Active/Inactive Flows" (Page 934).
7. Define one or more interfaces from which to monitor traffic. For more information, refer to "Adding a NetFlow Interface" (Page 935).
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 936).

16.4.3 Enabling/Disabling NetFlow

To enable or disable NetFlow, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable NetFlow by typing:

   Enabling NetFlow

   ```
   services netflow enabled
   ```

   Disabling NetFlow

   ```
   no services netflow enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

16.4.4 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. Make sure the CLI is in Configuration mode.
2. Set the engine ID by typing:

   ```
   services netflow engine-id { number }
   ```

3. Type `commit` and press **Enter** to save the changes.

16.4.5 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. Make sure the CLI is in Configuration mode.
2. Configure the maximum number of active flows tracked by NetFlow by typing:

   ```
   services netflow maxflows { number }
   ```

   Where { number } is the number of active flows. The default value is 16384, but the value can be set anywhere between 0 and 65535.
3. Type `commit` and press **Enter** to save the changes.

16.4.6 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » netflow » timeouts*** and configure the following parameters:

Parameter	Description
`active-timeout { active-timeout }`	**Synopsis:** An integer equal to or greater than 1 **Default:** 1800 The time in seconds (s) an active flow remains active.
`inactive-timeout { inactive-timeout }`	**Synopsis:** An integer equal to or greater than 1 **Default:** 15 The time in seconds (s) an inactive flow remains in the cache before it is deleted.

3. Type `commit` and press **Enter** to save the changes.

16.4.7 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.

16.4.7.1 Viewing a List of NetFlow Interfaces

To view a list of interfaces configured to monitor traffic for NetFlow, type:

```
show running-config services netflow interface
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services netflow interface | tab
NAME         DIRECTION  TYPE
------------------------------
switch.0001  both       ipv4

 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to "Adding a NetFlow Interface" (Page 935).

16.4.7.2 Adding a NetFlow Interface

To add a NetFlow interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the interface by typing:

   ```
   services netflow interface { interface } direction { di
   rection }
   ```

   Where:

   - { interface } is the desired interface
   - { direction } is 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
3. Type `commit` and press **Enter** to save the changes.

16.4.7.3 Deleting a NetFlow Interface

To delete a NetFlow interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the interface by typing:

   ```
   no services netflow interface { interface }
   ```

   Where { interface } is the desired interface.
3. Type `commit` and press **Enter** to save the changes.

16.4.8 Managing NetFlow Collectors

RUGGEDCOM ROX II can be configured to forward flows to up to four NetFlow collectors.

16.4.8.1 Viewing a List of NetFlow Collectors

To view a list of NetFlow collectors the device can send flows, type:

```
show running-config services netflow collector
```

If collectors have been configured, a table or list similar to the following example appears:

```
show running-config services netflow collector | tab
IP ADDRESS      PORT  ENABLED
------------------------------
172.30.142.224  6030  true

 !
!
```

If no collectors have been configured, add collectors as needed. For more information, refer to "Adding a NetFlow Collector" (Page 936).

16.4.8.2 Adding a NetFlow Collector

To define a NetFlow collector to which RUGGEDCOM ROX II will send flows, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the collector by typing:

Note

A single server can host multiple NetFlow collectors, each monitoring a specific UDP port.

```
services netflow collector { address } { port }
```

Where:

- { address } is the IPv4 address of the NetFlow collector
- { port } is the UDP port used by the NetFlow Collector to receive messages

3. [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 937).
4. Type `commit` and press **Enter** to save the changes.

16.4.8.3 Enabling/Disabling a NetFlow Collector

To enable or disable a NetFlow collector defined in RUGGEDCOM ROX II, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the collector by typing:

   Enabling

   ```
   services netflow collector { address } { port } enable
   ```

   Disabling

   ```
   no services netflow collector { address } { port } enable
   ```

   Where:

   - { address } is the IPv4 address of the NetFlow collector
   - { port } is the UDP port used by the NetFlow collector to receive messages
3. Type `commit` and press **Enter** to save the changes.

16.4.8.4 Deleting a NetFlow Collector

To delete a NetFlow collector, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the collector by typing:

   Note

   A single server can host multiple NetFlow collectors, each monitoring a specific UDP port. It is important to specify both the IP address and port number when deleting a NetFlow collector.

   ```
   no services netflow collector { address } { port }
   ```

   Where:

- { address } is the IPv4 address of the NetFlow collector
- { port } is the UDP port used by the NetFlow Collector to receive messages

3. Type `commit` and press **Enter** to save the changes.

16.4.9 Viewing the Status of NetFlow

To view the status of NetFlow, type:

```
show services netflow status
```

For example:

```
ruggedcom# show services netflow status
status
 flow-status
  active flows 2
 rate-status
  bits sec     19311176
  pkts sec     2399
  bits sec min 19009225
  pkts sec min 2358
```

The following information is displayed:

Parameter	Description
`bits-sec`	**Synopsis:** An integer The current rate in bits/s.
`pkts-sec`	**Synopsis:** An integer The current rate in packets/s.
`bits-sec-min`	**Synopsis:** An integer The average rate in bits/s over a minute.
`pkts-sec-min`	**Synopsis:** An integer The average rate in packets/s over a minute.

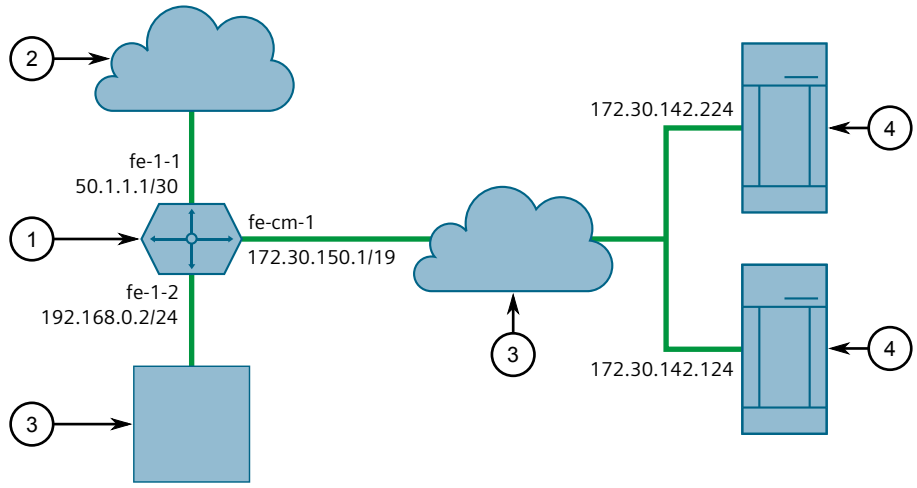
16.4.10 Example: Exporting Flows to Multiple Collectors

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 16.2 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 393).
2. Enable NetFlow. For more information, refer to "Enabling/Disabling NetFlow" (Page 933).
3. Define two NetFlow collectors and make sure they are both enabled. For more information, refer to "Adding a NetFlow Collector" (Page 936).
4. Define the interface that will be monitored by NetFlow. For more information, refer to "Adding a NetFlow Interface" (Page 935).
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
  !
 !
!
```

16.5 Managing Port Rate Limiting

This section describes how to manage port rate limiting.

16.5.1 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.

16.5.2 Configuring Port Rate Limiting

To configure port rate limiting, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » switch » { slot } » { port }***, where { slot } is the module and { port } is the switched Ethernet port.
3. Configuring the rate Limiting settings by configuring the following parameter(s) as required:

Parameter	Description
`ingress-limit { ingress-limit }`	**Synopsis:** An integer between 62 and 256000 or [disabled] **Default:** 1000 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.

Parameter	Description
	The default value is 1000 kbps. If not set(cleared), this feature is disabled.
`ingress-frames { ingress-frames }`	**Synopsis:** [broadcast | multicast | mcast-flood-ucast | all] **Default:** broadcast This parameter specifies the types of frames to rate-limit on this port. It applies only to received frames: • BROADCAST : only broadcast frames will be limited. • MULTICAST : all multicast frames (including broadcast) will be limited. • MCAST-FLOOD-UCAST : all multicast frames (including broadcast) will be limited. Unicast will not be limited. • ALL : all frames (both multicast and unicast) will be limited.
`egress-limit { egress-limit }`	**Synopsis:** [disabled] or An integer between 62 and 256000 **Default:** disabled 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.

4. Type `commit` and press **Enter** to save the changes.

17 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

17.1 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 944).
2. Configure the system time zone. For more information, refer to "Configuring the System Time Zone" (Page 944).
3. Configure the local time settings. For more information, refer to "Configuring the Local Time Settings" (Page 944).
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 955).
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 955).
6. Add remote NTP servers. For more information, refer to "Adding an NTP Server" (Page 950).
7. Add broadcast/mutlicast addresses for the NTP server. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 957).
8. If required, add server authentication keys. For more information, refer to "Adding a Server Key" (Page 952).
9. Add restrictions for the remote NTP servers. For more information, refer to "Adding a Server Restriction" (Page 953).
10. Enable and configure the NTP service. For more information, refer to "Enabling and Configuring the NTP Service" (Page 945).
11. View the status of the NTP service. For more information, refer to "Viewing the NTP Service Status" (Page 945).

17.2 Configuring the System Time and Date

To configure the system time and date, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the system time and date by typing:

   ```
   admin set-system-clock time { time-date }
   ```

   Where:

   - `{ time-date }` is the date time in the format YYYY-MM-DD HH:MM:SS
3. Type `commit` and press **Enter** to save the changes.

17.3 Configuring the System Time Zone

To configure the system time zone, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the system time zone by typing:

   Note

   The Etc/GMT time zones conform to the POSIX style and have their signs reversed from common usage. In POSIX style, zones west of Greenwich Mean Time (GMT) have a positive sign, while zones east of GMT have a negative sign.

   ```
   admin timezone category { category } zone { zone }
   ```

   Where:

   - `{ category }` is the time zone category
   - `{ zone }` is the time zone
3. Type `commit` and press **Enter** to save the changes.

17.4 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. Make sure the CLI is in Configuration mode.
2. Enable and configure the local NTP time settings by typing:

   ```
   services ntp local-clock enable stratum { number }
   ```

   Where:

   - `{ number }` is the stratum number of the local clock
3. Type `commit` and press **Enter** to save the changes.

17.5 Enabling and Configuring the NTP Service

To enable and configure the NTP service, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » ntp*** and configure the following parameters:

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.

Parameter	Description
`enabled { enabled }`	**Synopsis:** [true | false] **Default:** false Enables NTP service.
`bind-interface { bind interface }`	**Synopsis:** A string 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. If the bind interface is down, the source IP address for traffic transmitted by NTP will be the IP address of another egress interface.
`bind-ip-address { bind-ip-address }`	**Synopsis:** A string between 7 and 15 characters long The defined IP address is used as the source IP address for all outgoing NTP messages. 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.

3. Type `commit` and press **Enter** to save the changes.

17.6 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 945).
2. Display the NTP service status by typing:

```
services ntp ntp-status
```

A table similar to the following example appears:

```
ruggedcom# services ntp ntp-status
 ntp-status
   remote           refid      st t when poll reach   delay   offset  jitter
 ==============================================================================
 *142.3.100.2     .GPS.          1 u  937 1024  377   38.104   -0.273   0.802
  172.30.149.45   .INIT.        16 u    - 1024    0    0.000    0.000   0.000
 +206.186.255.226 128.138.140.44   2 u  413 1024  377   58.578    0.143
 27.963
 x206.186.255.227 CHU_AUDIO(1)     3 u  927 1024  377   58.034  10846.0
 30.289
 +209.87.233.53   209.87.233.52    2 u  449 1024  377   27.060   -1.132
 3.153
```

The following information is provided:

Parameter	Description
`{ remote }`	**Synopsis:** A string up to 40 characters long Remote address.
`reference-id`	**Synopsis:** A string up to 40 characters long The identification of the reference clock.
`stratum`	**Synopsis:** A string up to 32 characters long The stratum number of the reference clock.
`address-type`	**Synopsis:** A string up to 32 characters long The address type of the remote machine.
`when`	**Synopsis:** A string up to 32 characters long The number of seconds since the last poll of the reference clock.
`poll`	**Synopsis:** A string up to 32 characters long The polling interval in seconds.
`reach`	**Synopsis:** A string up to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
`delay`	**Synopsis:** A string up to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
`offset`	**Synopsis:** A string up to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
`jitter`	**Synopsis:** 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 *falseticker*.
.	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 *outlier*.
+	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.

17.7 Viewing the Status of Reference Clocks

To view the status of reference clocks, type:

```
show services ntp status
```

A table similar to the following example appears:

```
ruggedcom# show services ntp status reference-clock
                                REFERENCE           ADDRESS
ADDRESS          STATE          ID         STRATUM  TYPE     WHEN  POLL  REACH  DELAY  OFFSET
 JITTER
------------------------------------------------------------------------------------------------
127.127.1.0      System peer    .LOCL.  10       1        2     64    377    0.000  0.000   0.000
206.186.255.227  Not synchronized  .INIT.  16       -        -     1024  0      0.000  0.000   0.000
206.186.255.226  Not synchronized  .INIT.  16       -        -     1024  0      0.000  0.000   0.000
142.3.100.2      Not synchronized  .INIT.  16       -        -     1024  0      0.000  0.000   0.000
```

The following information is provided:

Parameter	Description
`{ address }`	**Synopsis:** A string up to 40 characters long The IP address of the reference clock.
`state`	**Synopsis:** A string up to 32 characters long The state of the clock.
`reference-id`	**Synopsis:** A string up to 40 characters long The identification of the reference clock.

Parameter	Description
`stratum`	**Synopsis:** A string up to 32 characters long The stratum number of the reference clock.
`address-type`	**Synopsis:** A string up to 32 characters long The address type of the remote machine.
`when`	**Synopsis:** A string up to 32 characters long The number of seconds since the last poll of the reference clock.
`poll`	**Synopsis:** A string up to 32 characters long The polling interval in seconds.
`reach`	**Synopsis:** A string up to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
`delay`	**Synopsis:** A string up to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
`offset`	**Synopsis:** A string up to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
`jitter`	**Synopsis:** A string up to 32 characters long The observed jitter (in milliseconds).

17.8 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 952).

17.8.1 Viewing a List of NTP Servers

To view a list of NTP servers configured on the device, type:

```
show running-config services ntp server
```

If servers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services ntp server | tab
                                                                    NTP
NAME             ENABLED  PEER  MINPOLL  MAXPOLL  IBURST  VERSION  PREFER  KEY
-------------------------------------------------------------------------------
142.3.100.2      X        -     6        10       -       -        X       -
206.186.255.226  X        -     6        10       -       -        -       -
206.186.255.227  X        -     6        10       -       -        -       -

!
!
```

If no servers have been configured, add servers as needed. For more information, refer to "Adding an NTP Server" (Page 950).

17.8.2 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, type:

```
show services ntp status monitor-list
```

If hosts are detected, a table or list similar to the following example appears:

```
ruggedcom# show services ntp status monitor-list | tab
                                                                    AVERAGE   LAST
REMOTE         PORT  COUNT  MODE  VERSION  RESTRICT                  INTERVAL  INTERVAL
-------------------------------------------------------------------------------------
192.168.0.1    123   2      3     4        [ nomodify nopeer noquery notrap ]  447       887
192.168.0.2    123   1      3     4        [ nomodify nopeer noquery notrap ]  885       885
192.168.0.3    123   1      3     4        [ nomodify nopeer noquery notrap ]  883       883
192.168.0.4    123   1      3     4        [ nomodify nopeer noquery notrap ]  881       881
192.168.1.1    123   1      3     4        [ nomodify nopeer noquery notrap ]  862       862
192.168.1.3    123   1      3     4        [ nomodify nopeer noquery notrap ]  854       854
192.168.1.8    123   1      3     4        [ nomodify nopeer noquery notrap ]  850       850
192.168.2.1    123   1      4     4        [ nomodify nopeer noquery notrap ]  837       837
192.168.2.4    123   1      4     4        [ nomodify nopeer noquery notrap ]  834       834
192.168.2.10   123   1      4     4        [ nomodify nopeer noquery notrap ]  830       830
192.168.3.3    123   1      1     4        [ nomodify nopeer noquery notrap ]  823       823
192.168.3.7    123   1      1     4        [ nomodify nopeer noquery notrap ]  816       816
192.168.3.9    123   1      1     4        [ nomodify nopeer noquery notrap ]  813       813
```

The table/list provides the following information:

Parameter	Description
`{ remote }`	**Synopsis:** A string up to 40 characters long Remote address.
`port`	**Synopsis:** An integer UDP port number.
`count`	**Synopsis:** An integer Number of packets received.

Parameter	Description
`mode`	**Synopsis:** An integer Mode of last packet.
`version`	**Synopsis:** An integer Version of last packet.
`restrict`	**Synopsis:** [ignore | kod | limited | lowpriotrap | nomodify | nopeer | noquery | noserve | notrap | notrust | ntpport | version] Restrict flags.
`average-interval`	**Synopsis:** An integer Average interval (in seconds) between packets from this address.
`last-interval`	**Synopsis:** 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.

17.8.3 Adding an NTP Server

To configure an NTP server on the device, do the following:

1. Make sure the CLI is in Configuration mode.
2. [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 951).
3. Add the NTP server by typing:

   Note

   RUGGEDCOM ROX II supports both IPv4 and IPv6 addresses.

   ```
   services ntp server { IP Address }
   ```

   Where:

   - `{ IP Address }` is the address of the remote NTP server
4. Configure the following parameter(s) as required:

Parameter	Description
`enabled`	Turns on the NTP interface to this server.
`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.

Parameter	Description
`minpoll { minpoll }`	**Synopsis:** An integer between 4 and 17 **Default:** 6 The minimum poll interval for NTP messages, in seconds as a power of two.
`maxpoll { maxpoll }`	**Synopsis:** An integer between 4 and 17 **Default:** 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 { ntp-version }`	**Synopsis:** 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 { key }`	**Synopsis:** An integer equal to or greater than 1 An authentication key associated with this host.

5. [Optional] Set restrictions to control which NTP services can be accessed on the server. For more information, refer to "Adding a Server Restriction" (Page 953).
6. Type `commit` and press **Enter** to save the changes.

17.8.4 Deleting an NTP Server

To delete an NTP server configured on the device, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the NTP server by typing:

   ```
   no services ntp server { IP Address }
   ```

   Where:

   - `{ IP Address }` is the internal address of the remote NTP server.
3. Type `commit` and press **Enter** to save the changes.

17.8.5 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.

17.8.5.1 Viewing a List of Server Keys

To view a list of server keys, type:

```
show running-config services ntp key
```

If keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services ntp key
services
 ntp
  key 1
   value   $4$87sRT/Z+sxs9hYYI0d4IDw==
   trusted
  !
 !
!
```

If no server keys have been configured, add keys as needed. For more information, refer to "Adding a Server Key" (Page 952).

17.8.5.2 Adding a Server Key

To add a server key, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the key by typing:

   ```
   services ntp key { id }
   ```

   Where:

   - `{ id }` is the ID assigned to the key
3. Configure the following parameter(s) as required:

Parameter	Description
`value { value }`	**Synopsis:** 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.

4. Type `commit` and press **Enter** to save the changes.

17.8.5.3 Deleting a Server Key

To delete a server key, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the chosen key by typing:

   ```
   no services ntp key { id }
   ```

   Where:

   - `{ id }` is the ID assigned to the key
3. Type `commit` and press **Enter** to save the changes.

17.8.6 Managing Server Restrictions

Server restrictions control access to the NTP servers.

17.8.6.1 Viewing a List of Server Restrictions

To view a list of NTP server restrictions, type:

```
show running-config services ntp restrict
```

If restrictions have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services ntp restrict | tab
NAME       MASK     FLAGS
---------------------------
127.0.0.1  default  -

 !
!
```

If no server restrictions have been configured, add restrictions as needed. For more information, refer to "Adding a Server Restriction" (Page 953).

17.8.6.2 Adding a Server Restriction

To add an NTP server restriction, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the restriction by typing:

   ```
   services ntp restrict { address } { mask }
   ```

   Where:

   - `{ address }` is the IP address to match. The address can be a host or network IP address, or a valid host DNS name.
   - `{ mask }` is the mask used to match the address. A value of 255.255.255.255 indicates the address is treated as the address of an individual host.
3. 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 localhost, or to disable this feature entirely if not required. This prevents DDoS (Distributed Denial of Service) reflection/amplification attacks. To set this restriction, configure the following flags: **kod**, **nomodify**, **nopeer**, **noquery** and **notrap**.

Parameter	Description
`flags { flags }`	**Synopsis:** [ignore | kod | limited | lowpriotrap | nomodify | nopeer | noquery | noserve | notrap | notrust | ntpport | version] Flags restrict access to NTP services. An entry with no flags allows free access to the NTP server. • Version: Denies packets that do not match the current NTP version. • ntpport: Matches only if the source port in the packet is the standard NTP UDP port (123). • notrust: Denies service unless the packet is cryptographically authenticated. • notrap: Declines to to provide mode 6 control message trap service to matching hosts. • noserve: Denies all packets except ntpq(8) and ntpdc(8) queries. • noquery: Denies ntpq(8) and ntpdc(8) queries. • nopeer: Denies packets which result in mobilizing a new association. • nomodify: Denies ntpq(8) and ntpdc(8) queries attempting to modify the state of the server; queries returning information are permitted. • lowpriotrap: Declares traps set by matching hosts to be low priority. • limited: Denies service if the packet spacing violates the lower limits specified in the NTP discard setting. • kod: Sends a Kiss-o'-Death (KoD) packet when an access violation occurs. • ignore: Denies all packets.

4. Type `commit` and press **Enter** to save the changes.

17.8.6.3 Deleting a Server Restriction

To delete an NTP server restriction, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the restriction by typing:

   ```
   no services ntp restrict { address } { mask }
   ```

   Where:

   - `{ address }` is the IP address to match. The address can be a host or network IP address, or a valid host DNS name.
   - `{ mask }` is the mask used to match the address. A value of 255.255.255.255 indicates the address is treated as the address of an individual host.

3. Type `commit` and press **Enter** to save the changes.

17.9 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.

17.9.1 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » ntp » multicastclient*** and configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables the multicast message mode.
`address { address }`	**Synopsis:** A string between 1 and 253 characters long **Default:** 224.0.1.1 The multicast address on which the NTP client listens for NTP messages.

3. Add a multicast address for a known NTP server. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 957).
4. Type `commit` and press **Enter** to save the changes.

17.9.2 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. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » time » ntp***.
3. Configure the following parameters as required:

Parameter	Description
`broadcastclient`	Enables/disables the broadcast client.

4. Add a broadcast address for a known NTP server. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 957).
5. Type `commit` and press **Enter** to save the changes.

17.9.3 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.

17.9.3.1 Viewing a List of Broadcast/Multicast Addresses

To view a list of broadcast/multicast addresses, type:

```
show running-config services ntp broadcast
```

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services ntp broadcast
services
 ntp
  broadcast 224.0.0.1
   no enabled
   key 1
   no ntp-version
  !
 !
!
```

If no broadcast/multicast addresses have been configured, add addresses as needed. For more information, refer to "Adding a Broadcast/Multicast Address" (Page 957).

17.9.3.2 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. Make sure a server key has been configured with the broadcast/multicast setting to enable NTP authentication. For more information, refer to "Adding a Server Key" (Page 952).
2. Make sure the CLI is in Configuration mode.
3. Add the address by typing:

   ⚠ NOTICE

   The broadcast/multicast address must be the same as the address for the NTP multicast client.

   ```
   services ntp broadcast { address }
   ```

   Where:

   - `{ address }` is the broadcast or multicast address
4. Configure the following parameter(s) as required:

Parameter	Description
`enabled`	Enables sending broadcast or multicast NTP messages to this address.
`key { key }`	**Synopsis:** An integer equal to or greater than 1 Authentication key.
`ntp-version { ntp-version }`	**Synopsis:** 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.
`ttl { ttl }`	**Synopsis:** An integer between 1 and 127 **Default:** 1 Time to live.

5. Type `commit` and press **Enter** to save the changes.

17.9.3.3 Deleting a Broadcast/Multicast Address

To delete a broadcast/multicast address for an NTP server, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the restriction by typing:

   ```
   no services ntp broadcast { address }
   ```

   Where:

   - `{ address }` is the broadcast or multicast address
3. Type `commit` and press **Enter** to save the changes.

18 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 111).

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.

18.1 Viewing a List of Installed Applications

To view a list of RUGGEDCOM ROX II applications installed on the device, type:

```
show apps installed-apps
```

If applications have been installed, a table or list similar to the following example appears:

```
ruggedcom# show apps installed-apps
APP NAME  VERSION
------------------
crossbow  4.1.2
```

If no applications have been installed, install applications as needed. For more information, refer to "Installing an Application" (Page 959).

18.2 Installing an Application

To install an application, do the following:

1. Make sure the CLI is in Configuration mode.

2. Install the application by typing:

   ```
   admin rox-imaging apps install-app url { URL }
   ```

   Where:

   - `{ URL }` is the URL of the desired application

18.3 Upgrading an Application

To upgrade an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Install the application by typing:

   ```
   admin rox-imaging apps upgrade-app url { URL }
   ```

   Where:

   - `{ URL }` is the URL of the desired application

18.4 Uninstalling an Application

To uninstall an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Uninstall the application by typing:

   ```
   admin rox-imaging apps uninstall-app app-name { name }
   ```

   Where:

   - `{ name }` is the name of the application to uninstall as it appears in the repository configuration.

18.5 Managing the RUGGEDCOM CROSSBOW Application

RUGGEDCOM CROSSBOW is part of the RUGGEDCOM family of communications products. It was developed to address the need to interactively and securely access remote field devices to perform maintenance, configuration, and data retrieval functions.

RUGGEDCOM CROSSBOW allows a device maintenance application on a client PC to communicate with its associated devices remotely, as if the user's PC was directly connected to the end device.

The RUGGEDCOM CROSSBOW application enables a RUGGEDCOM ROX II device to launch a device maintenance application at the facility level. This is referred to as a Station Access Controller or SAC. A SAC is a local version of the primary CROSSBOW Server, which is located at a remote site. During normal operation, communications

occur as usual between the remote CROSSBOW Server (the enterprise server) and the devices within the facility. However, if network connectivity is lost, or if the network speed makes it impractical for an on-site operator to use the enterprise server connection, a user can launch CROSSBOW Client from within the facility, connect to the SAC, and restore access to all of the facility's devices using their usual RUGGEDCOM CROSSBOW interface.

Operations initiated via the SAC are logged and can be uploaded to the enterprise server database after the network connection is restored. The SAC appears as a device in the Device View in the main RUGGEDCOM CROSSBOW database.

Note

For more information about RUGGEDCOM CROSSBOW, refer to the technical documentation provided with the product.

18.5.1 Enabling/Disabling CROSSBOW

To enable or disable communication with a RUGGEDCOM CROSSBOW system, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable communication by typing:

   ```
   apps crossbow enabled
   ```

   Or disable communication by using the *no* version of the command:

   ```
   no apps crossbow enabled
   ```

3. Type `commit` and press **Enter** to save the changes.

18.5.2 Configuring the Client Connection

To configure the client connection for RUGGEDCOM CROSSBOW, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***apps » crossbow » client-connection***.
3. Configure the following parameters:

Parameter	Description
`ipaddr { ipaddr }`	**Synopsis:** A string between 7 and 15 characters long or A string between 6 and 40 characters long The IP address to which a client will connect to the Station Access Controller (SAC).

Parameter	Description
`port { port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 21000 The TCP port to which a client will connect to the Station Access Controller (SAC).
`ClientConnectionTimeout { ClientConnectionTimeout }`	**Synopsis:** An integer **Default:** 15 The Client Connection Timeout in minutes (set to 0 for no timeout).
`DeviceSessionTimeout { DeviceSessionTimeout }`	**Synopsis:** An integer **Default:** 15 The Device Session Timeout in minutes (set to 0 for no timeout).

4. Type `commit` and press **Enter** to save the changes.

18.5.3 Configuring CROSSBOW Certificates and Private Keys

To configure a certificate and and private key for RUGGEDCOM CROSSBOW, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a certificate. For more information, refer to "Adding a Certificate" (Page 225).
3. Add a private key. For more information, refer to "Adding a Private Key" (Page 220).
4. Configure the CA certificate and key for RUGGEDCOM CROSSBOW by typing:

   ```
   apps crossbow certificate cert { certificate } cert-private-key { key }
   ```

   Where:

   - `{ certificate }` is the name of the CA certificate loaded on the device
   - `{ key }` is the name of the private key loaded on the device
5. Type `commit` and press **Enter** to save the changes.

18.5.4 Managing SAC Connections

This section describes how to configure and manage Station Access Controller (SAC) connections for RUGGEDCOM CROSSBOW.

18.5.4.1 Viewing a List of SAC Connections

To view a list of SAC connections, type:

```
show running-config apps crossbow sac-connection
```

```
ruggedcom# show running-config apps crossbow sac-connection
apps crossbow sac-connection connection-list 172.30.155.102
 sam-name TestSAM2
!
```

If no SAC connections have been configured, add connections as needed. For more information, refer to "Adding a SAC Connection" (Page 963).

18.5.4.2 Adding a SAC Connection

To add a SAC connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the connection by typing:

   ```
   apps crossbow sac-connection { address }
   ```

   Where { address } is the IP address of parent Secure Access Manager (SAM) to which the SAC will connect.
3. Configure the following parameter(s) as required:

Parameter	Description
`sam-name { sam-name }`	**Synopsis:** A string between 1 and 128 characters long The common name in the certificate that the Secure Access Manager (SAM - parent of SAC) will present when mutually authenticating with the Station Access Controller (SAC).
`sam-port { sam-port }`	**Synopsis:** An integer between 0 and 65535 **Default:** 21000 The TCP port of SAM (parent of SAC) to which SAC (Station Access Controller) will connect.

4. Type `commit` and press **Enter** to save the changes.

18.5.4.3 Deleting a SAC Connection

To delete a SAC connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the area tag by typing:

   ```
   no apps crossbow sac-connection { address }
   ```

Where { address } is the IP address of parent Secure Access Manager (SAM) to which the SAC will connect.

3. Type `commit` and press **Enter** to save the changes.

18.5.5 Managing CROSSBOW CA Certificate Lists

This section describes how to configure CA (Certified Authority) certificates for the RUGGEDCOM CROSSBOW application.

18.5.5.1 Viewing a List of RUGGEDCOM CROSSBOW Certificate Lists

To view a list of CA certificate lists configured for the RUGGEDCOM CROSSBOW application, type:

```
show running-config apps crossbow certificate ca-cert-list
```

If CA certificate lists have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config apps crossbow certificate ca-cert-list
apps crossbow certificate ca-cert-list Crossbow_CA
!
```

If no CA certificate lists have been configured, add lists as needed. For more information, refer to "Adding a CA Certificate List" (Page 964).

18.5.5.2 Adding a CA Certificate List

To add a CA certificate list for the RUGGEDCOM CROSSBOW application, do the following:

1. Make sure the required CA (Certified Authority) certificate has been added to the device. For more information, refer to "Adding a CA Certificate and CRL" (Page 218).
2. Make sure the CLI is in Configuration mode.
3. Add the certificate list by typing:

   ```
   apps crossbow certificate ca-cert-list { name }
   ```

   Where:

   - `{ name }` is the name of the CA (Certified Authority) certificate.
4. Type `commit` and press **Enter** to save the changes.

18.5.5.3 Deleting a CA Certificate List

To delete a CA certificate list for the RUGGEDCOM CROSSBOW application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the CA certificate by typing:

   ```
   no apps crossbow certificate ca-cert-list { name }
   ```

   Where:

   - `{ name }` is the name of the CA (Certified Authority) certificate.
3. Type `commit` and press **Enter** to save the changes.

18.5.6 Viewing the Status of RUGGEDCOM CROSSBOW

To view the status of RUGGEDCOM CROSSBOW, type:

```
show apps crossbow status
```

A table or list similar to the following example appears:

```
ruggedcom# show apps crossbow status
apps crossbow status
 daemon status "crossbowd is running"
```

18.5.7 Viewing the RUGGEDCOM CROSSBOW Log

To view the RUGGEDCOM CROSSBOW log , do the following:

1. Make sure the CLI is in Configuration mode.
2. Display the log by typing:

   ```
   show log crossbow.log
   ```

   A table or list similar to the following appears:

```
ruggedcom# show log crossbow.log
Jun  1 15:44:02 Rx1500 crossbowd[17124]:  crossbowd
 [17124],              P:Log Level set to 2
Jun  1 15:44:02 Rx1500 crossbowd[17124]:  crossbowd
 [17124],              P:Starting Crossbow Server
Jun  1 15:44:04 Rx1500 crossbowd[17136]:  CrossBow
 [17136],              P:Log Level set to 2
Jun  1 15:44:04 Rx1500 crossbowd[17137]:  CrossBow
 [17137],              P:Log Level set to 2
Jun  1 15:44:04 Rx1500 crossbowd[17136]:  CrossBow
 [17136],              W:Win_eLAN_Protocol_SSL_Daemon::SetUseTLS12():172:
 Specifically configuring this TCPServer to use TLS 1.3 along with TLS1.2 as
 per configuration.
Jun  1 15:44:04 Rx1500 crossbowd[17136]:  CrossBow
 [17136],              W:Win_eLAN_Protocol_SSL_Daemon::SetUseTLS12():176: En
abling Internal security API for TCPServer
```

```
Jun  1 15:44:04 Rx1500 crossbowd[17136]:  CrossBow
 [17136],              W:CipherSuiteNames parameter value is :
Jun  1 15:44:04 Rx1500 crossbowd[17136]:  CrossBow
 [17136],              W:Win_eLAN_Protocol_SSL_Daemon::SetTLSCiphers():269:On
 ROX Enabling both TLS1.2 and TLS1.3 ciphers for TCPServer
Jun  1 15:44:04 Rx1500 crossbowd[17137]:  CrossBow
 [17137],              W:Win_eLAN_Protocol_SSL_Daemon::SetUseTLS12():172:
 Specifically configuring this TCPServer to use TLS 1.3 along with TLS1.2 as
 per configuration.
Jun  1 15:44:04 Rx1500 crossbowd[17137]:  CrossBow
 [17137],              W:Win_eLAN_Protocol_SSL_Daemon::SetUseTLS12():176: En
abling Internal security API for TCPServer
Jun  1 15:44:04 Rx1500 crossbowd[17137]:  CrossBow
 [17137],              W:CipherSuiteNames parameter value is :
Jun  1 15:44:04 Rx1500 crossbowd[17137]:  CrossBow
 [17137],              W:Win_eLAN_Protocol_SSL_Daemon::SetTLSCiphers():269:On
 ROX Enabling both TLS1.2 and TLS1.3 ciphers for TCPServer
.
.
.
```

19 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:

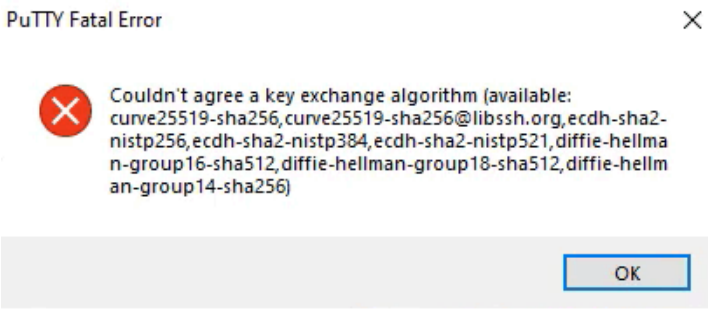
For further assistance, contact Siemens Customer Support.

Note

For a description of pre-configured alarms, refer to "Pre-Configured Alarms" (Page 144).

19.1 Management Access

The following describes common problems related to management access.

Problem	Solution
SSH/Telnet client displays a key exchange error when attempting to access RUGGEDCOM ROX II.	Some SSH/Telnet clients, such as PuTTy, may present an error message stating an agreement on a key exchange algorithm could not be reached.  Figure 19.1 PuTTy Fatal Error This issue can be resolved by either: • Installing the latest version of the SSH/Telnet client • Using an alternative application, such as **TeraTerm** (https://osdn.net/projects/ttssh2) or **securecrt** (https://www.vandyke.com/products/securecrt/) • Downgrading the Key Exchange (KEX) algorithm used by RUGGEDCOM ROX II to a lower grade cipher For more information about downgrading the KEX algorithm, refer to "Enabling SSH Server and NETCONF Algorithms" (Page 169).

19.2 Feature Keys

The following describes common problems related to feature keys.

Problem	Solution
A file-based feature key does not match the hardware	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. 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.

19.3 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.	A possible cause of intermittent operation is that of a *duplex mismatch*. 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. 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. The ping command with flood options is a useful tool for testing commissioned links. The command `ping 192.168.0.1 500 2` 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.
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.

19.4 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.	Is the port used to connect the router included in the Router Ports list? To determine whether the multicast stream is being delivered to the router, view the statistics collected for switched Ethernet ports.

Problem	Solution
	For more information, refer to "Viewing Switched Ethernet Port Statistics" (Page 342). Verify the traffic count transmitted to the router is the same as the traffic count received from the multicasting source.
The video stream at an end station is of poor quality.	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. 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. **Note** Multicasting will introduce latency in all traffic on the network. Plan the network carefully to account for capacity and latency concerns.
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?	IGMP is not broken. This may in fact be proper switch behavior. 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. The same behavior will be observed when the switch resets or when IGMP Snooping is being disabled for the VLAN.

19.5 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. 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 971). 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.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	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. 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. Either one will allow the Proposal-Agreement protocol to be used.
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	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. 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. 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

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.

19.6 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 *edge* 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.

Problem	Solution
send messages to devices in the other VLAN.	

19.7 Firmware Updates

The following describes common errors and possible solutions related to firmware updates. If further assistance is needed, contact Siemens Customer Support.

Error Message	Solution
unknown firmware image file	The firmware image is not valid for the modem installed in the device, or the firmware download is accidentally interrupted. Check the connectivity between the device and the remote server. Make sure the connectivity is reliable.
mis-matched carrier	The new firmware is not targeted to the modem currently installed in the device. Check the firmware file name in the version information file. Make sure the file name has PRI ID of modem installed in the device. Manually download the firmware to the device, then execute qmi-firware-update command to determine what carrier the firmware is targeting. See command and option in (*).
url connection/downloading failure	The device is not able to reach the remote host server based on the URL configuration. Or, the version information file or firmware file is not found on the remote server. Check the URL configuration, and make sure the remote server is reachable. Check the path of the URL configuration. Make sure the new firmware file is in the correct location in the remote server.
invalid firmware information	The version information file name or firmware file name does not exist in server. Check the existence of the version information file name and firmware file name in remote server.
Unspecified error.	Check the syslog for more details.

20 Reference

This chapter provides additional information that may be required to understand and/or configure related features in RUGGEDCOM ROX II.

20.1 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 974).
- **IF-MIB**
  For more information, refer to "IF-MIB" (Page 980).
- **IP-MIB**
  For more information, refer to "IP-MIB" (Page 987).
- **TCP-MIB**
  For more information, refer to "TCP-MIB" (Page 992).
- **UDP-MIB**
  For more information, refer to "UDP-MIB" (Page 995).
- **LLDP-MIB**
  For more information, refer to "LLDP-MIB" (Page 995).
- **Q-BRIDGE-MIB**
  For more information, refer to "Q-BRIDGE-MIB" (Page 1003).
- **RUGGEDCOM-SYS-INFO-MIB**
  For more information, refer to "RUGGEDCOM-SYS-INFO-MIB" (Page 1008).
- **SNMP-FRAMEWORK-MIB**
  For more information, refer to "SNMP-FRAMEWORK-MIB" (Page 1012).
- **SNMP-USER-BASED-SM-MIB**
  For more information, refer to "SNMP-USER-BASED-SM-MIB" (Page 1013).
- **SNMPv2-MIB**
  For more information, refer to "SNMPv2-MIB" (Page 1017).

- **SNMP-VIEW-BASED-ACM-MIB**
  For more information, refer to "SNMP-VIEW-BASED-ACM-MIB" (Page 1019).
- **BGP4-MIB**
  For more information, refer to "BGP4-MIB" (Page 1022).
- **IP-FORWARD-MIB**
  For more information, refer to "IP-FORWARD-MIB" (Page 1022).
- **RFC1213-MIB**
  For more information, refer to "RFC1213-MIB" (Page 1025).
- **PIM-STD-MIB**
  For more information, refer to "PIM-STD-MIB" (Page 1028).
- **MPLS-LDP-STD-MIB**
  For more information, refer to "MPLS-LDP-STD-MIB" (Page 1028).
- **MPLS-LDP-GENERIC-STD-MIB**
  For more information, refer to "MPLS-LDP-GENERIC-STD-MIB" (Page 1029).
- **DS1-MIB**

  For more information, refer to "DS1-MIB" (Page 1029).
- **IEC-62439-2-MIB**
  For more information, refer to "IEC-62439-2-MIB" (Page 1037).

BRIDGE-MIB

Object	Description
dot1dBaseBridgeAddress	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.1 **Description:** 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 BridgeIdentifier is formed, which is used in the Spanning Tree Protocol.
dot1dBaseNumPorts	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.2 **Description:** The number of ports controlled by this bridging entity.
dot1dBaseType	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.3 **Description:** 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.
dot1dBasePort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.4.1.1

Object	Description
	Description: The port number of the port for which this entry contains bridge management information.
dot1dBasePortIfIndex	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.4.1.2 **Description:** The value of the instance of the ifIndex object, defined in IF-MIB, for the interface corresponding to this port.
dot1dBasePortCircuit	**Syntax:** OID **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.4.1.3 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.4.1.4 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.1.4.1.5 **Description:** The number of frames discarded by this port due to an excessive size. It is incremented by both transparent and source route bridges.
dot1dStpProtocolSpecification	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.1 **Description:** 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	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.2 **Description:** 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	**Syntax:** Timeticks

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.17.2.3 **Description:** 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.
dot1dStpTopChanges	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.4 **Description:** The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
dot1dStpDesignatedRoot	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.5 **Description:** 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.
dot1dStpRootCost	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.6 **Description:** The cost of the path to the root as seen from this bridge.
dot1dStpRootPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.7 **Description:** The port number of the port that offers the lowest cost path from this bridge to the root bridge.
dot1dStpMaxAge	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.8 **Description:** 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.
dot1dStpHelloTime	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.9 **Description:** 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.
dot1dStpHoldTime	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.10 **Description:** 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.

Object	Description
dot1dStpForwardDelay	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.11 **Description:** 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.
dot1dStpBridgeMaxAge	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.12 **Description:** 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.
dot1dStpBridgeHelloTime	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.13 **Description:** 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.
dot1dStpBridgeForwardDelay	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.14 **Description:** 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.
dot1dStpPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.1 **Description:** The port number of the port for which this entry contains Spanning Tree Protocol management information.
dot1dStpPortPriority	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.15.1.2 **Description:** 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.

Object	Description
dot1dStpPortState	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.3 **Description:** 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).
dot1dStpPortEnable	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.15.1.4 **Description:** The enabled/disabled status of the port.
dot1dStpPortPathCost	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.2.15.1.5 **Description:** 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.
dot1dStpPortDesignatedRoot	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.6 **Description:** 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.
dot1dStpPortDesignatedCost	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.7 **Description:** 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.
dot1dStpPortDesignatedBridge	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.8 **Description:** The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
dot1dStpPortDesignatedPort	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.9 **Description:** The Port Identifier of the port on the Designated Bridge for this port's segment.
dot1dStpPortForwardTransitions	**Syntax:** Counter32

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.17.2.15.1.10 **Description:** The number of times this port has transitioned from the Learning state to the Forwarding state.
dot1dTpLearnedEntryDiscards	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.4.1 **Description:** 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.
dot1dTpAgingTime	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.4.2 **Description:** The timeout period in seconds for aging out dynamically-learned forwarding information. 802.1D-1998 recommends a default of 300 seconds.
dot1dTpPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.4.4.1.1 **Description:** The port number of the port for which this entry contains Transparent bridging management information.
dot1dTpPortMaxInfo	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.4.4.1.2 **Description:** The maximum size of the INFO (non-MAC) field that this port will receive or transmit.
dot1dTpPortInFrames	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.4.4.1.3 **Description:** 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.
dot1dTpPortOutFrames	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.4.4.1.4 **Description:** 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.
dot1dTpPortInDiscards	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.4.4.1.5

Object	Description
	Description: Count of received valid frames that were discarded (i.e., filtered) by the Forwarding Process.

IF-MIB

Object	Description
ifIndex	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.1 **Description:** 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.
ifDescr	**Syntax:** String **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.2 **Description:** 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.
ifType	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.3 **Description:** 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.
ifSpeed	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.5 **Description:** 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 interace's speed. For a sub-layer which has no concept of bandwidth, this object should be zero.
ifAdminStatus	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.2.2.1.7 **Description:** 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).
ifOperStatus	**Syntax:** Integer **Access:** Read-Only

Object	Description
	OID: .1.3.6.1.2.1.2.2.1.8 **Description:** 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.
ifLastChange	**Syntax:** Timeticks **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.9 **Description:** 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.
ifLinkUpDownTrapEnable	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.31.1.1.1.14 **Description:** 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.
ifConnectorPresent	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.17 **Description:** This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise.
ifHighSpeed	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.15 **Description:** 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.
ifName	**Syntax:** String **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.1 **Description:** 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

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	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.1 **Description:** The number of network interfaces (regardless of their current state) present on this system.
ifAlias	**Syntax:** String **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.18 **Description:** 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.
ifTableLastChange	**Syntax:** Timeticks **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.5 **Description:** 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.
ifHCInUcastPkts	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.7 **Description:** 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.
ifHCInBroadcastPkts	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.9 **Description:** 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.

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	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.12 **Description:** 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.
ifHCInOctets	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.6 **Description:** 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.
ifInOctets	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.10 **Description:** 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.
ifInErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.14 **Description:** 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.
ifMtu	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.4 **Description:** 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.
ifInBroadcastPkts	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.3 **Description:** 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.

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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.17 **Description:** 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.
ifOutBroadcastPkts	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.5 **Description:** 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.
ifPromiscuousMode	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.16 **Description:** 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.
ifHCInMulticastPkts	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.8 **Description:** 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.
ifHCOutUcastPkts	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.11 **Description:** 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.

Object	Description
ifHCOutBroadcastPkts	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.13 **Description:**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.
ifHCOutOctets	**Syntax:** Counter64 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.10 **Description:** 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.
ifOutOctets	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.16 **Description:** 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.
ifOutErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.20 **Description:** 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.
ifInUcastPkts	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.11 **Description:** 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.
ifInDiscards	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.13 **Description:** 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

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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.4 **Description:** 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.
ifOutDiscards	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.19 **Description:** 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.
ifInUnknownProtos	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.2.2.1.15 **Description:** 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.
ifInMulticastPkts	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.2 **Description:** 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.
ifCounterDiscontinuityTime	**Syntax:** Timeticks **Access:** Read-Only **OID:** .1.3.6.1.2.1.31.1.1.1.19 **Description:** 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

Object	Description
	such discontinuities have occurred since the last re- initialization of the local management subsystem, then this object contains a zero value.
linkUp	**OID:** .1.3.6.1.6.3.1.1.5.4 **Description:** 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	**OID:** .1.3.6.1.6.3.1.1.5.3 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.1 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.4 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.6 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only

Object	Description
	OID: .1.3.6.1.2.1.4.8 **Description:** 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.
ipOutDiscards	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.11 **Description:** 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.
ipReasmTimeout	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.13 **Description:** The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
ipReasmFails	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.16 **Description:** 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.
ipFragFails	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.18 **Description:** 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.
ipAdEntAddr	**Syntax:** IpAddress **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.20.1.1 **Description:** The IPv4 address to which this entry's addressing information pertains.
ipAdEntBcastAddr	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.20.1.4

Object	Description
	Description: 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.
ipNetToMediaIfIndex	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.22.1.1 **Description:** 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'.
ipNetToMediaNetAddress	**Syntax:** IpAddress **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.22.1.3 **Description:** 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'.
ipRoutingDiscards	**OID:** .1.3.6.1.2.1.4.23
ipDefaultTTL	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.4.2 **Description:** 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.
ipInAddrErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.5 **Description:** 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.
ipInUnknownProtos	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.7 **Description:** The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Object	Description
	This object has been deprecated, as a new IP version-neutral table has been added. It is loosely replaced by ipSystemStatsInUnknownProtos.
ipInDelivers	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.9 **Description:** 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.
ipOutNoRoutes	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.12 **Description:** 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.
ipReasmReqds	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.14 **Description:** 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.
ipFragOKs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.17 **Description:** 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.
ipFragCreates	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.19 **Description:** 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.
ipAdEntIfIndex	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.20.1.2 **Description:** 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.
ipAdEntReasmMaxSize	**Syntax:** Integer

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.4.20.1.5 **Description:** The size of the largest IPv4 datagram which this entity can re-assemble from incoming IPv4 fragmented datagrams received on this interface.
ipNetToMediaPhysAddress	**Syntax:** String **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.22.1.2 **Description:** 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.
ipNetToMediaType	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.22.1.4 **Description:** 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.
ipInReceives	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.3 **Description:** 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 ipSystemStatsInRecieves.
ipOutRequests	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.10 **Description:** 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.
ipReasmOKs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.15

Object	Description
	Description: 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	**Syntax:** IpAddress **Access:** Read-Only **OID:** .1.3.6.1.2.1.4.20.1.3 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.1 **Description:** The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.2 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.4 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.6 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.8 **Description:** 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	**Syntax:** Counter32

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.6.11 **Description:** 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.
tcpConnLocalAddress	**Syntax:** IpAddress **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.13.1.2 **Description:** 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.
tcpConnRemAddress	**Syntax:** IpAddress **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.13.1.4 **Description:** The remote IP address for this TCP connection.
tcpInErrs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.14 **Description:** 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.
tcpRtoMax	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.3 **Description:** 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).
tcpActiveOpens	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.5 **Description:** 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.
tcpAttemptFails	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.7 **Description:** 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.
tcpCurrEstab	**Syntax:** Gauge32

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.6.9 **Description:** The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
tcpRetransSegs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.12 **Description:** 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.
tcpConnLocalPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.13.1.3 **Description:** The local port number for this TCP connection.
tcpConnRemPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.13.1.5 **Description:** The remote port number for this TCP connection.
tcpOutRsts	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.15 **Description:** 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.
tcpInSegs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.17 **Description:** 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.
tcpConnState	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.6.13.1.1 **Description:** 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).

UDP-MIB

Object	Description
udpInDatagrams	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.7.1 **Description:** 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.
udpNoPorts	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.7.2 **Description:** 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.
udpInErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.7.3 **Description:** 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.
udpLocalAddress	**Syntax:** IpAddress **Access:** Read-Only **OID:** .1.3.6.1.2.1.7.5.1.1 **Description:** 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.
udpOutDatagrams	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.7.4 **Description:** 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.
udpLocalPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.7.5.1.2 **Description:** The local port number for this UDP listener.

LLDP-MIB

Object	Description
lldpPortConfigAdminStatus	**Syntax:** Integer **Access:** Read-Write

Object	Description
	OID: .1.0.8802.1.1.2.1.1.6.1.2 **Description:** The administratively desired status of the local LLDP agent. If the associated lldpPortConfigAdminStatus 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 lldpPortConfigAdminStatus 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 lldpPortConfigAdminStatus object has a value of 'txAndRx(3)', then the LLDP agent will transmit and receive LLDP frames on this port. If the associated lldpPortConfigAdminStatus 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 lldpPortConfigAdminStatus becomes disabled, then the information will naturally age out.
lldpNotificationInterval	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.1.5 **Description:** This object controls the transmission of LLDP notifications. the agent must not generate more than one lldpRemTablesChange 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 lldpRemoteSystemsData 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 lldpStatsRemTableLastChangeTime to detect any missed lldpRemTablesChange 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.
lldpPortConfigNotificationEnable	**Syntax:** Integer **Access:** Read-Write **OID:** .1.0.8802.1.1.2.1.1.6.1.3 **Description:** The lldpPortConfigNotificationEnable 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.
lldpMessageTxInterval	**Syntax:** Integer **Access:** Read-Write **OID:** .1.0.8802.1.1.2.1.1.1 **Description:** The interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value for lldpMessageTxInterval object is 30 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.
lldpMessageTxHoldMultiplier	**Syntax:** Integer **Access:** Read-Write **OID:** .1.0.8802.1.1.2.1.1.2 **Description:** The time-to-live value expressed as a multiple of the lldpMessageTxInterval 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: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) For example, if the value of

Object	Description
	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.
lldpReinitDelay	**Syntax:** Integer **Access:** Read-Write **OID:** .1.0.8802.1.1.2.1.1.3 **Description:** 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 lldpReintDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.
lldpTxDelay	**Syntax:** Integer **Access:** Read-Write **OID:** .1.0.8802.1.1.2.1.1.4 **Description:** 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: `1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval)` 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.
lldpPortConfigTLVsTxEnable	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.1.6.1.4 **Description:** 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.
lldpConfigManAddrPortsTxEnable	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.1.7.1.1 **Description:** 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.
lldpStatsRemTablesLastChangeTime	**Syntax:** Timeticks **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.1 **Description:** 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

Object	Description
	associated with remote systems. An NMS can use this object to reduce polling of the lldpRemoteSystemsData objects.
lldpStatsRemTablesInserts	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.2 **Description:** The number of times the complete set of information advertised by a particular MSAP has been inserted into tables contained in lldpRemoteSystemsData and lldpExtensions 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 lldpStatsRemTablesInserts since the insert is not completed yet or or in lldpStatsRemTablesDeletes, since the deletion would only be a partial deletion. If the failure was the result of lack of resources, the lldpStatsRemTablesDrops counter should be incremented once.
lldpStatsRemTablesDeletes	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.3 **Description:** 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. 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.
lldpStatsRemTablesDrops	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.4 **Description:** The number of times the complete set of information advertised by a particular MSAP could not be entered into tables contained in lldpRemoteSystemsData and lldpExtensions objects because of insufficient resources.
lldpStatsRemTablesAgeouts	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.5 **Description:** 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 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.
lldpStatsRxPortFramesDiscardedTotal	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.7.1.2

Object	Description
	Description: 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 formating 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.
lldpStatsRxPortFramesErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.7.1.3 **Description:** The number of invalid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
lldpStatsRxPortFramesTotal	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.7.1.4 **Description:** The number of valid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
lldpStatsRxPortTLVsDiscardedTotal	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.7.1.5 **Description:** The number of LLDP TLVs discarded for any reason by this LLDP agent on the indicated port.
lldpStatsRxPortTLVsUnrecognizedTotal	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.7.1.6 **Description:** 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.
lldpStatsRxPortAgeoutsTotal	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.2.7.1.7 **Description:** 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.
lldpStatsTxPortFramesTotal	**Syntax:** Counter32

Object	Description
	Access: Read-Only **OID:** .1.0.8802.1.1.2.1.2.6.1.2 **Description:** 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.
lldpLocChassisIdSubtype	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.1 **Description:** The type of encoding used to identify the chassis associated with the local system.
lldpLocChassisId	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.2 **Description:** The string value used to identify the chassis component associated with the local system.
lldpLocPortIdSubtype	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.7.1.2 **Description:** The type of port identifier encoding used in the associated 'lldpLocPortId' object.
lldpLocPortId	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.7.1.3 **Description:** The string value used to identify the port component associated with a given port in the local system.
lldpLocPortDesc	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.7.1.4 **Description:** 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.
lldpLocSysDesc	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.4 **Description:** 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.
lldpLocSysName	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.3 **Description:** 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.
lldpLocSysCapSupported	**Syntax:** Hex-String

Object	Description
	Access: Read-Only **OID:** .1.0.8802.1.1.2.1.3.5 **Description:** The bitmap value used to identify which system capabilities are supported on the local system.
lldpLocSysCapEnabled	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.6 **Description:** The bitmap value used to identify which system capabilities are enabled on the local system.
lldpLocManAddrLen	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.8.1.3 **Description:** 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 adress.
lldpLocManAddrIfSubtype	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.8.1.4 **Description:** The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the local system.
lldpLocManAddrIfId	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.3.8.1.5 **Description:** The integer value used to identify the interface number regarding the management address component associated with the local system.
lldpLocManAddrOID	**Syntax:** OID **Access:** Read-Only **OID:** 1.0.8802.1.1.2.1.3.8.1.6 **Description:** 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.
lldpRemChassisIdSubtype	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.4 **Description:** The type of encoding used to identify the chassis associated with the remote system.
lldpRemChassisId	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.5 **Description:** The string value used to identify the chassis component associated with the remote system.

Object	Description
lldpRemPortIdSubtype	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.6 **Description:** The type of port identifier encoding used in the associated 'lldpRemPortId' object.
lldpRemPortId	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.7 **Description:** The string value used to identify the port component associated with the remote system.
lldpRemPortDesc	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.8 **Description:** The string value used to identify the description of the given port associated with the remote system.
lldpRemSysName	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.9 **Description:** The string value used to identify the system name of the remote system.
lldpRemSysDesc	**Syntax:** String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.10 **Description:** The string value used to identify the system description of the remote system.
lldpRemSysCapSupported	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.11 **Description:** The bitmap value used to identify which system capabilities are supported on the remote system.
lldpRemSysCapEnabled	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.1.1.12 **Description:** The bitmap value used to identify which system capabilities are enabled on the remote system.
lldpRemManAddrIfSubtype	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.2.1.3 **Description:** The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system.
lldpRemManAddrIfId	**Syntax:** Integer **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.2.1.4

Object	Description
	Description: The integer value used to identify the interface number regarding the management address component associated with the remote system.
lldpRemManAddrOID	**Syntax:** OID **Access:** Read-Only **OID:** .1.0.8802.1.1.2.1.4.2.1.5 **Description:** 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.
lldpRemUnknownTLVInfo	**OID:** .1.0.8802.1.1.2.1.4.3.1.2 **Description:** This object represents the value extracted from the value field of the TLV.
lldpRemOrgDefInfo	**OID:** .1.0.8802.1.1.2.1.4.4.1.4 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.1.1 **Description:** The version number of IEEE 802.1Q that this device supports.
dot1qMaxVlanId	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.1.2 **Description:** The maximum IEEE 802.1Q VLAN-ID that this device supports.
dot1qMaxSupportedVlans	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.1.3 **Description:** The maximum number of IEEE 802.1Q VLANs that this device supports.
dot1qNumVlans	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.1.4 **Description:** The current number of IEEE 802.1Q VLANs that are configured in this device.
dot1qGvrpStatus	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.1.5 **Description:** 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

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	**OID:** .1.3.6.1.2.1.17.7.1.4.1 **Syntax:** Counter32 **Access:** Read-Only **Description:** 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.
dot1qVlanFdbId	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.3 **Description:** 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.
dot1qVlanCurrentEgressPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.4 **Description:** The set of ports that are transmitting traffic for this VLAN as either tagged or untagged frames.
dot1qVlanCurrentUntaggedPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.5 **Description:** The set of ports that are transmitting traffic for this VLAN as untagged frames.
dot1qVlanStatus	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.6 **Description:** 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.
dot1qVlanCreationTime	**Syntax:** Timeticks **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.7 **Description:** The value of sysUpTime when this VLAN was created.
dot1qVlanStaticName	**Syntax:** String **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.1 **Description:** An administratively assigned string, which may be used to identify the VLAN.
dot1qVlanStaticEgressPorts	**Syntax:** Hex-String

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.2 **Description:** 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.
dot1qVlanForbiddenEgressPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.3 **Description:** 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.
dot1qVlanStaticUntaggedPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.4 **Description:** 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.
dot1qVlanStaticRowStatus	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.5 **Description:** This object indicates the status of this entry.
dot1qNextFreeLocalVlanIndex	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.4 **Description:** The next available value for dot1qVlanIndex of a local VLAN entry in dot1qVlanStaticTable. This will report values >=4096 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.
dot1qPvid	**Syntax:** Gauge32

Object	Description
	Access: Read-Write **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.1 **Description:** 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.
dot1qPortAcceptableFrameTypes	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.2 **Description:** 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.
dot1qPortIngressFiltering	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.3 **Description:** 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.
dot1qPortGvrpStatus	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.4 **Description:** 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.
dot1qFdbDynamicCount	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.1.1.2 **Description:** A collection of objects providing information about all unicast addresses, learned dynamically or statically configured by management, in each Filtering Database.
dot1qTpFdbPort	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.2.1.2 **Description:** 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

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	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.2.1.3 **Description:** The status of this entry. The meanings of the values are: • 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. • 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. • learned(3) - the value of the corresponding instance of dot1qTpFdbPort was learned and is being used. • 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. • mgmt(5) - the value of the corresponding instance of dot1qTpFdbAddress is also the value of an existing instance of dot1qStaticAddress.
dot1qTpGroupEgressPorts	**OID:** .1.3.6.1.2.1.17.7.1.2.3.1.2 **Description:** 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.
dot1qTpGroupLearnt	**OID:** .1.3.6.1.2.1.17.7.1.2.3.1.3 **Description:** The subset of ports in dot1qTpGroupEgressPorts that were learned by GMRP or some other dynamic mechanism, in this Filtering database.
dot1qForwardAllPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.4.1.1 **Description:** 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.
dot1qForwardAllStaticPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.4.1.2 **Description:** 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

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	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.4.1.3 **Description:** 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.
dot1qForwardUnregisteredPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.5.1.1 **Description:** 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.
dot1qForwardUnregisteredStaticPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.5.1.2 **Description:** 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.
dot1qForwardUnregisteredForbiddenPorts	**Syntax:** Hex-String **Access:** Read-Only **OID:** .1.3.6.1.2.1.17.7.1.2.5.1.3 **Description:** 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.

RUGGEDCOM-SYS-INFO-MIB

Object	Description
rcDeviceErrBootupError	**Syntax:** String

Object	Description
	Access: Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.1 **Description:** The error discovered during bootup process. If there was no error during device bootup, zero length string will be retreived.
rcDeviceErrWatchdogReset	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.2 **Description:** Indicates whether the last device reboot was caused by wachdog.
rcDeviceErrConfigurationFailure	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.3 **Description:** Indicates whether errors were detected while applying configuration settings from configuration file. Configuration is updated from the configureation 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.
rcDeviceErrCrashLogCreated	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.4 **Description:** 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.
rcDeviceErrStackOverflow	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.5 **Description:** 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.
rcDeviceErrHeapError	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.6 **Description:** 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.
rcDeviceErrDateAndTimeSetFailed	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.7 **Description:** Indicates whether the date and time setting in the device falied. Whenever the value of this object changes from false(2) to true(1), the device will generate genericTrap notification.
rcDeviceErrNtpServerUnreachable	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.8

Object	Description
	Description: 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.9 **Description:** Indicates whether the the file was transfered 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.10 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.1.11 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.2.3 **Description:** The temperature measured in the device.
rcDeviceStsPowerSupply1	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.2.4 **Description:** Indicates the status of Power Supply Module 1. Whenever the value of this object changes from functional(2) to notFunctional(3), or from notFunctionl(3) to functional(2), the device will generate powerSupplyTrap notification.
rcDeviceStsPowerSupply2	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.2.5 **Description:** Indicates the status of Power Supply Module 2. Whenever the value of this object changes from functional(2) to notFunctional(3), or from notFunctionl(3) to functional(2), the device will generate powerSupplyTrap notification.
rcDeviceInfoMainBoardType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.4 **Description:** The identification code of the device main board.
rcDeviceInfoTotalRam	**Syntax:** Integer **Access:** Read-Only

Object	Description
	OID: 1.3.6.1.4.1.15004.4.2.3.5 **Description:** The total number of bytes of RAM in the system control CPU.
rcDeviceInfoBootSwVersion	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.2 **Description:** 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	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.3 **Description:** 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	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.6 **Description:** 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	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.7 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.8 **Description:** 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	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.3.1 **Description:** The manufacturing serial number of the device.
rcDeviceCommReset	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.4.1

Object	Description
	Description: 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.4.1.15004.4.2.4.2 **Description:** 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	**Syntax:** Integer **Access:** Read-Write **OID:** 1.3.6.1.4.1.15004.4.2.4.3 **Description:** 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	**Syntax:** Integer **Access:** Read-Write **OID:** 1.3.6.1.4.1.15004.4.2.4.4 **Description:** 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	**Syntax:** Integer **Access:** Read-Write **OID:** 1.3.6.1.4.1.15004.4.2.4.5 **Description:** 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)'.

SNMP-FRAMEWORK-MIB

Object	Description
snmpEngineID	**Syntax:** Hex-String **Access:** Read-Only **OID:** 1.3.6.1.6.3.10.2.1.1 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.10.2.1.2 **Description:** The number of times that the SNMP engine has (re-)initialized itself since snmpEngineID was last configured.
snmpEngineTime	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.10.2.1.3 **Description:** The number of seconds since the value of the snmpEngineBoots object last changed. When incrementing this object's

Object	Description
	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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.10.2.1.4 **Description:** 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	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.1.1 **Description:** 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.
usmStatsNotInTimeWindows	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.1.2 **Description:** The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
usmStatsUnknownUserNames	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.1.3 **Description:** 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.
usmStatsUnknownEngineIDs	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.1.4 **Description:** 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.
usmStatsWrongDigests	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.1.5 **Description:** The total number of packets received by the SNMP engine which were dropped because they didn't contain the expected digest value.
usmStatsDecryptionErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.1.6

Object	Description
	Description: The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.
usmUserSpinLock	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.1 **Description:** An advisory lock used to allow several cooperating Command Generator Applications to coordinate their use of facilities to alter secrets in the usmUserTable.
usmUserSecurityName	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.3 **Description:** 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.
usmUserCloneFrom	**Syntax:** OID **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.4 **Description:** 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.
usmUserAuthProtocol	**Syntax:** OID **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.5 **Description:** 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

Object	Description
	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.
usmUserAuthKeyChange	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.6 **Description:** 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 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.
usmUserOwnAuthKeyChange	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.7 **Description:** 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 umsUserName 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.
usmUserPrivProtocol	**Syntax:** OID **Access:** Read-Only

Object	Description
	OID: 1.3.6.1.6.3.15.1.2.2.1.8 **Description:** 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 the corresponding instance of usmUserAuthProtocol cannot have a value of usmNoAuthProtocol. If it does, then an 'inconsistentValue' error must be returned.
usmUserPrivKeyChange	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.9 **Description:** 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.
usmUserOwnPrivKeyChange	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.10 **Description:** 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 umsUserName 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.
usmUserPublic	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.11

Object	Description
	Description: 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.
usmUserStorageType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.12 **Description:** 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 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.15.1.2.2.1.13 **Description:** 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.

SNMPv2-MIB

Object	Description
snmpInPkts	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.1 **Description:** The total number of messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.3

Object	Description
	Description: The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
snmpInASNParseErrs	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.6 **Description:** The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpSilentDrops	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.31 **Description:** 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 was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.32 **Description:** 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.
snmpEnableAuthenTraps	**Syntax:** Integer **Access:** Read-Write **OID:** 1.3.6.1.2.1.11.30 **Description:** 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.
snmpInBadCommunityNames	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.4 **Description:** 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.

Object	Description
snmpInBadCommunityUses	**Syntax:** Counter32 **Access:** Read-Only **OID:** 1.3.6.1.2.1.11.5 **Description:** A collection of objects providing basic instrumentation of a SNMP entity which supports community-based authentication.
snmpSetSerialNo	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.1.1.6.1 **Description:** 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.

SNMP-VIEW-BASED-ACM-MIB

Object	Description
vacmContextName	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.1.1.1 **Description:** A human readable name identifying a particular context at a particular SNMP entity. The empty contextName (zero length) represents the default context.
vacmGroupName	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.2.1.3 **Description:** 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 vacmAccesTable.
vacmSecurityToGroupStorageType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.2.1.4 **Description:** 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.
vacmSecurityToGroupStatus	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.2.1.5 **Description:** 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

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.
vacmAccessContextMatch	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.4.1.4 **Description:** 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.
vacmAccessReadViewName	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.4.1.5 **Description:** 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 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	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.4.1.6 **Description:** 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.
vacmAccessNotifyViewName	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.4.1.7 **Description:** 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.
vacmAccessStorageType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.4.1.8 **Description:** 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.
vacmAccessStatus	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.4.1.9 **Description:** The status of this conceptual row. The RowStatus TC [RFC2579] requires that this DESCRIPTION clause states under which circumstances

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.
vacmViewSpinLock	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.5.1 **Description:** 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.
vacmViewTreeFamilyMask	**Syntax:** String **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.5.2.1.3 **Description:** 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.

Object	Description
vacmViewTreeFamilyType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.5.2.1.4 **Description:** 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.
vacmViewTreeFamilyStorageType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.5.2.1.5 **Description:** 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.
vacmViewTreeFamilyStatus	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.6.3.16.1.5.2.1.6 **Description:** 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.

BGP4-MIB

Object	Description
bgpVersion	**Syntax:** Hex-String **Access:** Read-Only **OID:** 1.3.6.1.2.1.15.1 **Description:** 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, is present and set, then the version (i+1) of the BGP is supported.
bgpLocalAs	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.15.2 **Description:** The local autonomous system number.
bgpIdentifier	**Syntax:** IpAddress **Access:** Read-Only **OID:** 1.3.6.1.2.1.15.4 **Description:** The BGP Identifier of the local system.

IP-FORWARD-MIB

Object	Description
ipCidrRouteNumber	**Syntax:** Gauge32

Object	Description
	Access: Read-Only **OID:** 1.3.6.1.2.1.4.24.3 **Description:** The number of current ipCidrRouteTable entries that are not invalid. This object is deprecated in favor of inetCidrRouteNumber and the inetCidrRouteTable.
ipCidrRouteDest	**Syntax:** IpAddress **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.1 **Description:** 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 x must be rejected if the bitwise logical-AND of x with the value of the corresponding instance of the ipCidrRouteMask object is not equal to x.
ipCidrRouteNextHop	**Syntax:** IpAddress **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.4 **Description:** On remote routes, the address of the next system en route; Otherwise, 0.0.0.0.
ipCidrRouteType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.6 **Description:** 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	**Syntax:** OID **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.9 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.11 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.13

Object	Description
	Description: 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.15 **Description:** 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	**Syntax:** IpAddress **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.2 **Description:** 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 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.3 **Description:** 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.
ipCidrRouteIfIndex	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.5 **Description:** The ifIndex value that identifies the local interface through which the next hop of this route should be reached.
ipCidrRouteProto	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.7 **Description:** 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.
ipCidrRouteAge	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.8 **Description:** 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.
ipCidrRouteNextHopAS	**Syntax:** Integer **Access:** Read-Only

Object	Description
	OID: 1.3.6.1.2.1.4.24.4.1.10 **Description:** 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.
ipCidrRouteMetric2	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.12 **Description:** 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.
ipCidrRouteMetric4	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.14 **Description:** 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	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.4.24.4.1.16 **Description:** The row status variable, used according to row installation and removal conventions.

RFC1213-MIB

Object	Description
icmpInMsgs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.1 **Description:** The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
icmpInDestUnreachs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.3 **Description:** The number of ICMP Destination Unreachable messages received.
icmpInParmProbs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.5 **Description:** The number of ICMP Parameter Problem messages received.
icmpInRedirects	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.7

Object	Description
	Description: The number of ICMP Redirect messages received.
icmpInEchoReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.9 **Description:** The number of ICMP Echo Reply messages received.
icmpInTimestampReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.11 **Description:** The number of ICMP Timestamp Reply messages received.
icmpInAddrMaskReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.13 **Description:** The number of ICMP Address Mask Reply messages received.
icmpOutErrors	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.15 **Description:** 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.
icmpOutTimeExcds	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.17 **Description:** The number of ICMP Time Exceeded messages sent.
icmpOutSrcQuenchs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.19 **Description:** The number of ICMP Source Quench messages sent.
icmpOutEchos	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.21 **Description:** The number of ICMP Echo (request) messages sent.
icmpOutTimestamps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.23 **Description:** The number of ICMP Timestamp (request) messages sent.
icmpOutAddrMaskReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.26 **Description:** The number of ICMP Address Mask Reply messages sent.
icmpInErrors	**Syntax:** Counter32 **Access:** Read-Only

Object	Description
	OID: .1.3.6.1.2.1.5.2 **Description:** The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
icmpInTimeExcds	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.4 **Description:** The number of ICMP Time Exceeded messages received.
icmpInSrcQuenchs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.6 **Description:** The number of ICMP Source Quench messages received.
icmpInEchos	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.8 **Description:** The number of ICMP Echo (request) messages received.
icmpInTimestamps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.10 **Description:** The number of ICMP Timestamp (request) messages received.
icmpInAddrMasks	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.12 **Description:** The number of ICMP Address Mask Request messages received.
icmpOutMsgs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.14 **Description:** The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
icmpOutDestUnreachs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.16 **Description:** The number of ICMP Destination Unreachable messages sent.
icmpOutParmProbs	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.18 **Description:** The number of ICMP Parameter Problem messages sent.
icmpOutRedirects	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.20 **Description:** The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

Object	Description
icmpOutEchoReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5 **Description:** The number of ICMP Echo Reply messages sent.
icmpOutTimestampReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.24 **Description:** The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMaskReps	**Syntax:** Counter32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.5.26 **Description:** The number of ICMP Address Mask Reply messages sent.

PIM-STD-MIB

Object	Description
pimInterfaceAddressType	**Syntax:** IpAddress **Access:** Read-Only **OID:** 1.3.6.1.2.1.157.1.1.1.3 **Description:** The address type of this PIM interface.
pimInterfaceAddress	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.157.1.1.1.4 **Description:** The primary IP address of this router on this PIM interface. The InetAddressType is given by the pimInterfaceAddressType object.
pimInterfaceStorageType	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.157.1.1.1.28 **Description:** The storage type for this row. Rows having the value 'permanent' need not allow write-access to any columnar objects in the row.

MPLS-LDP-STD-MIB

Object	Description
mplsLdpLsrId	**Syntax:** IpAddress **Access:** Read-Only **OID:** 1.3.6.1.2.1.10.166.4.1.1.1 **Description:** A indication of whether this Label Switching Router supports loop detection. • none(1) -- Loop Detection is not supported on this LSR. • other(2) -- Loop Detection is supported but by a method other than those listed below. • hopCount(3) -- Loop Detection is supported by Hop Count only.

Object	Description
	• pathVector(4) -- Loop Detection is supported by Path Vector only. • hopCountAndPathVector(5) -- Loop Detection is supported by both Hop Count And Path Vector. 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.

MPLS-LDP-GENERIC-STD-MIB

Object	Description
mplsLdpEntityGenericLabelSpace	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.10.166.7.1.1.1.1.3 **Description:** 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.

DS1-MIB

Object	Description
ds1	**OID:** 1.3.6.1.2.1.10.18
dsx1LineIndex	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.10.18.6.1.1 **Description:** This object should be made equal to ifIndex. The next paragraph describes its previous usage. Making the object equal to ifIndex allows proper use of the ifStackTable and ds0/ds0bundle MIBs. Previously, this object was the identifier of a DS1 interface on a managed device. If there is an ifEntry that is directly associated with this and only this DS1 interface, it should have the same value as ifIndex. Otherwise, number the dsx1LineIndices with a unique identifier following the rules of choosing a number that is greater than ifNumber and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g., network side) with odd numbers.
dsx1IfIndex	**Syntax:** Integer **Access:** Read-Only **OID:** 1.3.6.1.2.1.10.18.6.1.2 **Description:** This value for this object is equal to the value of ifIndex from the Interfaces table (RFC 2863).
dsx1TimeElapsed	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.3 **Description:** This value for this object is equal to the value of ifIndex from the Interfaces table (RFC 2863).
dsx1ValidIntervals	**Syntax:** Integer **Access:** Read-Only

Object	Description
	OID: .1.3.6.1.2.1.10.18.6.1.4 **Description:** The number of previous near-end intervals for which data was collected. The value will be 96 unless the interface was brought online within the last 24 hours, in which case the value will be the number of complete 15-minute near-end intervals since the interface has been online. In the case where the agent is a proxy, it is possible that some intervals are unavailable. In this case, this interval is the maximum interval number for which data is available.
dsx1LineType	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.5 **Description:** Line type for T1 ISDN Primary Rate interfaces.
dsx1LineCoding	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.6 **Description:** Type of Zero Code Suppression for T1 ISDN Primary Rate interfaces.
dsx1SendCode	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.7 **Description:** This variable indicates what type of code is being sent across the DS1 interface by the device. Setting this variable causes the interface to send the code requested. The values mean the following: • dsx1SendNoCode: sending looped or normal data • dsx1SendLineCode: sending a request for a line loopback • dsx1SendPayloadCode: sending a request for a payload loopback • dsx1SendResetCode: sending a loopback termination request • dsx1SendQRS: sending a Quasi-Random Signal (QRS) test pattern • dsx1Send511Pattern: sending a 511-bit fixed test pattern • dsx1Send3in24Pattern: sending a fixed test pattern of 3 bits set in 24 • dsx1SendOtherTestPattern: sending a test pattern other than those described by this object
dsx1CircuitIdentifier	**Syntax:** String **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.8 **Description:** This variable contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.
dsx1LoopbackConfig	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.9 **Description:** This variable represents the desired loopback configuration of the DS1 interface. Agents supporting read/write access should return inconsistentValue in response to a requested loopback state that the interface does not support. The values mean: • dsx1NoLoop: not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as its value.

Object	Description
	• dsx1PayloadLoop: the received signal at this interface is looped through the device. Typically, the received signal is looped back for retransmission after it has passed through the device's framing function. • dsx1LineLoop: the received signal at this interface does not go through the device (minimum penetration) but is looped back out. • dsx1OtherLoop: loopbacks that are not defined here. • dsx1InwardLoop: the transmitted signal at this interface is looped back and received by the same interface. What is transmitted onto the line is product dependent. • dsx1DualLoop both dsx1LineLoop and dsx1InwardLoop will be active simultaneously.
dsx1LineStatus	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.10 **Description:** This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarms information. The dsx1LineStatus is a bitmap represented as a sum; therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are as follows: • 1 dsx1NoAlarm No alarm present • 2 dsx1RcvFarEndLOF Far end LOF (a.k.a. Yellow Alarm) • 4 dsx1XmtFarEndLOF Near end sending LOF indication • 8 dsx1RcvAIS Far end sending AIS • 16 dsx1XmtAIS Near end sending AIS • 32 dsx1LossOfFrame Near end LOF (a.k.a. Red Alarm) • 64 dsx1LossOfSignal Near end Loss of Signal • 128 dsx1LoopbackState Near end is looped • 256 dsx1T16AIS E1 TS16 AIS • 512 dsx1RcvFarEndLOMF Far end sending TS16 LOMF • 1024 dsx1XmtFarEndLOMF Near end sending TS16 LOMF • 2048 dsx1RcvTestCode Near end detects a test code • 4096 dsx1OtherFailure Any line status not defined here • 8192 dsx1UnavailSigState Near end in unavailable signal state • 16384 dsx1NetEquipOOS Carrier equipment out of service • 32768 dsx1RcvPayloadAIS DS2 payload AIS • 65536 dsx1Ds2PerfThreshold DS2 performance threshold exceeded
dsx1SignalMode	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.11 **Description:** 'none' indicates that no bits are reserved for signaling on this channel. 'robbedBit' indicates that DS1 Robbed Bit Signaling is in use. 'bitOriented' indicates that E1 Channel Associated Signaling is in use. 'messageOriented' indicates that Common Channel Signaling is in use on either channel 16 of an E1 link or channel 24 of a DS1.
dsx1TransmitClockSource	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.12

Object	Description
	Description: The source of transmit clock. • 'loopTiming' indicates that the recovered receive clock is used as the transmit clock. • 'localTiming' indicates that a local clock source is used or when an external clock is attached to the box containing the interface. • 'throughTiming' indicates that recovered receive clock from another interface is used as the transmit clock. • 'adaptive' indicates that the clock is recovered based on the data flow and not based on the physical layer
dsx1Fdl	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.13 **Description:** This bitmap describes the use of the facilities data link and is the sum of the capabilities. Set any bits that are appropriate: other(1), dsx1AnsiT1403(2), dsx1Att54016(4), dsx1FdlNone(8) 'other' indicates that a protocol other than one of the following is used. 'dsx1AnsiT1403' refers to the FDL exchange recommended by ANSI.'dsx1Att54016' refers to ESF FDL exchanges. 'dsx1FdlNone' indicates that the device does not use the FDL.
dsx1InvalidIntervals	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.14 **Description:** The number of intervals in the range from 0 to dsx1ValidIntervals for which no data is available. This object will typically be zero except in cases where the data for some intervals is not available (e.g., in proxy situations).
dsx1LineLength	**Syntax:** Integer **Access:** Read-Write **OID:** .1.3.6.1.2.1.10.18.6.1.15 **Description:** The length of the DS1 line in meters. This object provides information for line build-out circuitry. This object is only useful if the interface has configurable line build-out circuitry.
dsx1LineStatusLastChange	**Syntax:** Timeticks **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.16 **Description:** The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then this object contains a zero value.
dsx1LineStatusChangeTrapEnable	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.17 **Description:** Indicates whether dsx1LineStatusChange traps should be generated for this interface.
dsx1LoopbackStatus	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.18 **Description:** This variable represents the current state of the loopback on the DS1 interface. It contains information about loopbacks established by

Object	Description
	a manager and remotely from the far end. The dsx1LoopbackStatus is a bitmap represented as a sum; therefore, it can represent multiple loopbacks simultaneously. The various bit positions are as follows: • 1 dsx1NoLoopback • 2 dsx1NearEndPayloadLoopback • 4 dsx1NearEndLineLoopback • 8 dsx1NearEndOtherLoopback • 16 dsx1NearEndInwardLoopback • 32 dsx1FarEndPayloadLoopback • 64 dsx1FarEndLineLoopback
dsx1Ds1ChannelNumber	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.19 **Description:** This variable represents the channel number of the DS1/E1 on its parent DS2/E2 or DS3/E3. A value of 0 indicates that this DS1/E1 does not have a parent DS3/E3.
dsx1Channelization	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.20 **Description:** Indicates whether this DS1/E1 or DS2 is channelized or unchannelized. The value of enabledDs0(2) indicates that this is a DS1 channelized into DS0s. Setting this value will cause the creation, and resetting it to disabled(1) will cause the deletion of entries in the ifTable for the DS0s that are within the DS1. The value of enabledDs1(3) indicates that this is a DS2 channelized into DS1s. Setting this value will cause the creation, and resetting it to disabled(1) will cause the deletion of entries in the ifTable for the DS1s that are within the DS2.
dsx1LineMode	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.21 **Description:** This setting puts the T1 framer into either long-haul (CSU) mode or short-haul (DSU) mode.
dsx1LineBuildOut	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1 **Description:** Attenuation setting for T1 framer in long haul (CSU) mode. The optional values are -7.5dB, -15dB, -22.5dB, and 0dB.
dsx1LineImpedance	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.6.1.23 **Description:** Nominal line impedance. For T1 and J1 lines, the value is typically balanced100ohms(3). For E1 lines, the value is typically unbalanced75ohms(2) and balanced120ohms(4). When this object does not apply, or when the appropriate value is not known, the value should be set to notApplicable(1).
dsx1CurrentIndex	**Syntax:** Integer **Access:** Read-Only

Object	Description
	OID: .1.3.6.1.2.1.10.18.7.1.1 **Description:** The index value that uniquely identifies the DS1 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 as a dsx1LineIndex object instance.
dsx1CurrentESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.2 **Description:** The number of Errored Seconds.
dsx1CurrentSESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.3 **Description:** The number of Severely Errored Seconds.
dsx1CurrentSEFSs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.4 **Description:** The number of Severely Errored Framing Seconds.
dsx1CurrentUASs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.5 **Description:** The number of Unavailable Seconds.
dsx1CurrentCSSs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.6 **Description:** The number of Controlled Slip Seconds.
dsx1CurrentPCVs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.7 **Description:** The number of Path Coding Violations.
dsx1CurrentLESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.8 **Description:** The number of Line Errored Seconds.
dsx1CurrentBESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.9 **Description:** The number of Bursty Errored Seconds.
dsx1CurrentLCVs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.7.1.11 **Description:** The number of Degraded Minutes.
dsx1IntervalIndex	**Syntax:** Integer

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.1 **Description:** The index value that uniquely identifies the DS1 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 as a dsx1LineIndex object instance.
dsx1IntervalNumber	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.2 **Description:** A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the 15-minute interval completed 23 hours and 45 minutes prior to interval 1.
dsx1IntervalESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.3 **Description:** The number of Errored Seconds.
dsx1IntervalSESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.4 **Description:** The number of Severely Errored Seconds.
dsx1IntervalSEFSs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.5 **Description:** The number of Severely Errored Framing Seconds.
dsx1IntervalUASs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.6 **Description:** The number of Unavailable Seconds. This object may decrease if the occurrence of unavailable seconds occurs across an interval boundary.
dsx1IntervalCSSs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.7 **Description:** The number of Controlled Slip Seconds.
dsx1IntervalPCVs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.8 **Description:** The number of Path Coding Violations.
dsx1IntervalLESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.9 **Description:** The number of Line Errored Seconds.
dsx1IntervalBESs	**Syntax:** Gauge32 **Access:** Read-Only

Object	Description
	OID: .1.3.6.1.2.1.10.18.8.1.10 **Description:** The number of Bursty Errored Seconds.
dsx1IntervalDMs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.11 **Description:** The number of Degraded Minutes.
dsx1IntervalLCVs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.12 **Description:** The number of Line Coding Violations.
dsx1IntervalValidData	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.8.1.13 **Description:** This variable indicates whether the data for this interval is valid.
dsx1TotalIndex	**Syntax:** Integer **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.1 **Description:** The index value that uniquely identifies the DS1 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 as a dsx1LineIndex object instance.
dsx1TotalESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.2 **Description:** The number of Errored Seconds encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalSESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.3 **Description:** The number of Severely Errored Seconds encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalSEFSs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.4 **Description:** The number of Severely Errored Framing Seconds encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalUASs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.5 **Description:** The number of Unavailable Seconds encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalCSSs	**Syntax:** Gauge32

Object	Description
	Access: Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.6 **Description:** The number of Controlled Slip Seconds encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalPCVs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.7 **Description:** The number of Path Coding Violations encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalLESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.8 **Description:** The number of Line Errored Seconds encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalBESs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.9 **Description:** The number of Bursty Errored Seconds (BESs) encountered by a DS1 interface in the previous 24-hour interval. Invalid 15-minute intervals count as 0.
dsx1TotalLCVs	**Syntax:** Gauge32 **Access:** Read-Only **OID:** .1.3.6.1.2.1.10.18.9.1.11 **Description:** The number of Line Coding Violations (LCVs) encountered by a DS1 interface in the current 15-minute interval. Invalid 15-minute intervals count as 0.

IEC-62439-2-MIB

Object	Description
mrpDomainIndex	**Syntax:** Unsigned32 **Access:** not-accessible **OID:** 1.0.62439.1.1.1.1.1 **Description:** The index of the entry.
mrpDomainID	**Syntax:** IEC62439UuidType **Access:** read-only **OID:** 1.0.62439.1.1.1.1.2 **Description:** Universally unique identifier belongs to the MRP domain, which represents a ring.
mrpDomainName	**Syntax:** DisplayString **Access:** read-only **OID:** 1.0.62439.1.1.1.1.3

Object	Description
	Description: A logical name for the MRP domain to ease the management of MRP domains.
mrpDomainAdminRole	**Syntax:** INTEGER **Access:** read-only **OID:** 1.0.62439.1.1.1.1.4 **Description:** 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. If the value is set to client(1) the entity shall be set to the role of a Media Redundancy Client (MRC). If the value is set to manager(2) the entity shall be set to the role of a Media Redundancy Manager (MRM). 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. 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. 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). If the agent restricts the write access, no matter what reason, it shall reject write requests by responding with 'badValue'.
mrpDomainOperRole	**Syntax:** INTEGER **Access:** read-only **OID:** 1.0.62439.1.1.1.1.5 **Description:** The operational role of an MRP entity per domain. A value of disabled(0) signals that the entity doesn't work (whatever reason). A value of client(1) signals that the entity is in a client role. A value of manager(2) signals that the entity is the manager of this MRP domain. A value of managerAutoComp(3) signals that the entity is in automanager role complying to Annex A. A value of managerAuto(4) signals that the entity is in automanager role not supporting Annex A.
mrpDomainRingPort1	**Syntax:** Integer32 **Access:** read-only **OID:** 1.0.62439.1.1.1.1.6 **Description:** The ifIndex of the layer 2 interface which is used as ring port 1.

mrpDomainRingPort1State	**Syntax:** INTEGER
	Access: read-only
	OID: 1.0.62439.1.1.1.1.7
	Description: Operational state of the first Ring-Port.
	• disabled(1) indicates that all frames are dropped
	• blocked(2) indicates that all frames are dropped except
	  • MRP topology change frames and MRP test frames from a MRM,
	  • MRP link change frames from an MRC,

Object	Description
	• MRP interconnection topology change from a MIM, • MRP interconnection link change from a MIC, • frames from other protocols that also define to pass blocked(2) ports. • forwarding(3) indicates that all frames are passed through according to the forwarding behavior of IEEE 802.1D • not-connected(4) indicates that the port has no link
mrpDomainRingPort2	**Syntax:** Integer32 **Access:** read-only **OID:** 1.0.62439.1.1.1.1.8 **Description:** The ifIndex of the layer 2 interface, which is used as ring port 2.
mrpDomainRingPort2State	**Syntax:** INTEGER **Access:** read-only **OID:** 1.0.62439.1.1.1.1.9 **Description:** Operational state of the second Ring-Port. • disabled(1) indicates that all frames are dropped • blocked(2) indicates that all frames are dropped except • MRP topology change frames and MRP test frames from a MRM, • MRP link change frames from an MRC, • MRP interconnection topology change from a MIM, • MRP interconnection link change from a MIC, • frames from other protocols that also define to pass blocked(2) ports. • forwarding(3) indicates that all frames are passed through according to the forwarding behavior of IEEE 802.1D • not-connected(4) indicates that the port has no link
mrpDomainState	**Syntax:** BITS **Access:** read-only **OID:** 1.0.62439.1.1.1.1.10 **Description:** Operational status of the MRP entity. • disabled(0) – MRP switched off. All higher bits are invalid and shall be reset. • undefined(1) – Value is not valid. All higher bits are invalid and shall be reset. • ringOpen(2) – MRP ring redundancy lost. All higher bits are invalid and shall be reset. • reserved(3) – reserved for further extensions.
mrpDomainError	**Syntax:** BITS **Access:** read-only **OID:** 1.0.62439.1.1.1.1.11 **Description:** 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. • noError(0) – the operational state of the device is confom to administrative state. All higher bits are invalid and shall be reset. • invalidVlanId(1) – the assigned VLAN ID is not permitted.

Object	Description
	• invalid (2) – Value is not valid. All higher bits are invalid and shall be reset. • multipleMRM(3) – multiple active managers in ring domain. • singleSideReceive(4) – the test frames of an MRM have been seen, but only on one port.
mrpDomainBlocked	**Syntax:** INTEGER **Access:** read-only **OID:** 1.0.62439.1.1.1.1.12 **Description:** The entity supports blocked ring ports. 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. Set to enabled the manager demands that all clients shall support the blocked attribute also set to enabled. If mrpDomainBlocked is set disabled at the manager, then the value of mrpDomainBlocked can be arbitrary at the clients. • enabled(1) client: supports ring ports whose port state can be blocked. • manager: works only with clients supporting blocked ring ports. • disabled(2) client: no support of blocked ring ports. • manager: Work with clients supporting blocked ring ports and with clients not supporting blocked ring ports.
mrpDomainVlanId	**Syntax:** Unsigned32 **Access:** read-only **OID:** 1.0.62439.1.1.1.1.13 **Description:** The VLAN ID assigned to the MRP protocol. The VLAN ID only is in use when the bit invalidVlanId is not set in mrpDomainError. If value is set to 0 no VLAN is assigned. The invalidVlanId shall be set to 0 (no Error).
mrpDomainManagerPriority	**Syntax:** INTEGER **Access:** read-only **OID:** 1.0.62439.1.1.1.1.14 **Description:** 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.
mrpDomainRingOpenCount	**Syntax:** Counter32 **Access:** read-only **OID:** 1.0.62439.1.1.1.1.15 **Description:** Counter for ring-state changes to open.
mrpDomainLastRingOpenChange	**Syntax:** TimeTicks **Access:** read-only **OID:** 1.0.62439.1.1.1.1.16 **Description:** Timeticks since last change of ring-state to ring open.
mrpDomainRoundTripDelayMax	**Syntax:** Unsigned32

Object	Description
	Access: read-only **OID:** 1.0.62439.1.1.1.1.17 **Description:** The max. Round-Trip-Delay (in milliseconds), which was measured since startup.
mrpDomainRoundTripDelayMin	**Syntax:** Unsigned32 **Access:** read-only **OID:** 1.0.62439.1.1.1.1.18 **Description:** The min. Round-Trip-Delay (in milliseconds), which was measured since startup.
mrpDomainResetRoundTripDelays	**Syntax:** INTEGER **Access:** not-accessible **OID:** 1.0.62439.1.1.1.1.19 **Description:** A write request with resetDelays(1) shall reset the values of mrpDomainRoundTripDelayMax and mrpDomainRoundTripDelayMin to zero at the same time.
mrpDomainMRMReactOnLinkChange	**Syntax:** INTEGER **Access:** read-only **OID:** 1.0.62439.1.1.1.1.20 **Description:** Tells whether the MRM reacts on link down MRP link change frames. • enabled(1) indicates that the MRM reacts immediately on link down MRP link change frames • disabled(2) indicates that the MRM does not react on link down MRP link change frames

20.2 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	**MIB:** SNMPv2-MIB **Standard:** RFC 3418 **OID:** 1.3.6.1.6.3.1.1.5.5 **Definition:** 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.

Variable	Description
coldStart	**MIB:** SNMPv2-MIB **Standard:** RFC 3418 **OID:** 1.3.6.1.6.3.1.1.5.1 **Definition:** A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
warmStart	**MIB:** SNMPv2-MIB **Standard:** RFC 3418 **OID:** 1.3.6.1.6.3.1.1.5.2 **Definition:** A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.
newRoot	**MIB:** BRIDGE-MIB **Standard:** RFC 4188 **OID:** 1.3.6.1.2.1.17.0.1 **Definition:** 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.
topologyChange	**MIB:** BRIDGE-MIB **Standard:** RFC 4188 **OID:** 1.3.6.1.2.1.17.0.2 **Definition:** 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.
lldpRemTablesChange	**MIB:** LLDP-MIB **Standard:** IEEE Std 802.1AB-2005 **OID:** 1.0.8802.1.1.2.0.0.1 **Definition:** 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.
linkUp	**MIB:** IF-MIB **Standard:** RFC 1229, 2863, 2233, 1573 **OID:** 1.3.6.1.6.3.1.1.5.4

Variable	Description
	Definition: 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	**MIB:** IF-MIB **Standard:** RFC 1229, 2863, 2233, 1573 **OID:** 1.3.6.1.6.3.1.1.5.3 **Definition:** 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.
dsx1LineStatusChange	**MIB:** DS1-MIB **Standard:** RFC 3895 **OID:** 1.3.6.1.2.1.10.18.15.0.1 **Definition:** 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.

20.3 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	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4 **Definition:** The main subtree for new MIB development where specific RUGGEDCOM proprietary MIBs can be placed.
ruggedcomTrapsModule	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1 **Definition:** The RUGGEDCOM MIB providing traps information.

Variable	Description
ruggedcomTrapsModuleObjects	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1 **Definition:** A group of objects that define the RUGGEDCOM traps module.
trapGenericTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.1 **Definition:** The main subtree for the RUGGEDCOM generic traps.
genericTrapSeverity	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.1.1 **Syntax:** Integer **Definition:** The severity level of the generic trap.
genericTrapDescription	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.1.2 **Syntax:** String **Definition:** A description of a generic trap.
trapPowerSupplyTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.2 **Definition:** The main subtree for the RUGGEDCOM power supply trap.
powerSupplyDescription	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.2.1 **Syntax:** String **Definition:** A description of a power supply that fails.
powerSupplyIdentifier	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.2.2 **Syntax:** Integer **Definition:** The identified power supply (e.g. power supply 1).
trapSwUpgradeTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.3 **Definition:** The main subtree for the RUGGEDCOM software upgrade trap.
trapHotswapModuleStateChangeTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.6 **Definition:** The main subtree for the RUGGEDCOM hotswap module state change trap.
hotswapModuleSlot	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.6.1 **Syntax:** RcHotswapModuleSlot **Definition:** The physical slot where the module is located.
hotswapModulePreviousState	**MIB:** RUGGEDCOM-TRAPS-MIB

Variable	Description
	OID: 1.3.6.1.4.1.15004.4.1.1.6.2 **Syntax:** RcHotswapModuleState **Definition:** The previous state of the module.
trapModuleTypeMismatchTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.8 **Definition:** The main subtree for the RUGGEDCOM module type mismatch trap.
trapRTCBatteryLowTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.11 **Definition:** The main subtree for the RUGGEDCOM RTC battery low trap.
trapSecurityCertificateExpiryTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.12 **Definition:** The main subtree for the RUGGEDCOM security certificate expiration trap.
trapUserAuthFailure	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.14 **Syntax:** String **Definition:** The main subtree for the RUGGEDCOM login failure trap.
userAuthFailureMessage	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.14.1 **Syntax:** String **Definition:** The login failure message. The message contains the name, reason, IP address, context, and protocol.
trapSuccessUsrChgPwd	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.15 **Syntax:** String **Definition:** The main subtree for the RUGGEDCOM successful user changed password trap.
successUsrChgPwd	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.15.1 **Syntax:** String **Definition:** The username of the user whose password was successfully changed.
trapRmonThresholdRise	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.16 **Definition:** The main subtree for the RUGGEDCOM RMON threshold rising alarm trap.
rmonThresholdRiseInterface	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.16.1 **Syntax:** String

Variable	Description
	Definition: The name of the interface that crossed an RMON threshold value.
rmonThresholdRiseStatistic	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.16.2 **Syntax:** String **Definition:** The specific statistic for which an RMON threshold was crossed.
rmonThresholdRiseThroughput	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.16.3 **Syntax:** String **Definition:** The current throughput value when this trap is sent.
trapExtDeviceAction	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.17 **Syntax:** String **Definition:** The main subtree for the RUGGEDCOM USB status trap.
extDeviceActionMessage	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.1.17.1 **Syntax:** String **Definition:** The USB status message. The message notifies if a USB is inserted.
ruggedcomTrapsModuleConformance	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5 **Definition:** A group of objects that define the RUGGEDCOM module conformance trap.
ruggedcomTrapsModuleGroups	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2 **Definition:** A group of objects that define the RUGGEDCOM traps module.
ruggedcomGenericTrapGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.1 **Definition:** A group of objects that define the generic trap.
ruggedcomPowerSupplyGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.2 **Definition:** A group of objects that define the RUGGEDCOM power supply failure trap.
ruggedcomNotificationsGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.3 **Definition:** The RUGGEDCOM notifications group.
ruggedcomPowerSupplyIdentGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.5

Variable	Description
	Definition: A group of objects that define RUGGEDCOM power supply identification.
ruggedcomHotswapModuleSCNotifGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.7 **Definition:** The RUGGEDCOM Hotswap Module notifications group.
ruggedcomModuleStateChangeGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.9 **Definition:** A group of objects that define the RUGGEDCOM Module State Change trap.
ruggedcomHotswapModuleSCNotifGroup01	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.11 **Definition:** The RUGGEDCOM Hotswap Module notifications group.
ruggedcomRTCBatteryLowGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.13 **Definition:** A group of objects for RTC battery low indication.
ruggedcomSecurityGroup02	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.14 **Definition:** A group of objects to indicate security certificate expiry.
rcPswdChgTrapNotifyGroup	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.4.1.5.2.25 **Definition:** A group of trap objects to notify the password was successfully changed.
rcSysInfo	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2 **Definition:** RUGGEDCOM system information MIB.
rcDeviceInfo	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2.3 **Definition:** The main subtree for the RUGGEDCOM device info trap.
rcDeviceInfoBootSwVersion	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2.3.2 **Definition:** The version and the build date of the boot loader software
rcDeviceInfoMainSwVersion	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2.3.3 **Definition:** The version and the build date of the main operating system software.
rcDeviceInfoPendingBootSwVersion	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2.3.6 **Definition:** The version and the build date of the boot loader software that has been loaded to the

Variable	Description
	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	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2.3.7 **Definition:** 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	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.2.3.8 **Syntax:** Integer **Definition:** 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 cfgChangeTrap notification.
rcCellularModem	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15 **Definition:** The main subtree for the cellular modem.
rcCellularModemStats	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15.1
rcCellularModemStatsTable	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15.1.1 **Syntax:** SEQUENCE OF RcCellularModemStatsEntry **Definition:** The Table of Currently Active Sim Cards.
rcCellularModemStatsEntry	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15.1.1.1 **Syntax:** RcCellularModemStatsEntry **Definition:** The Current Sim Card information.
rcCellularModemStatsCurrentSlot	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15.1.1.1.1 **Definition:** The name of the SIM card which is currently being used.
rcCellularModemStatsCurrentPort	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15.1.1.1.2 **Syntax:** String
rcCellularModemStatsActiveSimName	**MIB:** RUGGEDCOM-SYS-INFO-MIB

Variable	Description
	OID: 1.3.6.1.4.1.15004.4.15.1.1.1.3 **Syntax:** String **Definition:** The name of the SIM card which is currently being used.
rcCellularModemStatsActiveSimIccid	**MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.4.15.1.1.1.4 **Syntax:** String **Definition:** The ICCID of the SIM card which is currently being used.
ruggedcomTraps	**MIB:** RUGGEDCOM-MIB.mib **OID:** 1.3.6.1.4.1.15004.5 **Definition:** The root of the subtree where RUGGEDCOM traps can be placed.
genericTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** A generic trap generated by RUGGEDCOM devices.
powerSupplyTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.2 **Definition:** 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 *powerSupplyDescription* at the time the trap is generated. The status of power supply units in the device can be retrieved via objects *rcDeviceStsPowerSupply1* and *rcDeviceStsPowerSupply2*. *powerSupplyIdentifier* object is recommended to be added as an optional parameter to the list of objects.
swUpgradeTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.3 **Definition:** A generic trap generated upon software upgrade. The rate at which this notification is provided is 60 seconds.
cfgChangeTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.4 **Definition:** A generic trap generated upon configuration change. The rate at which this notification is provided is 60 seconds.
hotswapModuleStateChangeTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.7 **Definition:** A trap generated when a RUGGEDCOM ROX II module changes state. The first traps are generated during initial startup.
moduleTypeMismatchTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.9

Variable	Description
	Definition: 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.
securityCertificateExpiryTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.16 **Definition:** A trap indicating that at least one security certificate on the device is within 30 days of expiration. It is generated by RUGGEDCOM devices.
rcSuccessUsrChgPwdTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20 **Definition:** A trap generated when a user's password is successfully changed.
rcCellularModemStatsTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.45 **Definition:** A trap generated when a failover event occurs.
rcUserLoginFailureTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.46 **Definition:** A trap generated when a user login failure occurs.
rcExtDeviceActionTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.47 **Definition:** A trap generated when a USB Device is inserted.
rcRmonThresholdRiseTrap	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.48 **Definition:** A trap generated when a threshold value has been crossed for an interface.
rcMrpManagerRingClosed	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.50 **Definition:** A trap indicating the closed state of the MRP Manager ring. The Manager is identified by its MRP instance ID.
rcMrpManagerRingOpen	**MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.51 **Definition:** A trap indicating the open state of the MRP Manager ring. The Manager is identified by its MRP instance ID.
rcTunnels	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16 **Definition:** The RUGGEDCOM MIB providing tunnel status and traps.
rcIpsecTunnelObjects	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1

Variable	Description
	Definition: The main subtree for all IPsec tunnel objects.
rcIpsecTunnelTable	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1.1 **Syntax:** SEQUENCE OF RcIpsecTunnelEntry **Definition:** The IPsec Connections Tunnel Table. There is one entry in this table for each IPsec Tunnel.
rcIpsecTunnelEntry	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1.1.1 **Syntax:** RcIpsecTunnelEntry **Definition:** Each entry contains the attributes associated with an IPsec Tunnel.
rcIpsecConnIndex	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1.1.1.1 **Syntax:** Integer **Definition:** The table index number of the IPsec connection.
rcIpsecConnName	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1.1.1.2 **Syntax:** String **Definition:** The name of the IPsec connection. The name is unique so it can be used as an index into the connection table.
rcIpsecConnStatus	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1.1.1.3 **Syntax:** RcTunnelStatus **Definition:** The status of the IPsec connection. Refer to the TunnelStatus object for definitions of states.
rcIpsecConnNumPeers	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.1.1.1.4 **Syntax:** Integer **Definition:** The number of active peers on the IPsec connection.
rcGreTunnelObjects	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.2 **Definition:** The main subtree for all the various GRE tunnel objects.
rcGreTunnelTable	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.2.1 **Syntax:** SEQUENCE OF RcGreTunnelEntry **Definition:** The GRE Tunnels Table. There is one entry in this table for each GRE Tunnel.
rcGreTunnelEntry	**MIB:** RUGGEDCOM-TUNNELS-MIB

Variable	Description
	OID: 1.3.6.1.4.1.15004.4.16.2.1.1 **Syntax:** RcGreTunnelEntry **Definition:** Each entry contains the attributes associated with a GRE Tunnel.
rcGreTunnelIndex	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.2.1.1.1 **Syntax:** Integer **Definition:** The table index number of the GRE tunnel.
rcGreTunnelName	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.2.1.1.2 **Syntax:** String **Definition:** The name of the GRE tunnel.
rcGreTunnelStatus	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.2.1.1.3 **Syntax:** RcTunnelStatus **Definition:** The status of the GRE tunnel. Refer to the *TunnelStatus* object for definitions of states.
rcTunnelTraps	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5 **Definition:** The main subtree for the RUGGEDCOM tunnel traps.
rcTunnelIpsecTraps	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5.1 **Definition:** The main subtree for the RUGGEDCOM IPsec tunnel traps.
rcIpsecTunnelUpTrap (Notifications)	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5.1.1 **Definition:** A trap generated when IPsec tunnel connections are established (come up).
rcIpsecTunnelDownTrap (Notifications)	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5.1.2 **Definition:** A trap generated when IPsec tunnel connections are disconnected (go down).
rcTunnelGreTraps	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5.2 **Definition:** The main subtree for the RUGGEDCOM GRE tunnel traps.
rcGreTunnelDownTrap (Notifications)	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5.2.2 **Definition:** A trap generated when GRE tunnels are disconnected (go down).
rcGreTunnelUpTrap (Notifications)	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.5.2.1

Variable	Description
	Definition: A trap generated when GRE tunnels are established (come up).
rcTunnelsConformance	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6 **Definition:** The main subtree for the RUGGEDCOM tunnels conformance traps.
rcTunnelsIpsecGroups	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.1 **Definition:** A group of objects that define RUGGEDCOM IPsec tunnels.
rcTunIpsecObjectsGroup	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.1.1 **Definition:** A group of objects providing information for IPsec tunnels.
rcTunIpsecTrapsGroup	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.1.2 **Definition:** A group of objects that define RUGGEDCOM Ipsec tunnel traps.
rcTunIpsecNotificationsGroup	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.1.3 **Definition:** The RUGGEDCOM notifications group for IPsec tunnel traps.
rcTunnelsGreGroups	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.2 **Definition:** A group of objects that define RUGGEDCOM GRE tunnels.
rcTunGreObjectsGroup	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.2.1 **Definition:** A group of objects providing information for GRE tunnels.
rcTunGreTrapsGroup	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.2.2 **Definition:** A group of objects that define RUGGEDCOM GRE tunnel traps.
rcTunGreNotificationsGroup	**MIB:** RUGGEDCOM-TUNNELS-MIB **OID:** 1.3.6.1.4.1.15004.4.16.6.2.3 **Definition:** The RUGGEDCOM notifications group for GRE tunnel traps.

20.4 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
Server Host Key Algorithms			
ssh-ed25519	4	✓	✓
ssh-rsa	3		✓
KEX Algorithms			
diffie-hellman-group18-sha512	4	✓	✓
diffie-hellman-group14-sha1	3		✓
diffie-hellman-group14-sha256	3		✓
MAC Algorithms			
hmac-sha2-256	4	✓	✓
hmac-sha2-512	4	✓	✓
hmac-sha1	1		✓
Encryption Algorithms			
aes128-ctr	4	✓	✓
aes192-ctr	4	✓	✓
aes256-ctr	4	✓	✓

Service: HTTPS Server (TCP/443)

Cipher Suite/Protocol	Grade	Enabled by Default	Configurable
Protocols			
TLS v1.2	5	✓	✓
TLS v1.0	2		✓
Cipher Suites			
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		✓
Elliptic Curve			
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
Server Host Key			
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		✓
KEX Algorithm			
diffie-hellman-group16-sha512	4	✓	✓
diffie-hellman-group18-sha512	4	✓	✓
ecdh-sha2-nistp256	4	✓	✓
ecdh-sha2-nistp384	4	✓	✓

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		✓
MAC Algorithm			
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	✓	✓
Encryption Algorithm			
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