SIEMENS

RUGGEDCOM ROX II v2.13

CLI User Guide

For RX1400

5/2019
RC1416-EN-03

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

Serial Server 9

Wireless 10

Tunneling and VPNs 11

Unicast and Multicast Routing 12

Network Redundancy 13

Network Discovery and Management 14

Traffic Control and Classification 15

Time Services 16

Continued on next page

SIEMENS

RUGGEDCOM ROX II v2.13

CLI User Guide

For RX1400

5/2019
RC1416-EN-03

Continued

Virtualization 17

Applications 18

Troubleshooting 19

Copyright © 2019 Siemens Canada Ltd

All rights reserved. Dissemination or reproduction of this document, or evaluation and communication of its contents, is not authorized except where expressly permitted. Violations are liable for damages. All rights reserved, particularly for the purposes of patent application or trademark registration.

This document contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Siemens Canada Ltd.

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd.

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.

Open Source

RUGGEDCOM ROX II is based on Linux®. Linux® is made available under the terms of the GNU General Public License Version 2.0 [http://www.gnu.org/licenses/gpl-2.0.html].

RUGGEDCOM ROX II contains additional Open Source Software. For license conditions, refer to the associated *License Conditions* document.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit https://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit https://support.automation.siemens.com.

Warranty

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

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

Contacting Siemens

Address
Siemens Canada Ltd
Industry Sector
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
ruggedcom.info.i-ia@siemens.com

Web
https://www.siemens.com/ruggedcom

Table of Contents

Preface xliii
Conventions xliii
Related Documents xliv
System Requirements xlvi
Accessing Documentation xlvi
License Conditions xlvi
Training xlvi
Customer Support xlvii

Chapter 1
Introduction 1
1.1 Features and Benefits 1
1.2 Feature Keys 5
1.3 Security Recommendations 6
1.4 Available Services by Port 9
1.5 User Permissions 10
1.6 Removable Memory 13
1.7 Logged Events 14
1.7.1 Structure of a Syslog Event 14
1.7.2 Syslog Event Types 15
1.7.3 Logged Security Events 15

Chapter 2
Using RUGGEDCOM ROX II 21
2.1 Default User Names and Passwords 21
2.2 Logging In 22
2.3 Logging Out 22
2.4 Using Network Utilities 23
2.4.1 Pinging an IPv4 Address or Host 23
2.4.2 Pinging an IPv6 Address or Host 24
2.4.3 Pinging MPLS Endpoints 24
2.4.4 Pinging VRF Endpoints 24
2.4.5 Tracing a Route to an IPv4 Host 24
2.4.6 Tracing a Route to an IPv6 Host 25
2.4.7 Tracing a Route to an MPLS Endpoint 25

2.4.8 Tracing a Route to a VRF Endpoint 25
2.4.9 Capturing Packets from a Network Interface 26
2.4.10 Capturing Packets from a VRF Network Interface 26
2.5 Using the Command Line Interface 27
2.5.1 Accessing Different CLI Modes 27
2.5.2 Using Command Line Completion 28
2.5.3 Displaying Available Commands 28
2.5.4 Editing Commands 29
2.5.5 Using Double Quotes 30
2.5.6 Using Output Redirects 30
2.5.7 Using Regular Expressions 35
2.5.8 Using CLI Utilities 36
2.5.9 Specifying a Range 37
2.5.10 Common Commands 37
2.5.10.1 Basic CLI Commands 37
2.5.10.2 File Commands 39
2.5.10.3 Interface and Services Commands 41
2.5.10.4 Administration Commands 42
2.5.10.5 Configuration Mode General Commands 43
2.6 Configuring the CLI Interface 47
2.7 Accessing Different Modes 48
2.7.1 Managing Maintenance Mode Authorization 48
2.7.1.1 Temporarily Enabling Maintenance Mode Authorization 48
2.7.1.2 Permanently Enabling Maintenance Mode Authorization 49
2.7.1.3 Disabling Maintenance Mode Authorization 50
2.7.2 Accessing Maintenance Mode 50
2.7.3 Accessing BIST Mode 51
2.7.4 Accessing Service Mode 53

Chapter 3
Getting Started 55
3.1 Connecting to RUGGEDCOM ROX II 55
3.1.1 Default IP Address 55
3.1.2 Connecting Directly 55
3.1.3 Connecting Remotely 56
3.2 Configuring a Basic Network 57
3.2.1 Configuring a Basic IPv4 Network 57
3.2.2 Configuring a Basic IPv6 Network 57

Chapter 4
Device Management 59
4.1 Displaying Device and Software Information 59
4.2 Determining the GPS Location of the Device 60
4.3 Viewing Chassis Information and Status 61
4.3.1 Viewing the Slot Hardware 61
4.3.2 Viewing Flash Card Storage Utilization 61
4.3.3 Viewing CPU/RAM Utilization 62
4.3.4 Viewing the Slot Status 63
4.3.5 Viewing the Slot Sensor Status 64
4.4 Viewing the Parts List 64
4.5 Shutting Down the Device 65
4.6 Rebooting the Device 66
4.7 Restoring Factory Defaults 66
4.8 Decommissioning the Device 66
4.9 Viewing a List of Line Module Configurations 67
4.10 Managing Feature Keys 67
4.10.1 Viewing the Contents of a Feature Key 68
4.10.2 Installing Feature Keys 68
4.11 Managing Files 70
4.11.1 Installing Files 70
4.11.2 Backing Up Files 71
4.12 Managing Logs 71
4.12.1 Viewing Logs 72
4.12.2 Deleting Logs 73
4.12.3 Configuring Secure Remote Syslog 73
4.12.3.1 Enabling/Disabling Secure Remote Syslog 74
4.12.3.2 Viewing a List of Permitted Peers 74
4.12.3.3 Adding a Permitted Peer 75
4.12.3.4 Deleting a Permitted Peer 75
4.12.3.5 Configuring a Source IP Address for Remote Syslog Messages 75
4.12.4 Managing Diagnostic Logs 76
4.12.4.1 Enabling/Disabling the Developer's Log 76
4.12.4.2 Enabling/Disabling the SNMP Log 77
4.12.4.3 Enabling/Disabling the NETCONF Summary Log 78
4.12.4.4 Enabling/Disabling the NETCONF Trace Log 78
4.12.4.5 Enabling/Disabling the XPATH Trace Log 79
4.12.4.6 Enabling/Disabling the WebUI Trace Log 80
4.12.5 Managing Remote Syslog Servers 80
4.12.5.1 Viewing a List of Remote Servers 80

4.12.5.2 Adding a Remote Server 81
4.12.5.3 Deleting a Remote Server 81
4.12.6 Managing Remote Server Selectors 82
4.12.6.1 Viewing a List of Remote Server Selectors 82
4.12.6.2 Adding a Remote Server Selector 82
4.12.6.3 Deleting a Remote Server Selector 83
4.13 Managing the Software Configuration 84
4.13.1 Saving the Configuration 84
4.13.2 Loading a Configuration 84
4.14 Managing Automatic Configuration Loading 85
4.14.1 Enabling/Disabling Automatic Configuration Loading 85
4.14.2 Automatically Loading a Configuration File from a Removable Drive 85
4.14.3 Overriding Factory Settings Using a Removable Drive 86
4.15 Upgrading/Downgrading the RUGGEDCOM ROX II Software 87
4.15.1 Configuring the Upgrade Source 87
4.15.2 Setting Up an Upgrade Server 88
4.15.2.1 Configuring the Upgrade Server 89
4.15.2.2 Adding Software Releases to the Upgrade Server 90
4.15.2.3 Adding Firmware Releases to the Upgrade Server 90
4.15.3 Upgrading the RUGGEDCOM ROX II Software 91
4.15.4 Stopping/Declining a Software Upgrade 92
4.15.5 Downgrading the RUGGEDCOM ROX II Software 93
4.15.5.1 Rolling Back a Software Upgrade 93
4.15.5.2 Downgrading Using ROXflash 93
4.16 Monitoring Firmware Integrity 94
4.16.1 Enabling/Disabling the Boot Time Firmware Integrity 95
4.16.2 Checking the Firmware Integrity 95
4.16.3 Scheduling a Recurring Firmware Integrity Check 96
4.16.4 Viewing the Status of the Firmware Integrity Check 96
4.17 Managing SFP Transceivers 97
4.17.1 SFP Transceiver Support 97
4.17.2 Viewing SFP Information 98
4.17.3 Enabling/Disabling Smart SFP Mode 99

Chapter 5
System Administration 101
5.1 Configuring the System Name and Location 101
5.2 Configuring the Host Name 102
5.3 Customizing the Welcome Screen 102
5.4 Setting the Maximum Number of Sessions 102
5.5 Enabling and Configuring WWW Interface Sessions 103

5.6 Enabling/Disabling Remote Access Through a VRF Interface 104
5.7 Managing Alarms 105
5.7.1 Pre-Configured Alarms 106
5.7.2 Viewing a List of Active Alarms 106
5.7.3 Clearing and Acknowledging Alarms 107
5.7.3.1 Clearing Alarms 107
5.7.3.2 Acknowledging Alarms 107
5.7.4 Configuring an Alarm 108
5.8 Managing Users 109
5.8.1 Viewing a List of Users 109
5.8.2 Adding a User 110
5.8.3 Deleting a User 110
5.8.4 Monitoring Users 110
5.8.4.1 Kicking Users from the Network 111
5.8.4.2 Sending Messages to Users 111
5.9 Managing Passwords and Passphrases 111
5.9.1 Configuring Password/Passphrase Complexity Rules 112
5.9.2 Setting a User Password/Passphrase 113
5.9.3 Setting the Boot Password/Passphrase 114
5.9.4 Setting the Maintenance Password/Passphrase 114
5.9.5 Resetting the Admin Password/Passphrase 115
5.9.6 Resetting the Boot Password/Passphrase 116
5.9.7 Resetting the Maintenance Password/Passphrase 117
5.10 Scheduling Jobs 118
5.10.1 Viewing a List of Scheduled Jobs 118
5.10.2 Adding a Scheduled Job 119
5.10.3 Deleting a Scheduled Job 120

Chapter 6
Security 121
6.1 Enabling and Configuring CLI Sessions 121
6.2 Enabling and Configuring SFTP Sessions 122
6.3 Enabling/Disabling Brute Force Attack Protection 123
6.4 Enabling/Disabling SYN Cookies 124
6.5 Managing Port Security 125
6.5.1 Port Security Concepts 125
6.5.1.1 Static MAC Address-Based Authentication 126
6.5.1.2 IEEE 802.1x Authentication 126
6.5.1.3 IEEE 802.1X Authentication with MAC Address-Based Authentication 127
6.5.1.4 Assigning VLANS with Tunnel Attributes 127
6.5.2 Configuring Port Security 128

6.5.3 Viewing the Security Status of Switched Ethernet Ports 129
6.6 Managing User Authentication 130
6.6.1 Setting the User Authentication Mode 130
6.6.2 Managing User Authentication Keys 131
6.6.2.1 Determining Which Keys are Associated to a User 131
6.6.2.2 Adding a User Authentication Key 132
6.6.2.3 Deleting a User Authentication Key 132
6.6.2.4 Associating/Disassociating a User Authentication Key 133
6.6.3 Managing RADIUS Authentication 134
6.6.3.1 Configuring RADIUS Authentication for LOGIN Services 135
6.6.3.2 Configuring RADIUS Authentication for PPP Services 136
6.6.3.3 Configuring RADIUS Authentication for Switched Ethernet Ports 136
6.6.4 Configuring TACACS+ Authentication 137
6.7 Managing Certificates and Keys 138
6.7.1 Viewing the Local Host SSH/RSA Public Key 139
6.7.2 Managing the Trusted Certificate Store 139
6.7.2.1 Configuring the Trusted Certificate Store 140
6.7.2.2 Enabling/Disabling the Trusted Certificate Store 140
6.7.2.3 List of Root Certificates in the Trusted Certificate Store 140
6.7.3 Managing CA Certificates for the Trusted Certificate Store 166
6.7.3.1 Viewing a List of CA Certificates Added to the Trusted Certificate Store 166
6.7.3.2 Adding a CA Certificate to the Trusted Certificate Store 167
6.7.3.3 Deleting a CA Certificate from the Trusted Certificate Store 167
6.7.4 Managing CA Certificates and CRLs 167
6.7.4.1 Viewing a List of CA Certificates and CRLs 168
6.7.4.2 Viewing the Status of a CA Certificate and CRL 168
6.7.4.3 Adding a CA Certificate and CRL 169
6.7.4.4 Deleting a CA Certificate and CRL 170
6.7.5 Managing Private Keys 170
6.7.5.1 Viewing a List of Private Keys 171
6.7.5.2 Adding a Private Key 171
6.7.5.3 Deleting a Private Key 172
6.7.6 Managing Public Keys 172
6.7.6.1 Viewing a List of Public Keys 172
6.7.6.2 Adding a Public Key 173
6.7.6.3 Adding an IPSec-Formatted Public Key 173
6.7.6.4 Deleting a Public Key 174
6.7.7 Managing Certificates 174
6.7.7.1 Viewing a List of Certificates 175
6.7.7.2 Viewing the Status of a Certificate 175

6.7.7.3 Adding a Certificate 176
6.7.7.4 Deleting a Certificate 176
6.7.8 Managing Known Hosts 177
6.7.8.1 Viewing a List of Known Hosts 177
6.7.8.2 Adding a Known Host 177
6.7.8.3 Deleting a Known Host 178
6.8 Managing Firewalls 178
6.8.1 Firewall Concepts 179
6.8.1.1 Stateless vs. Stateful Firewalls 179
6.8.1.2 Linux netfilter 180
6.8.1.3 Network Address Translation 180
6.8.1.4 Port Forwarding 181
6.8.1.5 Protecting Against a SYN Flood Attack 181
6.8.1.6 Protecting Against IP Spoofing 181
6.8.2 Viewing a List of Firewalls 182
6.8.3 Adding a Firewall 182
6.8.4 Deleting a Firewall 183
6.8.5 Working with Multiple Firewall Configurations 183
6.8.6 Configuring the Firewall for a VPN 184
6.8.7 Configuring the Firewall for a VPN in a DMZ 185
6.8.8 Configuring Netfilter 185
6.8.9 Managing Zones 186
6.8.9.1 Viewing a List of Zones 186
6.8.9.2 Adding a Zone 187
6.8.9.3 Deleting a Zone 187
6.8.10 Managing Interfaces 188
6.8.10.1 Viewing a List of Interfaces 188
6.8.10.2 Adding an Interface 189
6.8.10.3 Associating an Interface with a Zone 190
6.8.10.4 Configuring a Broadcast Address 190
6.8.10.5 Deleting an Interface 191
6.8.11 Managing Hosts 191
6.8.11.1 Viewing a List of Hosts 191
6.8.11.2 Adding a Host 192
6.8.11.3 Deleting a Host 193
6.8.12 Managing Policies 193
6.8.12.1 Viewing a List of Policies 194
6.8.12.2 Adding a Policy 194
6.8.12.3 Configuring the Source Zone 195
6.8.12.4 Configuring the Destination Zone 195

6.8.12.5 Deleting a Policy 196
6.8.13 Managing Network Address Translation Settings 196
6.8.13.1 Viewing a List of NAT Settings 196
6.8.13.2 Adding a NAT Setting 197
6.8.13.3 Deleting a NAT Setting 198
6.8.14 Managing Masquerade and SNAT Settings 198
6.8.14.1 Viewing a List of Masquerade and SNAT Settings 198
6.8.14.2 Adding Masquerade or SNAT Settings 199
6.8.14.3 Deleting a Masquerade or SNAT Setting 200
6.8.15 Managing Rules 200
6.8.15.1 Viewing a List of Rules 201
6.8.15.2 Adding a Rule 201
6.8.15.3 Configuring the Source Zone 203
6.8.15.4 Configuring the Destination Zone 203
6.8.15.5 Deleting a Rule 204
6.8.16 Validating a Firewall Configuration 204
6.8.17 Enabling/Disabling a Firewall 204
6.9 Restricting Management Access to Specific Interfaces 205

Chapter 7
IP Address Assignment 209
7.1 Managing IP Addresses for Routable Interfaces 209
7.1.1 Configuring Costing for Routable Interfaces 209
7.1.2 Viewing Statistics for Routable Interfaces 210
7.1.3 Managing IPv4 Addresses 211
7.1.3.1 Viewing a List of IPv4 Addresses 211
7.1.3.2 Adding an IPv4 Address 212
7.1.3.3 Deleting an IPv4 Address 212
7.1.4 Managing IPv6 Addresses 213
7.1.4.1 Viewing a List of IPv6 Addresses 213
7.1.4.2 Adding an IPv6 Address 213
7.1.4.3 Deleting an IPv6 Address 214
7.1.5 Configuring IPv6 Neighbor Discovery 214
7.1.6 Managing IPv6 Network Prefixes 216
7.1.6.1 Adding an IPv6 Network Prefix 216
7.1.6.2 Deleting an IPv6 Network Prefix 217
7.2 Managing the DHCP Relay Agent 217
7.2.1 Configuring the DHCP Relay Agent 218
7.2.2 Assigning a DHCP Server Address 218
7.2.3 Viewing a List of DHCP Client Ports 218
7.2.4 Adding a DHCP Client Port 219

7.2.5 Deleting a DHCP Client Port 219
7.2.6 Example: Configuring the Device as a Relay Agent 219
7.3 Managing the DHCP Server 221
7.3.1 Viewing a List of Active Leases 221
7.3.2 Configuring the DHCP Server 222
7.3.3 Enabling/Disabling the DHCP Server 223
7.3.4 Configuring DHCP Server Options 223
7.3.5 Managing DHCP Client Configuration Options 224
7.3.5.1 Configuring Standard DHCP Client Configuration Options (IPv4) 225
7.3.5.2 Configuring Standard DHCP Client Configuration Options (IPv6) 226
7.3.5.3 Viewing a List of Custom DHCP Client Configuration Options 227
7.3.5.4 Adding a Custom DHCP Client Configuration Option 228
7.3.5.5 Deleting a Custom DHCP Client Configuration Option 228
7.3.6 Managing DHCP Listen Interfaces 229
7.3.6.1 Viewing a List of DHCP Listen Interfaces 229
7.3.6.2 Adding a DHCP Listen Interface 230
7.3.6.3 Deleting a DHCP Listen Interface 230
7.3.7 Managing Shared Networks 230
7.3.7.1 Viewing a List of Shared Networks 231
7.3.7.2 Adding a Shared Network 231
7.3.7.3 Configuring Shared Network Options 232
7.3.7.4 Deleting a Shared Network 233
7.3.8 Managing Subnets 233
7.3.8.1 Viewing a List of Subnets 234
7.3.8.2 Adding a Subnet 234
7.3.8.3 Configuring Subnet Options 235
7.3.8.4 Deleting a Subnet 237
7.3.9 Managing Host Groups 237
7.3.9.1 Viewing a List of Host Groups 237
7.3.9.2 Adding a Host Group 238
7.3.9.3 Configuring Host Group Options 238
7.3.9.4 Deleting a Host Group 240
7.3.10 Managing DHCP Hosts 240
7.3.10.1 Viewing a List of Hosts 240
7.3.10.2 Adding a Host 241
7.3.10.3 Configuring Host Options 241
7.3.10.4 Deleting Hosts 243
7.3.11 Managing Address Pools (IPv4) 244
7.3.11.1 Viewing a List of Address Pools (IPv4) 244
7.3.11.2 Adding an Address Pool (IPv4) 244

7.3.11.3 Deleting an Address Pool (IPv4) 245
7.3.12 Managing Address Pools (IPv6) 246
7.3.12.1 Viewing a List of Address Pools (IPv6) 246
7.3.12.2 Adding an Address Pool (IPv6) 246
7.3.12.3 Deleting an Address Pool (IPv6) 247
7.3.13 Managing IP Ranges (IPv4) 248
7.3.13.1 Viewing a List of IP Ranges (IPv4) 248
7.3.13.2 Adding an IP Range (IPv4) 248
7.3.13.3 Deleting an IP Range (IPv4) 249
7.3.14 Managing IP Ranges (IPv6) 249
7.3.14.1 Viewing a List of IP Ranges (IPv6) 250
7.3.14.2 Adding an IP Range (IPv6) 250
7.3.14.3 Deleting an IP Range (IPv6) 251
7.3.15 Managing IPv6 Prefixes 251
7.3.15.1 Viewing a List of IPv6 Prefixes 251
7.3.15.2 Adding an IPv6 Prefix 252
7.3.15.3 Deleting an IPv6 Prefix 252
7.3.16 Managing Temporary Subnets 253
7.3.16.1 Viewing a List of Temporary Subnets 253
7.3.16.2 Adding a Temporary Subnet 253
7.3.16.3 Deleting a Temporary Subnet 254
7.3.17 Managing IPv6 Subnets 254
7.3.17.1 Viewing a List of IPv6 Subnets 254
7.3.17.2 Adding a IPv6 Subnet 255
7.3.17.3 Deleting an IPv6 Subnet 255
7.3.18 Managing Option 82 Classes for Address Pools 256
7.3.18.1 Viewing a List of Option 82 Classes for Address Pools 256
7.3.18.2 Adding an Option 82 Class to an Address Pool 257
7.3.18.3 Deleting an Option 82 Class From an Address Pool 257
7.3.19 Example: Configuring the Device as a DHCP Server to Support a Relay Agent 258
7.4 Managing Static DNS 262
7.4.1 Managing Domain Names 262
7.4.1.1 Viewing a List of Domain Names 262
7.4.1.2 Adding a Domain Name 262
7.4.1.3 Deleting a Domain Name 263
7.4.2 Managing Domain Name Servers 263
7.4.2.1 Viewing a List of Domain Name Servers 263
7.4.2.2 Adding a Domain Name Server 264
7.4.2.3 Deleting a Domain Name Server 264
7.5 Managing Dynamic DNS 264

7.5.1 Enabling and Configuring Dynamic DNS 265
7.5.2 Managing Dynamic DNS Servers 266
7.5.2.1 Viewing a List of Dynamic DNS Servers 266
7.5.2.2 Viewing the Status of a Dynamic DNS Server 266
7.5.2.3 Adding a Dynamic DNS Server 267
7.5.2.4 Deleting a Dynamic DNS Server 267
7.5.3 Managing Dynamic DNS Server Host Names 267
7.5.3.1 Viewing a List of Host Names 268
7.5.3.2 Adding a Host Name 268
7.5.3.3 Deleting a Host Name 269

Chapter 8
Layer 2 271
8.1 Managing Switched Ethernet Ports 271
8.1.1 Viewing a List of Switched Ethernet Ports 271
8.1.2 Configuring a Switched Ethernet Port 272
8.1.3 Viewing Switched Ethernet Port Statistics 276
8.1.4 Viewing the Status of a Switched Ethernet Port 276
8.1.5 Viewing RMON Port Statistics 277
8.1.6 Clearing Switched Ethernet Port Statistics 280
8.1.7 Resetting a Switched Ethernet Port 281
8.1.8 Testing Switched Ethernet Port Cables 281
8.1.8.1 Running a Cable Diagnostic Test 281
8.1.8.2 Viewing Cable Diagnostic Statistics 282
8.1.8.3 Clearing Cable Diagnostic Statistics 283
8.2 Managing Ethernet Trunk Interfaces 284
8.2.1 Viewing a List of Ethernet Trunk Interfaces 284
8.2.2 Adding an Ethernet Trunk Interface 284
8.2.3 Deleting an Ethernet Trunk Interface 286
8.2.4 Managing Ethernet Trunk Ports 287
8.2.4.1 Viewing a List of Ethernet Trunk Ports 287
8.2.4.2 Adding an Ethernet Trunk Port 287
8.2.4.3 Deleting an Ethernet Trunk Port 288
8.3 Managing MAC Addresses 288
8.3.1 Viewing a Dynamic List of MAC Addresses 288
8.3.2 Purging the Dynamic MAC Address List 289
8.3.3 Configuring MAC Address Learning Options 290
8.3.4 Managing Static MAC Addresses 290
8.3.4.1 Viewing a List of Static MAC Addresses 290
8.3.4.2 Adding a Static MAC Address 291
8.3.4.3 Deleting a Static MAC Address 291

8.4 Managing Multicast Filtering 292
8.4.1 Multicast Filtering Concepts 292
8.4.1.1 IGMP 292
8.4.1.2 GMRP (GARP Multicast Registration Protocol) 296
8.4.2 Enabling and Configuring GMRP 299
8.4.3 Managing IGMP Snooping 299
8.4.3.1 Configuring IGMP Snooping 299
8.4.3.2 Viewing a List of Router Ports 300
8.4.3.3 Adding a Router Port 300
8.4.3.4 Deleting a Router Port 301
8.4.4 Managing the Static Multicast Group Table 301
8.4.4.1 Viewing a List of Static Multicast Group Entries 301
8.4.4.2 Adding a Static Multicast Group Entry 302
8.4.4.3 Deleting a Static Multicast Group Entry 302
8.4.5 Managing Egress Ports for Multicast Groups 302
8.4.5.1 Viewing a List of Egress Ports 303
8.4.5.2 Adding an Egress Port 303
8.4.5.3 Deleting an Egress Port 303
8.4.6 Viewing a Summary of Multicast Groups 304
8.4.7 Viewing a List of IP Multicast Groups 304
8.5 Managing VLANs 305
8.5.1 VLAN Concepts 306
8.5.1.1 Tagged vs. Untagged Frames 306
8.5.1.2 Native VLAN 306
8.5.1.3 Edge and Trunk Port Types 307
8.5.1.4 Ingress Filtering 307
8.5.1.5 Forbidden Ports List 307
8.5.1.6 VLAN-Aware Mode of Operation 308
8.5.1.7 GARP VLAN Registration Protocol (GVRP) 308
8.5.1.8 PVLAN Edge 309
8.5.1.9 VLAN Advantages 310
8.5.2 Configuring the Internal VLAN Range 311
8.5.3 Enabling/Disabling Ingress Filtering 312
8.5.4 Managing VLANs for Switched Ethernet Ports 313
8.5.4.1 Viewing VLAN Assignments for Switched Ethernet Ports 313
8.5.4.2 Configuring VLANs for Switched Ethernet Ports 314
8.5.5 Managing Static VLANs 314
8.5.5.1 Viewing a List of Static VLANs 315
8.5.5.2 Adding a Static VLAN 315
8.5.5.3 Deleting a Static VLAN 316

8.5.6 Managing Forbidden Ports 316
8.5.6.1 Viewing a List of Forbidden Ports 316
8.5.6.2 Adding a Forbidden Port 317
8.5.6.3 Deleting a Forbidden Port 317
8.5.7 Managing VLANs for Interfaces and Tunnels 317

Chapter 9
Serial Server 319
9.1 Managing Serial Ports 319
9.1.1 Viewing a List of Serial Ports 319
9.1.2 Viewing Serial Port Statistics 320
9.1.3 Viewing Transport Connection Statistics 321
9.1.4 Viewing DNP Device Table Statistics 322
9.1.5 Clearing Serial Port Statistics 323
9.1.6 Configuring a Serial Port 323
9.1.7 Restarting the Serial Server 324
9.1.8 Resetting a Serial Port 324
9.2 Managing Serial Port Protocols 324
9.2.1 Serial Port Protocol Concepts 325
9.2.1.1 Raw Socket Applications 325
9.2.1.2 Modbus TCP Applications 326
9.2.1.3 DNP Applications 327
9.2.1.4 Incoming/Outgoing Serial Connections 328
9.2.2 Viewing a List of Serial Port Protocols 328
9.2.3 Adding a Serial Port Protocol 328
9.2.4 Configuring the DNP Protocol 329
9.2.5 Configuring the Modbus TCP Protocol 329
9.2.6 Configuring the Raw Socket Protocol 330
9.2.7 Deleting a Serial Port Protocol 331
9.3 Managing Device Address Tables 332
9.3.1 Viewing a List of Device Address Tables 332
9.3.2 Adding a Device Address Table 332
9.3.3 Deleting a Device Address Table 333
9.4 Managing Serial Multicast Streaming 333
9.4.1 Understanding Serial Multicast Streaming 334
9.4.1.1 Sink vs. Source Ports 334
9.4.1.2 Multicast Streaming Examples 334
9.4.2 Configuring Serial Multicast Streaming 335
9.4.3 Example: Serial Interfaces Configured as a Sink for Multicast Streams 335
9.4.4 Example: Serial Interfaces Configured as a Source for Multicast Streams 338
9.4.5 Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams 340

9.5 Managing Remote Hosts 343
9.5.1 Viewing a List of Remote Hosts 343
9.5.2 Adding a Remote Host 344
9.5.3 Deleting a Remote Host 344
9.6 Managing Local Hosts 345
9.6.1 Viewing a List of Local Hosts 345
9.6.2 Adding a Local Host 345
9.6.3 Deleting a Local Host 346
9.7 Managing Remote Host Interfaces 346
9.7.1 Viewing a List of Remote Host Interfaces 347
9.7.2 Adding a Remote Host Interface 347
9.7.3 Deleting a Remote Host Interface 348
9.8 Managing Local Host Interfaces 348
9.8.1 Viewing a List of Local Host Interfaces 348
9.8.2 Adding a Local Host Interface 349
9.8.3 Deleting a Local Host Interface 349

Chapter 10
Wireless 351
10.1 Managing the WLAN Interface 351
10.1.1 Enabling and Configuring the WLAN Interface 351
10.1.2 Managing Wireless Access Points 353
10.1.2.1 Viewing a List of Wireless Access Points 353
10.1.2.2 Viewing the Status of Wireless Access Points 354
10.1.2.3 Viewing the Status of WLAN Client Associations 355
10.1.2.4 Adding a Wireless Access Point 355
10.1.2.5 Configuring WPA-EAP 357
10.1.2.6 Deleting a Wireless Access Point 357
10.1.3 Managing WLAN Clients 357
10.1.3.1 Viewing a List of WLAN Clients 358
10.1.3.2 Viewing the Status of the WLAN Clients 358
10.1.3.3 Adding a WLAN Client 359
10.1.3.4 Configuring WPA-EAP Authentication 360
10.1.3.5 Adding a CA Certificate for WPA-EAP Authentication 361
10.1.3.6 Deleting a WLAN Client 361
10.1.3.7 Scanning for WLAN Clients 362
10.1.4 Example: Configuring a WLAN with a Firewall 362
10.2 Managing Cellular Modem Interfaces 365
10.2.1 Enabling/Disabling Cellular Modem Interfaces 366
10.2.2 Configuring a Cellular Modem Interface 366
10.2.3 Activating Dual SIM Cards 367

10.2.4 Viewing a List of Cellular Modem Interfaces 367
10.2.5 Viewing the Status of a Cellular Modem Interface 367
10.2.6 Viewing PPP Interface Statistics 368
10.3 Running AT Commands 369
10.4 Connecting as a PPP Client 369
10.5 Managing Cellular Modem Profiles 370
10.5.1 Viewing a List of GSM Profiles 370
10.5.2 Adding a GSM Profile 370
10.5.3 Deleting a GSM Profile 372
10.6 Managing the LTE Modem 372
10.6.1 Viewing LTE Cellular Modem Information 372
10.6.2 Configuring the LTE Modem 374
10.6.3 Enabling/Disabling the LTE Modem 375
10.6.4 Resetting the Cellular Modem 375
10.6.5 Enabling/Disabling GPS 376
10.6.6 Viewing the Configured GPS Mode 376
10.6.7 Enabling and Configuring GPS NMEA Data Streams 376
10.6.8 Changing the Active SIM Card 377
10.6.9 Managing Firmware Updates 378
10.6.9.1 Viewing the Firmware Update Status 378
10.6.9.2 Configuring the Firmware Update Mode and Source 379
10.6.9.3 Launching a Firmware Update 380

Chapter 11
Tunneling and VPNs 381
11.1 Managing Virtual Switches 381
11.1.1 Viewing a List of Virtual Switches 382
11.1.2 Adding a Virtual Switch 383
11.1.3 Deleting a Virtual Switch 384
11.1.4 Managing Virtual Switch Interfaces 384
11.1.4.1 Viewing a List of Virtual Switch Interfaces 384
11.1.4.2 Adding a Virtual Switch Interface 385
11.1.4.3 Deleting a Virtual Switch Interface 385
11.1.5 Filtering Virtual Switch Traffic 386
11.1.5.1 Enabling/Disabling Virtual Switch Filtering 386
11.1.5.2 Viewing a List of Virtual Switch Filters 386
11.1.5.3 Adding a Virtual Switch Filter 387
11.1.5.4 Deleting a Virtual Switch Filter 387
11.1.6 Managing Filtering Rules 388
11.1.6.1 Viewing a List of Rules 388
11.1.6.2 Viewing a List of Rules Assigned to a Virtual Switch Filter 388

11.1.6.3 Adding a Rule 389
11.1.6.4 Adding a Rule to a Virtual Switch Filter 390
11.1.6.5 Deleting a Rule 390
11.1.6.6 Deleting a Rule from a Virtual Switch Filter 390
11.1.7 Managing In/Out Interfaces 391
11.1.7.1 Viewing a List of In/Out Interfaces 391
11.1.7.2 Adding an In/Out Interface 392
11.1.7.3 Deleting an In/Out Interface 392
11.1.8 Managing VLANs for Virtual Switches 392
11.1.8.1 Viewing a List of Virtual Switch VLANs 393
11.1.8.2 Adding a Virtual Switch VLAN 393
11.1.8.3 Deleting a Virtual Switch VLAN 394
11.2 Managing the Layer2 Tunnel Daemon 394
11.2.1 Viewing Round Trip Time Statistics 394
11.2.2 Configuring the Layer 2 Tunnel Daemon 395
11.3 Managing L2TP Tunnels 396
11.3.1 Configuring L2TP Tunnels 396
11.3.2 Configuring DNS Servers 397
11.3.3 Configuring PPP Options 397
11.3.4 Configuring WINS Servers 398
11.4 Managing L2TPv3 Tunnels 398
11.4.1 L2TPv3 Tunnel Scenarios 399
11.4.2 Creating an L2TPv3 Tunnel 400
11.4.3 Managing Static L2TPv3 Tunnels 401
11.4.3.1 Enabling/Disabling Static L2TPv3 Tunnels 401
11.4.3.2 Viewing a List of Static L2TPv3 Tunnels 402
11.4.3.3 Adding a Static L2TPv3 Tunnel 402
11.4.3.4 Deleting a Static L2TPv3 Tunnel 403
11.4.4 Managing Dynamic L2TPv3 Tunnels 404
11.4.4.1 Enabling and Configuring Dynamic L2TPv3 Tunnels 404
11.4.4.2 Viewing a List of Dynamic L2TPv3 Tunnels 405
11.4.4.3 Adding a Dynamic L2TPv3 Tunnel 405
11.4.4.4 Deleting a Dynamic L2TPv3 Tunnel 407
11.4.5 Managing Sessions for L2TPv3 Tunnels 407
11.4.5.1 Viewing a List of Sessions 407
11.4.5.2 Adding a Session 408
11.4.5.3 Deleting a Session 409
11.4.6 Managing VLANs for L2TPv3 Tunnels 410
11.4.6.1 Viewing a List of VLANs 410
11.4.6.2 Adding a VLAN 410

11.4.6.3 Deleting a VLAN 411
11.5 Managing GOOSE Tunnels 411
11.5.1 Viewing the GOOSE Tunnel Statistics 412
11.5.2 Viewing a List of GOOSE Tunnels 413
11.5.3 Adding a GOOSE Tunnel 413
11.5.4 Deleting a GOOSE Tunnel 414
11.5.5 Managing Remote Daemons for GOOSE Tunnels 414
11.5.5.1 Viewing a List of Remote Daemons 415
11.5.5.2 Adding a Remote Daemon 415
11.5.5.3 Deleting a Remote Daemon 415
11.6 Managing Generic Tunnels 416
11.6.1 Viewing the Generic Tunnel Statistics 416
11.6.2 Viewing a List of Generic Tunnels 417
11.6.3 Adding a Generic Tunnel 417
11.6.4 Deleting a Generic Tunnel 418
11.6.5 Managing Remote Daemon IP Addresses for Generic Tunnels 418
11.6.5.1 Viewing a List of IP Addresses 419
11.6.5.2 Adding an IP Address 419
11.6.5.3 Deleting an IP Address 419
11.6.6 Managing Remote Daemon Egress Interfaces for Generic Tunnels 420
11.6.6.1 Viewing a List of Egress Interfaces 420
11.6.6.2 Adding an Egress Interface 420
11.6.6.3 Deleting an Egress Interface 421
11.6.7 Managing Ethernet Types for Generic Tunnels 421
11.6.7.1 Viewing a List of Ethernet Types 421
11.6.7.2 Adding an Ethernet Type 421
11.6.7.3 Deleting an Ethernet Type 422
11.7 Managing Generic Routing Encapsulation Tunnels 422
11.7.1 Viewing Statistics for GRE Tunnels 423
11.7.2 Viewing a List of GRE Tunnels 424
11.7.3 Adding a GRE Tunnel 425
11.7.4 Configuring a DSCP Marking for GRE Tunnel Traffic 426
11.7.5 Enabling/Disabling Keepalive Messages 426
11.7.6 Deleting a GRE Tunnel 427
11.7.7 Example: Configuring a GRE Tunnel with IPsec 428
11.8 Managing IPsec Tunnels 434
11.8.1 IPsec Tunneling Concepts 434
11.8.1.1 IPsec Modes 435
11.8.1.2 Supported Encryption Protocols 435
11.8.1.3 Public and Secret Key Cryptography 435

11.8.1.4 X509 Certificates 436
11.8.1.5 NAT Traversal 436
11.8.1.6 Remote IPsec Client Support 436
11.8.1.7 IPsec and Router Interfaces 437
11.8.2 Configuring IPsec Tunnels 437
11.8.3 Configuring Certificates and Keys 438
11.8.4 Viewing the IPsec Tunnel Status 438
11.8.5 Managing Pre-Shared Keys 439
11.8.5.1 Viewing a List of Pre-Shared Keys 440
11.8.5.2 Adding a Pre-Shared Key 440
11.8.5.3 Deleting a Pre-Shared Key 440
11.8.6 Managing Connections 441
11.8.6.1 Viewing a List of Connections 441
11.8.6.2 Adding a Connection 442
11.8.6.3 Configuring Dead Peer Detection 443
11.8.6.4 Deleting a Connection 444
11.8.6.5 Viewing the Status of a Connection 444
11.8.7 Managing the Internet Key Exchange (IKE) Protocol 445
11.8.7.1 Viewing a List of IKE Algorithms 445
11.8.7.2 Adding an IKE Algorithm 446
11.8.7.3 Deleting an IKE Algorithm 446
11.8.8 Managing the Encapsulated Security Payload (ESP) Protocol 447
11.8.8.1 Configuring ESP Encryption 447
11.8.8.2 Viewing a List of ESP Algorithms 447
11.8.8.3 Adding an ESP Algorithm 448
11.8.8.4 Deleting an ESP Algorithm 448
11.8.9 Configuring the Connection Ends 449
11.8.10 Managing Private Subnets 450
11.8.10.1 Configuring Private Subnets for Connection Ends 451
11.8.10.2 Viewing a List of Addresses for Private Subnets 451
11.8.10.3 Adding an Address for a Private Subnet 451
11.8.10.4 Deleting an Address for a Private Subnet 452
11.8.11 Example: Configuring an Encrypted VPN Tunnel 452
11.9 Managing 6in4 and 4in6 Tunnels 456
11.9.1 Enabling/Disabling 6in4 or 4in6 Tunnels 457
11.9.2 Viewing a List of 6in4 or 4in6 Tunnels 457
11.9.3 Viewing the Status of 6in4/4in6 Tunnels 457
11.9.4 Adding a 6in4 or 4in6 Tunnel 458
11.9.5 Deleting a 6in4 or 4in6 Tunnel 458
11.10 Managing DMVPN 459

11.10.1 Understanding DMVPN 459
11.10.2 Configuring DMVPN 461
11.10.3 Managing DMVPN Interfaces 461
11.10.3.1 Viewing a List of DMVPN Interfaces 461
11.10.3.2 Adding a DMVPN Interface 462
11.10.3.3 Deleting a DMVPN Interface 463
11.10.4 Viewing the Status of DMVPN 463

Chapter 12
Unicast and Multicast Routing 465
12.1 Viewing the Status of IPv4 Routes 465
12.2 Viewing the Status of IPv6 Routes 466
12.3 Viewing the Memory Statistics 467
12.4 Configuring ICMP 468
12.5 Managing Event Trackers 468
12.5.1 Viewing a List of Event Trackers 469
12.5.2 Viewing Event Tracker Statistics 469
12.5.3 Adding an Event Tracker 470
12.5.4 Deleting an Event Tracker 471
12.6 Managing IS-IS 471
12.6.1 IS-IS Concepts 472
12.6.1.1 IS-IS Routers 472
12.6.1.2 Network Entity Title (NET) Addresses 473
12.6.1.3 Advantages and Disadvantages of Using IS-IS 473
12.6.2 Configuring IS-IS 473
12.6.3 Viewing the Status of Neighbors 474
12.6.4 Viewing the Status of the Link-State Database 475
12.6.5 Managing Area Tags 476
12.6.5.1 Viewing a List of Area Tags 477
12.6.5.2 Adding an Area Tag 477
12.6.5.3 Deleting an Area Tag 479
12.6.6 Managing Interfaces 479
12.6.6.1 Viewing a List of Interfaces 479
12.6.6.2 Configuring an Interface 480
12.6.7 Managing LSP Generation 481
12.6.7.1 Viewing a List of LSP Generation Intervals 481
12.6.7.2 Adding an LSP Generation Interval 482
12.6.7.3 Deleting an LSP Generation Interval 482
12.6.8 Managing SPF Calculations 482
12.6.8.1 Viewing a List of SPF Calculation Intervals 483
12.6.8.2 Adding an SPF Calculation Interval 483

12.6.8.3 Deleting an SPF Calculation Interval 483
12.6.9 Managing the Lifetime of LSPs 484
12.6.9.1 Viewing a List of LSP Lifetime Intervals 484
12.6.9.2 Adding an LSP Lifetime Interval 485
12.6.9.3 Deleting an LSP Lifetime Interval 485
12.6.10 Managing LSP Refresh Intervals 485
12.6.10.1 Viewing a List of LSP Refresh Intervals 486
12.6.10.2 Adding an LSP Refresh Interval 486
12.6.10.3 Deleting an LSP Refresh Interval 487
12.6.11 Managing Network Entity Titles (NETs) 487
12.6.11.1 Viewing a List of NETs 488
12.6.11.2 Adding a NET 488
12.6.11.3 Deleting a NET 489
12.6.12 Managing Redistribution Metrics 489
12.6.12.1 Viewing a List of Redistribution Metrics 489
12.6.12.2 Adding a Redistribution Metric 490
12.6.12.3 Deleting a Redistribution Metric 490
12.7 Managing RIP 491
12.7.1 Configuring RIP 492
12.7.2 Viewing the Status of Dynamic RIP Routes 492
12.7.3 Managing Prefix Lists and Entries 494
12.7.3.1 Viewing a List of Prefix Lists 494
12.7.3.2 Viewing a List of Prefix Entries 495
12.7.3.3 Adding a Prefix List 495
12.7.3.4 Adding a Prefix Entry 495
12.7.3.5 Deleting a Prefix List 496
12.7.3.6 Deleting a Prefix Entry 496
12.7.4 Managing Networks 497
12.7.4.1 Configuring a Network 497
12.7.4.2 Tracking Commands 498
12.7.5 Managing Network IP Addresses 498
12.7.5.1 Viewing a List of Network IP Addresses 498
12.7.5.2 Adding a Network IP Address 499
12.7.5.3 Deleting a Network IP Address 499
12.7.6 Managing Network Interfaces 499
12.7.6.1 Viewing a List of Network Interfaces 500
12.7.6.2 Adding a Network Interface 500
12.7.6.3 Deleting a Network Interface 500
12.7.7 Managing Neighbors 501
12.7.7.1 Viewing a List of Neighbors 501

12.7.7.2 Adding a Neighbor 501
12.7.7.3 Deleting a Neighbor 501
12.7.8 Managing the Prefix List Distribution 502
12.7.8.1 Viewing a List of Prefix List Distribution Paths 502
12.7.8.2 Adding a Prefix List Distribution Path 502
12.7.8.3 Deleting a Prefix List Distribution Path 503
12.7.9 Managing Key Chains and Keys 503
12.7.9.1 Viewing a List of Key Chains 504
12.7.9.2 Viewing a List of Keys 504
12.7.9.3 Adding a Key Chain 504
12.7.9.4 Adding a Key 505
12.7.9.5 Deleting a Key Chain 506
12.7.9.6 Deleting a Key 506
12.7.10 Managing Redistribution Metrics 507
12.7.10.1 Viewing a List of Redistribution Metrics 507
12.7.10.2 Adding a Redistribution Metric 507
12.7.10.3 Deleting a Redistribution Metric 507
12.7.11 Managing Routing Interfaces 508
12.7.11.1 Viewing a List of Routing Interfaces 508
12.7.11.2 Configuring a Routing Interface 508
12.8 Managing BGP 509
12.8.1 Configuring BGP 510
12.8.2 Managing Route Maps 511
12.8.2.1 Viewing a List of Route Map Filters 512
12.8.2.2 Viewing a List of Route Map Filter Entries 512
12.8.2.3 Adding a Route Map Filter 512
12.8.2.4 Adding a Route Map Filter Entry 513
12.8.2.5 Deleting a Route Map Filter 513
12.8.2.6 Deleting a Route Map Filter Entry 514
12.8.2.7 Configuring Match Rules 514
12.8.2.8 Configuring a Set 515
12.8.3 Managing Prepended and Excluded Autonomous System Path Filters 515
12.8.3.1 Viewing a List of Prepended Autonomous System Path Filters 516
12.8.3.2 Viewing a List of Excluded Autonomous System Paths 516
12.8.3.3 Adding a Prepended Autonomous System Path Filter 516
12.8.3.4 Adding an Excluded Autonomous System Path filter 517
12.8.3.5 Deleting a Prepended Autonomous System Path Filter 517
12.8.3.6 Deleting an Excluded Autonomous System Path Filter 518
12.8.4 Managing Prefix Lists and Entries 518
12.8.4.1 Viewing a List of Prefix Lists 518

12.8.4.2 Viewing a List of Prefix Entries 519
12.8.4.3 Adding a Prefix List 519
12.8.4.4 Adding a Prefix Entry 520
12.8.4.5 Deleting a Prefix List 520
12.8.4.6 Deleting a Prefix Entry 521
12.8.5 Managing Autonomous System Paths and Entries 521
12.8.5.1 Viewing a List of Autonomous System Paths 521
12.8.5.2 Viewing a List of Autonomous System Path Entries 522
12.8.5.3 Adding an Autonomous System Path Filter 522
12.8.5.4 Adding an Autonomous System Path Filter Entry 522
12.8.5.5 Deleting an Autonomous System Path 523
12.8.5.6 Deleting an Autonomous System Path Filter Entry 523
12.8.6 Managing Neighbors 523
12.8.6.1 Viewing a List of Neighbors 524
12.8.6.2 Adding a Neighbor 524
12.8.6.3 Configuring the Distribution of Prefix Lists 525
12.8.6.4 Tracking Commands for BGP Neighbors 526
12.8.6.5 Deleting a Neighbor 526
12.8.7 Managing Networks 527
12.8.7.1 Viewing a List of Networks 527
12.8.7.2 Adding a Network 528
12.8.7.3 Tracking Commands for a BGP Network 528
12.8.7.4 Deleting a Network 528
12.8.8 Managing Aggregate Addresses 529
12.8.8.1 Viewing a List of Aggregate Addresses 529
12.8.8.2 Adding an Aggregate Address 529
12.8.8.3 Deleting an Aggregate Address 530
12.8.9 Managing Aggregate Address Options 530
12.8.9.1 Viewing a List of Aggregate Address Options 530
12.8.9.2 Adding an Aggregate Address Option 531
12.8.9.3 Deleting an Aggregate Address Option 531
12.8.10 Managing Redistribution Metrics 531
12.8.10.1 Viewing a List of Redistribution Metrics 531
12.8.10.2 Adding a Redistribution Metric 532
12.8.10.3 Deleting a Redistribution Metric 532
12.8.11 Managing Route Reflector Options 532
12.8.11.1 Understanding Route Reflectors 533
12.8.11.2 Configuring the Device as a Route Reflector 536
12.8.11.3 Configuring BGP Neighbors as Clients 536
12.8.11.4 Example: Basic Route Reflection 537

12.8.11.5 Example: Linking Clusters 539
12.8.11.6 Example: Clusters in Clusters 541
12.8.11.7 Example: Route Reflection in a VRF Instance 543
12.8.11.8 Example: Route Reflection with VPNv4 Clients 546
12.8.12 Viewing the Status of Dynamic BGP Routes 546
12.8.13 Resetting a BGP Session 549
12.9 Managing OSPF 550
12.9.1 OSPF Concepts 551
12.9.2 Configuring OSPF 551
12.9.3 Viewing the Status of Dynamic OSPF Routes 552
12.9.4 Managing Prefix Lists and Entries 554
12.9.4.1 Viewing a List of Prefix Lists 554
12.9.4.2 Viewing a List of Prefix Entries 555
12.9.4.3 Adding a Prefix List 556
12.9.4.4 Adding a Prefix Entry 556
12.9.4.5 Deleting a Prefix List 557
12.9.4.6 Deleting a Prefix Entry 557
12.9.5 Managing Areas 558
12.9.5.1 Viewing a List of Areas 558
12.9.5.2 Adding an Area 559
12.9.5.3 Deleting an Area 559
12.9.6 Managing Route Maps 560
12.9.6.1 Viewing a List of Route Map Filters 560
12.9.6.2 Viewing a List of Route Map Filter Entries 561
12.9.6.3 Adding a Route Map Filter 561
12.9.6.4 Adding a Route Map Filter Entry 562
12.9.6.5 Deleting a Route Map Filter 563
12.9.6.6 Deleting a Route Map Filter Entry 563
12.9.6.7 Configuring Match Rules 563
12.9.7 Managing Incoming Route Filters 564
12.9.7.1 Viewing List of Incoming Route Filters 564
12.9.7.2 Adding an Incoming Route Filter 565
12.9.7.3 Deleting an Incoming Route Filter 565
12.9.8 Managing Redistribution Metrics 566
12.9.8.1 Viewing a List of Redistribution Metrics 566
12.9.8.2 Adding a Redistribution Metric 566
12.9.8.3 Deleting a Redistribution Metric 567
12.9.9 Managing Routing Interfaces 567
12.9.9.1 Viewing a List of Routing Interfaces 568
12.9.9.2 Configuring a Routing Interface 568

12.9.10 Managing Message Digest Keys 570
12.9.10.1 Viewing a List of Message Digest Keys 571
12.9.10.2 Adding a Message Digest Key 571
12.9.10.3 Deleting a Message Digest Key 572
12.9.11 Managing ABR Route Summarization 572
12.9.11.1 Understanding ABR Route Summarization 573
12.9.11.2 Viewing a List of Summary Routes 573
12.9.11.3 Adding a Summary Route 573
12.9.11.4 Deleting a Summary Route 574
12.9.11.5 Example: Basic Route Summarization 574
12.10 Managing MPLS 576
12.10.1 Viewing the Status of IP Binding 576
12.10.2 Viewing the Status of the Forwarding Table 577
12.10.3 Enabling/Disabling MPLS 578
12.10.4 Managing the MPLS Interfaces 578
12.10.4.1 Viewing the Status of MPLS Interfaces 578
12.10.4.2 Viewing a List of MPLS Interfaces 579
12.10.4.3 Enabling/Disabling an MPLS Interface 579
12.10.5 Managing Static Label Binding 580
12.10.5.1 Viewing the Status of Static Label Binding 580
12.10.5.2 Viewing a List of Static Labels 580
12.10.5.3 Adding a Static Label 581
12.10.5.4 Deleting a Static Label 582
12.10.6 Managing Static Cross-Connects 582
12.10.6.1 Viewing the Status of Static Cross-Connects 582
12.10.6.2 Viewing a List of Static Cross-Connects 583
12.10.6.3 Adding a Static Cross-Connect 583
12.10.6.4 Deleting a Static Cross-Connect 584
12.10.7 Managing LDP 584
12.10.7.1 Viewing the Status of LDP Binding 585
12.10.7.2 Viewing the Status of the LDP Discovery Interfaces 585
12.10.7.3 Viewing the Status of the LDP Neighbor Local Node Information 586
12.10.7.4 Viewing the Status of the LDP Neighbor Connection Information 586
12.10.7.5 Viewing the Status of the LDP Neighbor Discovery Information 587
12.10.7.6 Configuring LDP 588
12.10.7.7 Configuring Neighbor Discovery 589
12.10.7.8 Viewing a List of LDP Interfaces 589
12.10.7.9 Enabling/Disabling an LDP Interface 589
12.11 Managing Virtual Routing and Forwarding (VRF) 590
12.11.1 VRF Concepts 591

12.11.1.1 VRF and VRF-Lite 591
12.11.1.2 Advantages and Disadvantages of Using VRF 591
12.11.2 Viewing VRF Interface Statistics 591
12.11.3 Configuring VRF 593
12.11.4 Configuring a VRF Interface 594
12.11.5 Managing VRF Definitions 594
12.11.5.1 Viewing a List of VRF Definitions 595
12.11.5.2 Adding a VRF Definition 595
12.11.5.3 Deleting a VRF Definition 596
12.11.6 Managing Route Targets 596
12.11.6.1 Viewing a List of Route Targets 597
12.11.6.2 Adding a Route Target 597
12.11.6.3 Deleting a Route Target 597
12.11.7 Managing VRF Instances and OSPF 598
12.11.7.1 Viewing a List of VRF Instances 598
12.11.7.2 Adding a VRF Instance and Configuring OSPF 598
12.11.7.3 Deleting a VRF Instance 600
12.11.8 Managing IP/VPN Tunnels 600
12.11.8.1 Viewing a List of IP/VPN Tunnels 601
12.11.8.2 Adding an IP/VPN Tunnel 601
12.11.8.3 Deleting an IP/VPN Tunnels 601
12.11.9 Managing VPNv4 Neighbors 602
12.11.9.1 Viewing a List of Neighbors 602
12.11.9.2 Adding a Neighbor 602
12.11.9.3 Deleting a Neighbor 603
12.11.10 Managing IPv4 Address Families 603
12.11.10.1 Viewing a List of IPv4 Address Families 603
12.11.10.2 Adding an IPv4 Address Family 604
12.11.10.3 Deleting an IPv4 Address Family 604
12.11.11 Managing Redistribution for IPv4 Address Families 605
12.11.11.1 Viewing a List of Redistributions 605
12.11.11.2 Adding a Redistribution 605
12.11.11.3 Deleting a Redistribution 606
12.11.12 Managing Neighbors for IPv4 Address Families 606
12.11.12.1 Viewing a List of Neighbors 607
12.11.12.2 Adding a Neighbor 607
12.11.12.3 Configuring the Distribution of Prefix Lists 608
12.11.12.4 Tracking Commands 609
12.11.12.5 Deleting a Neighbor 609
12.11.13 Managing Static VRF Routes 610

12.11.13.1 Viewing a List of Static VRF Routes 610
12.11.13.2 Adding a Static VRF Route 610
12.11.13.3 Configuring a Black Hole Connection for a Static VRF Route 611
12.11.13.4 Deleting a Static VRF Route 611
12.11.14 Managing Gateways for Static VRF Routes 612
12.11.14.1 Viewing a List of Gateways for Static VRF Routes 612
12.11.14.2 Adding a Gateway for a Static VRF Route 612
12.11.14.3 Deleting a Gateway for a Static VRF Route 613
12.11.15 Managing Interfaces for Static VRF Routes 613
12.11.15.1 Viewing a List of Interfaces for Static VRF Routes 613
12.11.15.2 Adding a Gateway for a Static VRF Route 614
12.11.15.3 Deleting a Gateway for a Static VRF Route 614
12.12 Managing Static Routing 615
12.12.1 Viewing a List of Static Routes 615
12.12.2 Adding an IPv4 Static Route 615
12.12.3 Adding an IPv6 Static Route 616
12.12.4 Deleting a Static Route 617
12.12.5 Configuring a Black Hole Connection for an IPv4 Static Route 617
12.12.6 Managing Gateways for Static Routes 617
12.12.6.1 Configuring Gateways for IPv6 Static Routes 618
12.12.6.2 Viewing a List of Gateways for IPv4 Static Routes 618
12.12.6.3 Adding a Gateway for an IPv4 Static Route 618
12.12.6.4 Deleting a Gateway for an IPv4 Static Route 619
12.12.7 Managing Interfaces for Static Routes 619
12.12.7.1 Configuring Interfaces for IPv6 Static Routes 619
12.12.7.2 Viewing a List of Interfaces for IPv4 Static Routes 620
12.12.7.3 Adding an Interface for an IPv4 Static Route 620
12.12.7.4 Deleting an Interface for an IPv4 Static Route 621
12.13 Managing Static Multicast Routing 621
12.13.1 Enabling/Disabling Static Multicast Routing 621
12.13.2 Managing Static Multicast Groups 622
12.13.2.1 Viewing a List of Static Multicast Groups 622
12.13.2.2 Adding a Static Multicast Group 622
12.13.2.3 Deleting a Static Multicast Group 623
12.13.3 Managing Out-Interfaces 623
12.13.3.1 Viewing a List of Out-Interfaces 623
12.13.3.2 Adding an Out-Interface 624
12.13.3.3 Deleting an Out-Interface 624
12.14 Managing Dynamic Multicast Routing 624
12.14.1 PIM-SM Concepts 626

12.14.2 Viewing the Status of PIM-SM 626
12.14.3 Viewing the Status of Dynamic Multicast Routing 630
12.14.4 Configuring PIM-SM 630
12.14.5 Setting the Device as a BSR Candidate 631
12.14.6 Setting the Device as an RP Candidate 631
12.14.7 Managing PIM-SM Interfaces 632
12.14.7.1 Viewing a List of PIM-SM Interfaces 632
12.14.7.2 Enabling/Disabling a PIM-SM Interface 633
12.14.8 Managing Static RP Addresses 633
12.14.8.1 Viewing a List of Static RP Addresses 633
12.14.8.2 Adding a Static RP Address 634
12.14.8.3 Deleting a Static RP Address 634
12.14.9 Managing Multicast Group Prefixes 635
12.14.9.1 Viewing a List of Multicast Group Prefixes 635
12.14.9.2 Adding a Multicast Group Prefix 635
12.14.9.3 Deleting a Multicast Group Prefix 636

Chapter 13
Network Redundancy 637
13.1 Managing VRRP 637
13.1.1 VRRP Concepts 638
13.1.1.1 Static Routing vs. VRRP 638
13.1.1.2 VRRP Terminology 638
13.1.1.3 Connection Synchronization 641
13.1.2 Viewing the Status of VRRP 641
13.1.3 Enabling/Disabling VRRP 642
13.1.4 Managing VRRP Trackers 642
13.1.4.1 Viewing a List of VRRP Trackers 643
13.1.4.2 Adding a VRRP Tracker 643
13.1.4.3 Deleting a VRRP Tracker 644
13.1.5 Managing VRRP Groups 644
13.1.5.1 Viewing a List of VRRP Groups 644
13.1.5.2 Adding a VRRP Group 645
13.1.5.3 Deleting a VRRP Group 645
13.1.6 Managing VRRP Instances 645
13.1.6.1 Viewing a List of VRRP Instances 646
13.1.6.2 Adding a VRRP Instance 646
13.1.6.3 Deleting a VRRP Instance 648
13.1.7 Managing VRRP Monitors 648
13.1.7.1 Viewing a List of VRRP Monitors 648
13.1.7.2 Adding a VRRP Monitor 649

13.1.7.3 Deleting a VRRP Monitor 649
13.1.8 Managing Track Scripts 650
13.1.8.1 Viewing a List of Track Scripts 650
13.1.8.2 Adding a Track Script 650
13.1.8.3 Deleting a Track Script 651
13.1.9 Managing Virtual IP Addresses 651
13.1.9.1 Viewing a List of Virtual IP Addresses 651
13.1.9.2 Adding a Virtual IP Address 652
13.1.9.3 Deleting a Virtual IP Address 652
13.1.10 Managing Connection Synchronization 652
13.1.10.1 Configuring Connection Synchronization 653
13.1.10.2 Enabling/Disabling Connection Synchronization 653
13.1.10.3 Viewing a List of Dedicated LInks 654
13.1.10.4 Adding a Dedicated Link 654
13.1.10.5 Deleting a Dedicated Link 655
13.1.10.6 Selecting a Default Dedicated Link 655
13.1.10.7 Viewing the Status of Each Dedicated Link 655
13.2 Managing VRRP within VRF 656
13.2.1 Configuring VRRP within VRF 657
13.2.2 Viewing the VRRP Status for a VRF 657
13.2.3 Configuring VRRP Service for a VRF 658
13.2.3.1 Viewing a List of VRFs Configured with VRRP Service 658
13.2.3.2 Adding VRRP Service to a VRF 659
13.2.3.3 Deleting VRRP Service from a VRF 659
13.2.4 Managing VRRP Trackers for a VRF 660
13.2.4.1 Viewing a List of VRRP Trackers for a VRF 660
13.2.4.2 Adding a VRRP Tracker for a VRF 660
13.2.4.3 Deleting a VRRP Tracker for a VRF 661
13.2.5 Managing VRRP Groups for a VRF 662
13.2.5.1 Viewing a List of VRRP Groups for a VRF 662
13.2.5.2 Adding a VRRP Group for a VRF 662
13.2.5.3 Deleting a VRRP Group 663
13.2.6 Managing VRRP Instances for a VRF 663
13.2.6.1 Viewing a List of VRRP Instances for a VRF 663
13.2.6.2 Adding a VRRP Instance for a VRF 664
13.2.6.3 Deleting a VRRP Instance for a VRF 665
13.2.7 Managing VRRP Monitors for a VRF 665
13.2.7.1 Viewing a List of VRRP Monitors for a VRF 665
13.2.7.2 Adding a VRRP Monitor to a VRF 666
13.2.7.3 Deleting a VRRP Monitor from a VRF 666

13.2.8 Managing VRRP Track Scripts for a VRF 667
13.2.8.1 Viewing a List of VRRP Track Scripts for a VRF 667
13.2.8.2 Adding a VRRP Track Script to a VRF 667
13.2.8.3 Deleting a VRRP Track Script from a VRF 668
13.2.9 Managing Virtual IP Addresses for a VRF 668
13.2.9.1 Viewing a List of Virtual IP Addresses 669
13.2.9.2 Adding a Virtual IP Address to a VRF 669
13.2.9.3 Deleting a Virtual IP Address from a VRF 669
13.2.10 Example: Configuring VRRP within a VRF 670
13.3 Managing Link Failover Protection 673
13.3.1 Viewing the Link Failover Log 673
13.3.2 Viewing the Link Failover Status 674
13.3.3 Managing Link Failover Parameters 675
13.3.3.1 Viewing a List of Link Failover Parameters 675
13.3.3.2 Adding a Link Failover Parameter 675
13.3.3.3 Deleting a Link Failover Parameter 676
13.3.4 Managing Link Failover Backup Interfaces 677
13.3.4.1 Viewing a List of Link Failover Backup Interfaces 677
13.3.4.2 Adding a Link Failover Backup Interface 677
13.3.4.3 Deleting a Link Failover Backup Interface 678
13.3.5 Managing Link Failover Ping Targets 679
13.3.5.1 Viewing a List of Link Failover Ping Targets 679
13.3.5.2 Adding a Link Failover Ping Target 679
13.3.5.3 Deleting a Link Failover Ping target 680
13.3.6 Testing Link Failover 680
13.3.7 Canceling a Link Failover Test 681
13.4 Managing Spanning Tree Protocol 681
13.4.1 RSTP Operation 681
13.4.1.1 RSTP States and Roles 682
13.4.1.2 Edge Ports 683
13.4.1.3 Point-to-Point and Multipoint Links 684
13.4.1.4 Path and Port Costs 684
13.4.1.5 Bridge Diameter 685
13.4.1.6 eRSTP 685
13.4.1.7 Fast Root Failover 685
13.4.2 RSTP Applications 686
13.4.2.1 RSTP in Structured Wiring Configurations 687
13.4.2.2 RSTP in Ring Backbone Configurations 688
13.4.2.3 RSTP Port Redundancy 690
13.4.3 MSTP Operation 690

13.4.3.1 MSTP Regions and Interoperability 691
13.4.3.2 MSTP Bridge and Port Roles 692
13.4.3.3 Benefits of MSTP 693
13.4.3.4 Implementing MSTP on a Bridged Network 694
13.4.4 Configuring STP Globally 694
13.4.5 Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces 697
13.4.6 Managing Multiple Spanning Tree Instances Globally 698
13.4.6.1 Viewing Statistics for Multiple Spanning Tree Instances 698
13.4.6.2 Viewing a List of Multiple Spanning Tree Instances 700
13.4.6.3 Adding a Multiple Spanning Tree Instance 700
13.4.6.4 Deleting a Multiple Spanning Tree Instance 701
13.4.7 Managing Multiple Spanning Tree Instances Per-Port 701
13.4.7.1 Viewing Per-Port Multiple Spanning Tree Instance Statistics 702
13.4.7.2 Viewing a List of Per-Port Multiple Spanning Tree Instances 703
13.4.7.3 Adding a Port-Specific Multiple Spanning Tree Instance 704
13.4.7.4 Deleting a Port-Specific Multiple Spanning Tree Instances 705
13.4.8 Viewing the Status of RSTP 706
13.4.9 Viewing RSTP Per-Port Statistics 708
13.4.10 Clearing Spanning Tree Protocol Statistics 710

Chapter 14
Network Discovery and Management 711
14.1 Managing LLDP 711
14.1.1 Configuring LLDP 712
14.1.2 Viewing Global Statistics and Advertised System Information 713
14.1.3 Viewing Statistics for LLDP Neighbors 715
14.1.4 Viewing Statistics for LLDP Ports 719
14.2 Managing SNMP 720
14.2.1 MIB Files and SNMP Traps 721
14.2.2 Enabling and Configuring SNMP Sessions 722
14.2.3 Viewing Statistics for SNMP 724
14.2.4 Discovering SNMP Engine IDs 725
14.2.5 Managing SNMP Communities 725
14.2.5.1 Viewing a List of SNMP Communities 726
14.2.5.2 Adding an SNMP Community 726
14.2.5.3 Deleting an SNMP Community 726
14.2.6 Managing SNMP Target Addresses 727
14.2.6.1 Viewing a List of SNMP Target Addresses 727
14.2.6.2 Adding an SNMP Target Address 727
14.2.6.3 Deleting an SNMP Target Address 729
14.2.7 Managing SNMP Users 729

14.2.7.1 Viewing a List of SNMP Users 730
14.2.7.2 Adding an SNMP User 730
14.2.7.3 Deleting an SNMP User 731
14.2.8 Managing SNMP Security Model Mapping 731
14.2.8.1 Viewing a List of SNMP Security Models 732
14.2.8.2 Adding an SNMP Security Model 732
14.2.8.3 Deleting an SNMP Security Model 732
14.2.9 Managing SNMP Group Access 733
14.2.9.1 Viewing a List of SNMP Groups 733
14.2.9.2 Adding an SNMP Group 733
14.2.9.3 Deleting an SNMP Group 734
14.3 Managing NETCONF 735
14.3.1 Enabling and Configuring NETCONF Sessions 735
14.3.2 Viewing NETCONF Statistics 736

Chapter 15
Traffic Control and Classification 739
15.1 Managing Port Mirroring 739
15.1.1 Configuring Port Mirroring 740
15.1.2 Managing Egress Source Ports 740
15.1.2.1 Viewing a List of Egress Source Ports 741
15.1.2.2 Adding an Egress Source Port 741
15.1.2.3 Deleting an Egress Source Port 741
15.1.3 Managing Ingress Source Ports 742
15.1.3.1 Viewing a List of Ingress Source Ports 742
15.1.3.2 Adding an Ingress Source Port 742
15.1.3.3 Deleting an Ingress Source Port 742
15.2 Managing Traffic Control 743
15.2.1 Enabling and Configuring Traffic Control 743
15.2.2 Managing Traffic Control Interfaces 745
15.2.2.1 Viewing a List of Traffic Control Interfaces 745
15.2.2.2 Adding a Traffic Control Interface 745
15.2.2.3 Deleting a Traffic Control Interface 746
15.2.3 Managing Traffic Control Priorities 747
15.2.3.1 Viewing a List of Traffic Control Priorities 747
15.2.3.2 Adding a Traffic Control Priority 748
15.2.3.3 Deleting a Traffic Control Priority 749
15.2.4 Managing Traffic Control Classes 749
15.2.4.1 Viewing a List of Traffic Control Classes 749
15.2.4.2 Adding a Traffic Control Class 750
15.2.4.3 Deleting a Traffic Control Class 751

15.2.5 Managing Traffic Control Devices 751
15.2.5.1 Viewing a List of Traffic Control Devices 752
15.2.5.2 Adding a Traffic Control Device 752
15.2.5.3 Deleting a Traffic Control Device 753
15.2.6 Managing Traffic Control Rules 753
15.2.6.1 Viewing a List of Traffic Control Rules 754
15.2.6.2 Adding a Traffic Control Rule 754
15.2.6.3 Configuring QoS Marking 756
15.2.6.4 Deleting aTraffic Control Rule 759
15.2.7 Managing QoS Mapping for VLANs 759
15.2.7.1 Viewing a List of QoS Maps for VLANs 760
15.2.7.2 Adding a QoS Map 760
15.2.7.3 Deleting a QoS Map 761
15.2.8 Managing Egress Markers for QoS Maps 761
15.2.8.1 Viewing a List of Egress Marks 762
15.2.8.2 Adding an Egress Mark 762
15.2.8.3 Deleting an Egress Mark 763
15.2.9 Viewing QoS Statistics 763
15.3 Managing Classes of Service 764
15.3.1 Configuring Classes of Service 765
15.3.2 Managing Priority-to-CoS Mapping 766
15.3.2.1 Viewing a List of Priority-to-CoS Mapping Entries 766
15.3.2.2 Adding a Priority-to-CoS Mapping Entry 766
15.3.2.3 Deleting a Priority-to-CoS Mapping Entry 767
15.3.3 Managing DSCP-to-CoS Mapping 767
15.3.3.1 Viewing a List of DSCP-to-CoS Mapping Entries 767
15.3.3.2 Adding a DSCP-to-CoS Mapping Entry 768
15.3.3.3 Deleting a DSCP-to-CoS Mapping Entry 768
15.4 Managing NetFlow Data Export 769
15.4.1 Understanding NetFlow Data Export 769
15.4.1.1 Flow Records 770
15.4.2 Configuring NetFlow Data Export 771
15.4.3 Enabling/Disabling NetFlow 771
15.4.4 Setting the NetFlow Engine ID 771
15.4.5 Controlling the NetFlow Cache 772
15.4.6 Controlling Active/Inactive Flows 772
15.4.7 Managing NetFlow Interfaces 773
15.4.7.1 Viewing a List of NetFlow Interfaces 773
15.4.7.2 Adding a NetFlow Interface 773
15.4.7.3 Deleting a NetFlow Interface 774

15.4.8 Managing NetFlow Collectors 774
15.4.8.1 Viewing a List of NetFlow Collectors 774
15.4.8.2 Adding a NetFlow Collector 775
15.4.8.3 Enabling/Disabling a NetFlow Collector 775
15.4.8.4 Deleting a NetFlow Collector 775
15.4.9 Viewing the Status of NetFlow 776
15.4.10 Example: Exporting Flows to Multiple Collectors 776
15.5 Managing Port Rate Limiting 778
15.5.1 Understanding Port Rate Limiting 778
15.5.2 Configuring Port Rate Limiting 778

Chapter 16
Time Services 781
16.1 Configuring the Time Synchronization Settings 781
16.2 Configuring the System Time and Date 782
16.3 Configuring the System Time Zone 782
16.4 Configuring the Local Time Settings 782
16.5 Enabling and Configuring the NTP Service 783
16.6 Viewing the NTP Service Status 783
16.7 Viewing the Status of Reference Clocks 785
16.8 Managing NTP Servers 786
16.8.1 Viewing a List of NTP Servers 786
16.8.2 Monitoring Subscribers 787
16.8.3 Adding an NTP Server 788
16.8.4 Deleting an NTP Server 789
16.8.5 Managing Server Keys 789
16.8.5.1 Viewing a List of Server Keys 789
16.8.5.2 Adding a Server Key 790
16.8.5.3 Deleting a Server Key 790
16.8.6 Managing Server Restrictions 790
16.8.6.1 Viewing a List of Server Restrictions 791
16.8.6.2 Adding a Server Restriction 791
16.8.6.3 Deleting a Server Restriction 792
16.9 Managing NTP Broadcast/Multicast Clients 792
16.9.1 Enabling and Configuring NTP Multicast Clients 793
16.9.2 Enabling and Configuring NTP Broadcast Clients 793
16.9.3 Managing NTP Broadcast/Multicast Addresses 793
16.9.3.1 Viewing a List of Broadcast/Multicast Addresses 794
16.9.3.2 Adding a Broadcast/Multicast Address 794
16.9.3.3 Deleting a Broadcast/Multicast Address 795

Chapter 17
Virtualization 797
17.1 Configuring Virtualization 798
17.2 Enabling/Disabling the Virtualization Service 798
17.3 Configuring Global Settings 799
17.4 Issuing VM Commands 799
17.5 Assigning a Network Interface 800
17.6 Accessing the Active Virtual Machine 801
17.7 Querying the Device Serial Number 801
17.8 Managing Virtual Machines 802
17.8.1 Building/Obtaining a Virtual Machine Image 802
17.8.2 Determining the Active Virtual Machine 802
17.8.3 Viewing a List of Virtual Machine Names 803
17.8.4 Adding a Virtual Machine 803
17.8.5 Extracting a Virtual Machine Archive 804
17.8.6 Loading an Existing Virtual Machine Image 805
17.8.7 Deleting a Virtual Machine 805
17.8.8 Deleting a Virtual Machine Archive 806
17.8.9 Starting a Virtual Machine 806
17.8.10 Stopping a Virtual Machine 806
17.9 Managing Serial Port Assigments 806
17.9.1 Assigning a Serial Port 807
17.9.2 Unassigning a Serial Port 807
17.10 Managing Virtual Interfaces 808
17.10.1 Viewing a List of Virtual Interfaces 808
17.10.2 Adding a Virtual Interface 808
17.10.3 Enabling/Disabling the VPE Network Interface 809
17.10.4 Deleting a Virtual Interface 809
17.11 Managing VPE Adapters 809
17.11.1 Viewing the Status of the VPE Adapter 810
17.11.2 Configuring a VPE Adapter 810
17.11.3 Starting/Stopping a VPE Adapter 811
17.12 Example: Enabling a Virtual Machine to Access a WLAN via a WLAN Client Interface 812

Chapter 18
Applications 819
18.1 Viewing a List of Installed Applications 819
18.2 Installing an Application 819
18.3 Upgrading an Application 820
18.4 Uninstalling an Application 820

18.5 Managing Application Repositories 821
18.5.1 Viewing a List of Repositories 821
18.5.2 Checking the Repository Connection 821
18.5.3 Adding a Repository 822
18.5.4 Deleting a Repository 822
18.6 Managing the RUGGEDCOM CROSSBOW Application 823
18.6.1 Enabling/Disabling CROSSBOW 823
18.6.2 Configuring the Client Connection 824
18.6.3 Configuring CROSSBOW Certificates and Private Keys 824
18.6.4 Managing SAC Connections 825
18.6.4.1 Viewing a List of SAC Connections 825
18.6.4.2 Adding a SAC Connection 825
18.6.4.3 Deleting a SAC Connection 826
18.6.5 Managing CROSSBOW CA Certificate Lists 826
18.6.5.1 Viewing a List of RUGGEDCOM CROSSBOW Certificate Lists 826
18.6.5.2 Adding a CA Certificate List 826
18.6.5.3 Deleting a CA Certificate List 827
18.6.6 Viewing the Status of RUGGEDCOM CROSSBOW 827
18.6.7 Viewing the RUGGEDCOM CROSSBOW Log 827

Chapter 19
Troubleshooting 829
19.1 Ethernet Ports 829
19.2 Multicast Filtering 830
19.3 Spanning Tree 830
19.4 VLANs 832
19.5 Firmware Updates 832

Preface

This guide describes the CLI user interface for RUGGEDCOM ROX II v2.13 running on the RUGGEDCOM RX1400. 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.

CONTENTS

- "Conventions"
- "Related Documents"
- "System Requirements"
- "Accessing Documentation"
- "License Conditions"
- "Training"
- "Customer Support"

Conventions

This CLI User Guide uses the following conventions to present information clearly and effectively.

Alerts

The following types of alerts are used when necessary to highlight important information.

DANGER!
DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.

WARNING!
WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.

CAUTION!
CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.

IMPORTANT!
IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.

NOTE
NOTE alerts provide additional information, such as facts, tips and details.

CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
command	Commands are in bold.
command parameter	Parameters are in plain text.
command parameter1 parameter2	Parameters are listed in the order they must be entered.
command parameter1 *parameter2*	Parameters in italics must be replaced with a user-defined value.
command [parameter1 | parameter2]	Alternative parameters are separated by a vertical bar (|). Square brackets indicate a required choice between two or more parameters.
command { parameter3 | parameter4 }	Curly brackets indicate an optional parameter(s).
command parameter1 parameter2 { parameter3 | parameter4 }	All commands and parameters are presented in the order they must be entered.

Related Documents

The following are other documents related to this product that may be of interest. Unless indicated otherwise, each document is available on the Siemens Industry Online Support (SIOS) [https://support.industry.siemens.com] website.

NOTE
Documents listed are those available at the time of publication. Newer versions of these documents or their associated products may be available. For more information, visit SIOS or consult a Siemens Customer Support representative.

Product Notes

Product notes are available online via SIOS [https://support.industry.siemens.com/cs/ca/en/ps/16008/pm].

User/Reference Guides

Document Title	Link
RUGGEDCOM ROX II v2.13 Web Interface User Guide	https://support.industry.siemens.com/cs/ww/en/view/109481696
RUGGEDCOM ROX II NETCONF Reference Guide	https://support.industry.siemens.com/cs/ww/en/view/109737085
RUGGEDCOM NMS v2.1 User Guide for Windows	https://support.industry.siemens.com/cs/ww/en/view/109737564
RUGGEDCOM NMS v2.1 User Guide for Linux	https://support.industry.siemens.com/cs/ww/en/view/109737563

Document Title	Link
RUGGEDCOM CROSSBOW User Guide	Available upon request

Catalogs

Document Title	Link
RUGGEDCOM SFP Transceivers Catalog	https://support.industry.siemens.com/cs/ww/en/view/109482309

FAQs/Application Examples

Document Title	Link
How to Upgrade the U-Boot Binary?	https://support.industry.siemens.com/cs/ww/en/view/109738243
Mean Time Between Failures (MTBF) – List for RUGGEDCOM Products	https://support.industry.siemens.com/cs/ww/en/view/109479200
How Can You Upgrade the GNU C Library? (Security Advisory SSA-994726)	https://support.industry.siemens.com/cs/ww/en/view/109474273
How Do You Calculate the Latency on a Switched Ethernet Network with RUGGEDCOM Switches or Routers?	https://support.industry.siemens.com/cs/ww/en/view/94772587
What Should You Watch Out For When Configuring a Link Aggregation Between SCALANCE X Switches and RUGGEDCOM Switches?	https://support.industry.siemens.com/cs/ww/en/view/76798136
What Should You Watch Out For When Ordering and Installing Interface Modules For RUGGEDCOM Switches?	https://support.industry.siemens.com/cs/ww/en/view/77896782
What Options Do You Have For Connecting an (R)STP Segment To a Ring Structure and How Can You Reduce the Ring Reconfiguration Time Through the EPLC Procedure?	https://support.industry.siemens.com/cs/ww/en/view/77363773
How to Implement Robust Ring Networks using RSTP and eRSTP?	https://support.industry.siemens.com/cs/ww/en/view/109738240
How to Change the Log Level?	https://support.industry.siemens.com/cs/ww/en/view/109744203
What is the Difference Between RSTP (Rapid Spanning Tree Protocol) and eRSTP (enhanced Rapid Spanning Tree Protocol 4) PBDU (Bridge Protocol Data Unit)?	https://support.industry.siemens.com/cs/ww/en/view/109476379
How to Regenerate Keys and Certificates?	https://support.industry.siemens.com/cs/ww/en/view/109738241
Using BGP Route Reflection with VPNv4 Clients	https://support.industry.siemens.com/cs/ww/en/view/109757209
Building a Linux-Based Virtual Machine Image	https://support.industry.siemens.com/cs/ww/en/view/109482423
How to Control Bidirectional Traffic when Using Port Mirroring	https://support.industry.siemens.com/cs/ww/en/view/109759351

Installation Guides

Document Title	Link
RUGGEDCOM RX1400 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109480955

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 RX1400
- 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 v2.13 is available online at https://www.siemens.com/ruggedcom. 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
```

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.

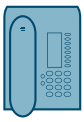
For more information about training services and course availability, visit https://www.siemens.com/ruggedcom or contact a Siemens Sales representative.

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:

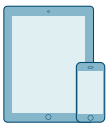
Online

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 http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.



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

1 Introduction

Welcome to the RUGGEDCOM ROX II (Rugged Operating System on Linux®) v2.13 CLI User Guide for the RUGGEDCOM RX1400. This document details how to configure the RX1400 via the RUGGEDCOM ROX II Command Line Interface (CLI). RUGGEDCOM ROX II also features a Web interface, which is described in a separate CLI User Guide.

IMPORTANT!
This CLI User Guide describes all features of RUGGEDCOM ROX II, but some features can only be configured through the Web interface. This is indicated throughout the CLI User Guide where applicable.

CONTENTS

- Section 1.1, “Features and Benefits”
- Section 1.2, “Feature Keys”
- Section 1.3, “Security Recommendations”
- Section 1.4, “Available Services by Port”
- Section 1.5, “User Permissions”
- Section 1.6, “Removable Memory”
- Section 1.7, “Logged Events”

Section 1.1

Features and Benefits

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
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

- **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.
- **Simple Network Management Protocol (SNMP)**
  SNMP provides a standardized method for network management stations to interrogate devices from different vendors. RUGGEDCOM ROX II supports v1, v2c and v3. SNMPv3 is generally recommended, as it provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions.

  RUGGEDCOM ROX II also supports numerous standard MIBs (Management Information Base) allowing 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. RUGGEDCOM 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.
- **Remote Monitoring and Configuration with RUGGEDCOM NMS**
  RUGGEDCOM NMS (RNMS) 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.

  RNMS is especially suited for remotely monitoring and configuring RUGGEDCOM routers, switches, serial servers and WiMAX wireless network equipment. For more information, contact a Siemens Sales representative.
- **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* available on https://www.siemens.com/ruggedcom.
- **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 or Cellular. 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.
- **MicroSD/MicroSDHC Support**
  Use a removable microSD or microSDHC Flash drive to manage important files and configure RUGGEDCOM ROX II.
  - Upgrade/Downgrade Firmware – Use the microSD or microSDHC Flash 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 microSD or microSDHC Flash drive, such as rollbacks, log files, feature keys and configuration files.
  - Share Files – Quickly configure or upgrade other RUGGEDCOM RX1400 devices by copying files using the same microSD/microSDHC Flash drive.

  IMPORTANT!
  Do not remove the microSD or microSDHC Flash drive during a file transfer.

  NOTE
  Only one partition is supported on the microSD/microSDHC Flash drive.
- **Virtual Machine Support**
  Utilize the built-in virtualization environment to run a guest Linux operating system and third-party applications on the device, enabling intelligence at the network edge.
- **Hot Swapping SFP Transceivers**
  SFP transceivers can be safely replaced with 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 an SFP transceiver with a different type, such as a 1000Base-X transceiver with a 100Base-FX transceiver.

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

  NOTE
  A reboot is required if an SFP transceiver is installed in a socket that was empty when the device was started.

Section 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:

- 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 new RUGGEDCOM RX1400 is ordered with a base feature key, which is permanently installed on the device. Additional feature keys can be installed on the microSD/microSDHC drive, which allows them to be moved to other devices when needed.

NOTE
Each feature key is signed with the serial number of the device it is intended to be used in. Feature keys can be used in other RUGGEDCOM ROX II devices, but a low-level alarm will be generated indicating a hardware mismatch.

Feature keys include the following features:

Feature	Feature Key				
	Layer 2 Standard Edition (L2SE)	L3SEL3HW	L3SEL2HW	L3SECL3HW	L3SECL2HW
VLANs (802.1Q)	✓	✓	✓	✓	✓
QoS (802.1p)	✓	✓	✓	✓	✓
MSTP (802.1Q-2005)	✓	✓	✓	✓	✓
RSTP	✓	✓	✓	✓	✓
eRSTP™	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓
L2TPv2 and L2TPv3	✓	✓	✓	✓	✓
Port Rate Limiting	✓	✓	✓	✓	✓
Broadcast Storm Filtering	✓	✓	✓	✓	✓
Port Mirroring	✓	✓	✓	✓	✓
SNMP v1/v2/v3	✓	✓	✓	✓	✓
RMON	✓	✓	✓	✓	✓
CLI	✓	✓	✓	✓	✓
HTML User Interface	✓	✓	✓	✓	✓
MPLS		✓	✓	✓	✓
DHCP		✓	✓	✓	✓
VRRPv2 and VRRPv3		✓	✓	✓	✓

Feature	Feature Key				
	Layer 2 Standard Edition (L2SE)	L3SEL3HW	L3SEL2HW	L3SECL3HW	L3SECL2HW
PIM-SM		✓	✓	✓	✓
Firewall		✓	✓	✓	✓
OSPF		✓	✓	✓	✓
BGP		✓	✓	✓	✓
RIP v1/v2		✓	✓	✓	✓
IS-IS		✓	✓	✓	✓
Traffic Prioritization		✓	✓	✓	✓
VPN				✓	✓
IPSec				✓	✓
Virtualization[a]	✓	✓	✓	✓	✓
Hardware Accelerated Layer 3 Switching		✓		✓	
Jumbo Frame Support		✓		✓	

[a] *Requires an additional feature key. For more information, refer to Chapter 17, Virtualization.*

For information about installing and viewing the contents of feature keys, refer to Section 4.10, "Managing Feature Keys".

Section 1.3

Security Recommendations

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

Authentication

CAUTION!
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 all user accounts, access modes (e.g. maintenance mode) and processes (where applicable) 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 Section 5.9, "Managing Passwords and Passphrases".

  This recommendation also applies to pre-shared keys (PSK) 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+ user authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.
- TACACS+ uses the MD5 algorithm for key encryption. Make sure to follow the security recommendations outlined in this User Guide and configure the environment according to *defense in depth* best practices.
- PAP (Password Authentication Protocol) is not considered a secure protocol and should only be enabled when required. Consider using CHAP (Challenge-Handshake Authentication Protocol) whenever possible.
- Use IPsec in conjunction with the L2TP protocol for increased security.
- It is recommended to use routing keys for authentication between routing neighbors to prevent unauthenticated routing updates.

Physical/Remote Access

- It is highly recommended to keep Brute Force Attack (BFA) protection enabled to prevent a third-party from obtaining unauthorized access to the device. For more information, refer to Section 6.3, "Enabling/Disabling Brute Force Attack Protection".
- SSH and SSL keys are accessible to users who connect to the device via the serial console. 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 person with malicious intent in possession of the flash card could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the card.
- Passwords/passphrases for service mode and maintenance mode should only be given to a limited number of trusted users. These modes provide access to private keys and certificates.

  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 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 Section 15.1.1, "Configuring Port Mirroring". For more information about enabling ingress filtering, refer to Section 8.5.3, "Enabling/Disabling Ingress Filtering".
- When using SNMP (Simple Network Management Protocol):
  - Limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures. For more information, refer to Section 14.2, "Managing SNMP".
  - Make sure the default community strings are changed to unique values.
- 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. For more information, refer to Section 6.8, "Managing Firewalls".
- Modbus is deactivated by default in RUGGEDCOM ROX II. If Modbus is required, make sure to follow the security recommendations outlined in this CLI User Guide and configure the environment according to defense-in-depth best practices.
- Configure secure remote system logging to forward all logs to a central location. For more information, refer to Section 4.12, "Managing Logs".
- 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, encrypt the files, store them in a secure place, and do not transfer them via insecure communication channels.
- It is highly recommended that critical applications be limited to private networks, or at least be accessible only through secure services, such as IPsec. 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 Section 6.8, "Managing Firewalls" and Section 11.8, "Managing IPsec Tunnels".
- The safekeeping and management of the certificates and keys is the responsibility of the device owner. Consider using RSA key sizes of 2048 bits in length for increased 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 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 Section 4.8, "Decommissioning the Device".
- Configure port security features on access ports to prevent an unauthorized third-party from physically connecting to the device. For more information, refer to Section 6.5.2, "Configuring Port Security".
- Be aware of insecure WLAN protocols, such as Open and WEP. Only use secure protocols when using WLAN, such as Wi-Fi Protected Access 2 (WPA2) and WPA-EAP (EAP-TLS).

» Virtualization

- The integrity of any operating system installed on a virtual machine must be verified by the user before use and all relevant security patches must be included. The operating system installed is the responsibility of the user and not that of Siemens Canada Ltd.
- Make sure any files included in a virtual machine image do not contain malicious content or code. Interfaces connecting the virtual machine to the Internet should be protected using security best practices.
- Use a VLAN or physical port – other than the RUGGEDCOM ROX II management port – to access a bridge interface on a virtual machine. The port used to access the virtual machine should be in a separate VLAN.

» Hardware/Software

CAUTION!
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 all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security website [https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Only enable the services that will be used on the device, including physical ports. 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 Transport Layer Security (TLS) versions and ciphers available are employed. Additionally, 1/n-1 record splitting is enabled in the latest Web browser versions of Mozilla Firefox, Google Chrome and Internet Explorer, 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 firmware often. 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 Section 4.16, “Monitoring Firmware Integrity”.

» 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.

Section 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 Open**
  The port state, whether it is always open and cannot be closed, or open only, but can be configured
- **Port Default**
  The default state of the port (i.e. open or closed)
- **Access Authorized**
  Denotes whether the ports/services are authenticated during access

Services	Port Number	Port Open	Port Default	Access Authorized
SSH	TCP/22	Open (if configured with login)	Open	Yes
SSH (Service Mode)	TCP/222	Open (if configured with login)	Closed	Yes
NETCONF	TCP/830	Open (if configured with login)	Open	Yes
SFTP	TCP/2222	Open (if configured with login)	Closed	Yes
HTTP	TCP/80	Open (if configured with login)	Open	N/A
NTP	UDP/123	Open (if configured)	Closed	No
SNMP	UDP/161	Open (if configured with login)	Closed	Yes
HTTPS	TCP/443	Open (if configured with login)	Open	Yes
TCP Modbus	TCP/502	Open (if configured)	Closed	No
IPSec IKE	UDP/500	Open (if configured)	Closed	Yes
IPSec NAT-T	UDP/4500	Open (if configured)	Closed	Yes
DNPv3	TCP/20000	Open (if configured)	Closed	No
RawSocket	TCP/configured	Open (if configured)	Closed	No
DHCP Agent	UDP/67	Open (if configured)	Closed	No
DHCP Server	UDP/67 listening, 68 responding	Open (if configured)	Closed	No
RADIUS	UDP/1812 to send, opens random port to listen	Open (if configured)	Closed	Yes
TACACS+	TCP/49 to send, opens random port to listen	Open (if configured)	Closed	Yes
L2TP	Random Port	Open (if configured)	Closed	Yes
BGP	TCP/179	Open (if configured)	Closed	No
RIP	UDP/520	Open (if configured)	Closed	No
MPLS-Ping	UDP/3503	Open (if configured)	Closed	No
LDP	TCP/646 and UDP/646	Open (if configured)	Closed	No
L2TPv3	UDP/1701	Open (if configured)	Closed	No

Section 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			Notes
	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	Administrator and operator can see status of active-alarms, acknowledge and clear alarms
/admin/alarms-config/	R/U	R/U	No	Administrator and operator cannot create or delete alarm-lists
/admin/users	C/R/U	No	No	
/admin/users/userid	R/U	R/U	No	Operator can only change own password and cannot create users.
/admin/cli	R/U	R/U	No	
/admin/snmp	C/R/U	No	No	
/admin/netconf	R/U	No	No	
/admin/dns	C/R/U	No	No	
/admin/webui	R/U	R/U	No	
/admin/scheduler	C/R/U	No	No	
/admin/contact	R/U	No	No	
/admin/hostname	R/U	No	No	
/admin/location	R/U	No	No	
/admin/session-limits	R/U	No	No	
/admin/session-security	R/U	No	No	
/admin/sftp	R/U	No	No	
/admin/time (status)	R	R	No	
/admin/switch-config (status)	R/U	R	No	
/admin/system	R/U	No	No	
/admin/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	

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
/admin/delete-all-ssh-known-hosts (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/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	
/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	

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
/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	No	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	

Section 1.6

Removable Memory

The RUGGEDCOM RX1400 features a user-accessible memory slot that supports a microSD or microSDHC Flash drive. 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 microSD or microSDHC Flash 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 microSD or microSDHC Flash drive, such as rollbacks, log files, feature keys and configuration files.
- Share Files – Quickly configure or upgrade other RUGGEDCOM RX1400 devices by copying files using the same microSD/microSDHC Flash drive.

IMPORTANT!
Do not remove the microSD or microSDHC Flash drive during a file transfer.

NOTE
Only one partition is supported on the microSD/microSDHC Flash drive.

Only the following file systems are supported on the microSD/microSDHC Flash drive: VFAT (recommended), ext2, ext3, ext4, FAT16 or FAT32. The advantage of using these file system types for the removable memory is that their contents can be modified on any general purpose computer that has a microSD/microSDHC interface.

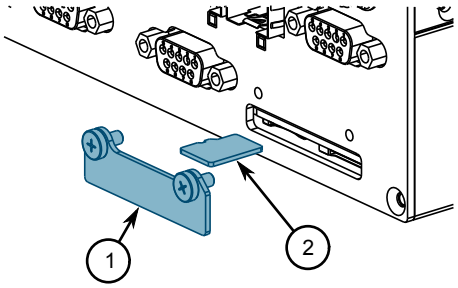


Figure 1: Memory Card Installation

1. Access Panel **2.** microSD/microSDHC Flash drive

For information about how to insert or remove the microSD/microSDHC Flash drive, refer to the *Installation Guide* for the RUGGEDCOM RX1400.

Section 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 Section 4.12.3, "Configuring Secure Remote Syslog".

CONTENTS

- Section 1.7.1, "Structure of a Syslog Event"
- Section 1.7.2, "Syslog Event Types"
- Section 1.7.3, "Logged Security Events"

Section 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[b]	The source of the event. Options include: • AUTH • AUTHPRIV • DAEMON • USER
Severity[b]	The severity level associated with the event. Options include: • INFO • NOTICE • AUTH • AUTHPRIV • ERR • CRITICAL • EMERGENCY
Message Text	Information about the event.

[b] *Text defined in the SNMP Manager.*

Section 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.

Section 1.7.3
Logged Security Events

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

Category	Event Message	Facility	Severity	Event Type	Log
SE_LOCAL_SUCCESSFUL_LOGON	ruggedcom confd[{pid}]: audit user: {user}/{user id} assigned to groups: {role}	LOG_AUTHPRIV	Info	Event	Auth.log
	ruggedcom rmfmgr[{pid}]:	LOG_AUTH	Notice	Event	Auth.log

Category	Event Message	Facility	Severity	Event Type	Log
	username:{user name} usid:{user id} started {context} session from ip:127.0.0.1 source-port:{src port} through {local interface} protocol				
SE_LOCAL_UNSUCCESSFUL_LOGON (Invalid Username)	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)	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	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)	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

Category	Event Message	Facility	Severity	Event Type	Log
SE_NETWORK_UNSUCCESSFUL_LOGON (Invalid Password)	audit user: {username}/0 Provided bad password	LOG_AUTHPRIV	Info	Event	Auth.log
	login failed, reason='Bad password', user='{username}', context='{session-type}', proto='{protocol}', user ipaddr='{source ip-address}'	LOG_AUTHPRIV	Error	Event	Auth.log
	audit user: {username}/0 Failed to login over {protocol}: Bad password	LOG_AUTHPRIV	Info	Event	Auth.log
SE_LOGOFF (Local)	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)	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	Enabling Brute Force Attack Protection	LOG_USER	Error	Event	Syslog
SE_ACCESS_PWD_DISABLED	Brute Force Attack protection not enabled	LOG_USER	Error	Alarm	Syslog
SE_ACCESS_PWD_CHANGED	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	audit user: {Username}/0 logged in through Web UI from {IP Address}	LOG_DAEMON	Info	Event	Auth.log
	audit user: {Username}/{User ID} assigned to groups: {User Group}	LOG_DAEMON	Info	Event	Auth.log
	username:{Username} usid:{User ID} started {Context} session from ip:{IP Address} source-port:{Port} through {Protocol} protocol	LOG_AUTH	Notice	Event	Auth.log
SE_ACCESS_DENIED	audit user: {Username}/0 Provided Invalid Password	LOG_DAEMON	Info	Alarm	Auth.log
	login failed, user:'{username}', reason='{reason}', user	LOG_AUTHPRIV	Error	Alarm	Auth.log

Category	Event Message	Facility	Severity	Event Type	Log
	ipaddr='{IP Address}', context='{context}', proto='{protocol}'				
SE_ACCOUNT_LOCKED_TEMP	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)	{Function}: deassert BFA alarm ip={IP address}	LOG_DAEMON	Verbose	Event	Syslog
SE_AUDIT_LOG_CLEARED	Deleted logs by restore-factory-defaults issued by user {Username}	LOG_DAEMON	Emergency	Alarm	Syslog
SE_COMMUNICATION_DATA_INTEGRITY_ERROR	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	username:{Username} usid:{User ID} stopped {Context} session from ip:{IP Address}	LOG_AUTH	Notice	Event	Auth.log
SE_SESSION_CLOSED (console)	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	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)	A failure was encountered in the upgrade process.	LOG_DAEMON	Notice	Event	Upgrade
SE_PATCH_DEPLOYMENT_FAILED (During uninstall - ROXFLASH)	A failure was encountered in the uninstallation process.	LOG_DAEMON	Notice	Event	Upgrade
SE_PATCH_DEPLOYMENT_FAILED (Can not connect to upgrade server - ROXFLASH)	Failed to get upgrade details from server, please verify connection.	LOG_DAEMON	Notice	Event	Upgrade
SE_PATCH_DEPLOYMENT_FAILED (No differences - ROXFLASH)	No differences detected in target version. Nothing to upgrade	LOG_DAEMON	Notice	Event	Upgrade

Category	Event Message	Facility	Severity	Event Type	Log
SE_PATCH_DEPLOYMENT_FAILED (Failed to configure boot partition - ROXFLASH)	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)	Failed upgrading target partition	LOG_DAEMON	Notice	Event	Upgrade
SE_PATCH_DEPLOYMENT_FAILED (General) - upgrade	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 interface.

CONTENTS

- Section 2.1, "Default User Names and Passwords"
- Section 2.2, "Logging In"
- Section 2.3, "Logging Out"
- Section 2.4, "Using Network Utilities"
- Section 2.5, "Using the Command Line Interface"
- Section 2.6, "Configuring the CLI Interface"
- Section 2.7, "Accessing Different Modes"

Section 2.1

Default User Names and Passwords

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

CAUTION!
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 Section 5.9, "Managing Passwords and Passphrases".

IMPORTANT!
Default passwords listed for Administrator and Operator access modes do not apply to WLAN-capable devices certified for use in the United States of America. In compliance with FCC regulations, the default passwords for these devices can only be obtained directly from Siemens. After initial use and before commissioning the device, these passwords can and should be changed to prevent unauthorized access.

For more information about obtaining the default passwords for a WLAN-capable device, contact Siemens Customer Support.

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

Mode	Username	Password
Guest	guest	guest

Section 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 Section 3.1, "Connecting to RUGGEDCOM ROX II".
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 Section 5.8.2, "Adding a User".
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 Section 2.1, "Default User Names and Passwords".

   IMPORTANT!
   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 Section 6.3, "Enabling/Disabling Brute Force Attack Protection".

   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#
```

Section 2.3
Logging Out

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

```
ruggedcom#  exit
```

Section 2.4
Using Network Utilities

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

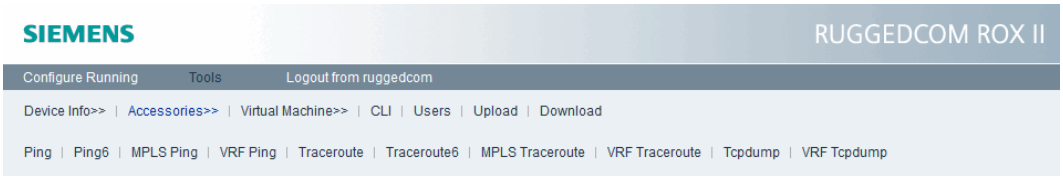


Figure 2: Accessories Menu

CONTENTS

- Section 2.4.1, “Pinging an IPv4 Address or Host”
- Section 2.4.2, “Pinging an IPv6 Address or Host”
- Section 2.4.3, “Pinging MPLS Endpoints”
- Section 2.4.4, “Pinging VRF Endpoints”
- Section 2.4.5, “Tracing a Route to an IPv4 Host”
- Section 2.4.6, “Tracing a Route to an IPv6 Host”
- Section 2.4.7, “Tracing a Route to an MPLS Endpoint”
- Section 2.4.8, “Tracing a Route to a VRF Endpoint”
- Section 2.4.9, “Capturing Packets from a Network Interface”
- Section 2.4.10, “Capturing Packets from a VRF Network Interface”

Section 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.

Section 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

Section 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

Section 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

Section 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  * * *
 .
 .
 .
```

Section 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  * * *
 .
 .
 .
```

Section 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

Section 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

Section 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
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.
linkheader	Displays the link level header.
port	The ports to trace.
proto { tCP | uDP | iCMP | aRP | vRRP | IqMP | oSPF | eSP | Ah }	The protocol(s) to filter out. To select more than one protocol, string the lowercase letters together. For example, tui will filter out TCP, UDP and ICMP packets. To ignore a protocol, place an n before the protocol name (e.g. ntui).
verbosity	The verbosity level. Type v, vv or vvv to set the level.

Section 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.
linkheader	Displays the link level header.
port	The ports to trace.
proto { tCP | uDP | iCMP | aRP | vRRP | IqMP | oSPF | eSP | Ah }	The protocol(s) to filter out. To select more than one protocol, string the lowercase letters together. For example, tui will filter out TCP, UDP and ICMP packets.

Parameter	Description
	To ignore a protocol, place an n before the protocol name (e.g. ntui).
`verbosity`	The verbosity level. Type v, vv or vvv to set the level.

Section 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.

CONTENTS

- Section 2.5.1, "Accessing Different CLI Modes"
- Section 2.5.2, "Using Command Line Completion"
- Section 2.5.3, "Displaying Available Commands"
- Section 2.5.4, "Editing Commands"
- Section 2.5.5, "Using Double Quotes"
- Section 2.5.6, "Using Output Redirects"
- Section 2.5.7, "Using Regular Expressions"
- Section 2.5.8, "Using CLI Utilities"
- Section 2.5.9, "Specifying a Range"
- Section 2.5.10, "Common Commands"

Section 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. 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 » serial » serport » 1***, the CLI prompt will be:

```
ruggedcom(config-serial-serport/1)#
```

Section 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.

Section 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#
```

Section 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

Section 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"
```

Section 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
```

Parameter	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    "Thu Oct  2 19:35:17 2014"`
	`  localtime "Thu Oct  2 15:35:17 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`
	` software-upgrade`
	`  upgrade-progress`
	`   software partition   "Partition #1"`
	`   current version      "ROX 2.7.0-QA3.1 (2014-10-21 14:59)"`
	`   upgrade state        Inactive`
	`   status message       ""`
	`   filesystem copy      0`
	`   package download     0`
	`   package installation 0`
	`   last upgrade attempt "Thu Oct  2 09:57:46 EDT 2014"`
	`   last upgrade result  "Upgrade Successful"`

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 Section 2.5.7, “Using Regular Expressions”.

Parameter	Description

	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`
	`----------------------------------------------------------`
	`swport    SM M88E6097F, 4FT 2GP    -       -`
	`serport   2xRS232/422/485          -       -`
	`celport   1x Cell LTE NAM A/R/B/T  -       -`
	`wlanport  1x WLAN 802.11           -       -`

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,DESCRIPTION,DATE TIME,USER`
	` ACTIONS,ACTUATORS`
	`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-module`
	`                                  BYPASS  OVERCURRENT`
	`SLOT      DETECTED MODULE          STATUS  STATUS`
	`----------------------------------------------------------`
	`swport    SM M88E6097F, 4FT 2GP    -       -`
	`serport   2xRS232/422/485          -       -`
	`celport   1x Cell LTE NAM A/R/B/T  -       -`
	`wlanport  1x WLAN 802.11           -       -`
	`show chassis line-modules line-module | de-select bypass`
	`SLOT      DETECTED MODULE`
	`---------------------------------`
	`swport    SM M88E6097F, 4FT 2GP`
	`serport   2xRS232/422/485`
	`celport   1x Cell LTE NAM A/R/B/T`
	`wlanport  1x WLAN 802.11`

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://ruggedcom.com/ns/rmf_admin">`
	`  <alarms>`
	`  <active-alarms>`

Parameter	Description
	<subsystem>switch</subsystem> <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 Section 2.5.7, "Using Regular Expressions".
	For example, show admin | exclude netconf shows the *admin* information, excluding the `netconf` lines.
	`ruggedcom# show admin | exclude netconf`
	`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`
	` notifications 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 Section 2.5.7, "Using Regular Expressions".
	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"`
	`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`

Parameter	Description

	<pre> 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</pre>

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:
	<pre>ruggedcom# show chassis | begin line-modules
	 line-modules
	  line-module
	                                BYPASS OVERCURRENT
	SLOT DETECTED MODULE STATUS STATUS
	--- 	
	swport SM M88E6097F, 4FT 2GP - -
	eth none - -
	serport 2xRS232/422/485 - -
	celport 1x Cell LTE EU - -</pre>
	For example, show chassis | begin line-modules | notab suppresses the table formatting:
	<pre>ruggedcom# show chassis | begin line-modules | notab
	 line-modules
	  line-module swport
	   detected module "SM M88E6097F, 4FT 2GP"
	  line-module eth
	   detected module none
	  line-module serport
	   detected module 2xRS232/422/485
	  line-module celport
	   detected module "1x Cell LTE EU"</pre>

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. For example, show chassis line-modules line-module | select detected-module displays the DETECTED MODULE column.

Parameter	Description
	``` 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 Section 2.5.7, "Using Regular Expressions". For example, show chassis | begin line-modules | until status returns the **chassis** information beginning with `line-modules` and ending with `status`: ``` ruggedcom# show chassis | begin line-modules | until status line-modules line-module BYPASS OVERCURRENT SLOT DETECTED MODULE STATUS STATUS --- swport SM M88E6097F, 4FT 2GP - - eth none - - serport 2xRS232/422/485 - - celport 1x Cell LTE EU - - ```

Section 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 Section 2.5.6, "Using Output Redirects".

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*

Character	Description	Example
+	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
```

Section 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.

Parameter	Description
ssh host *address/name* { bind-address *address* | cipher-spec *cipher* | list-ciphers | login *name* | port *number* | sub-system *name* }	Opens a secure shell on another host. Parameters include: • `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 ciphers to support for encrypting the session. To see the list of supported ciphers, use the `list-ciphers` option. • `list-ciphers` is the list of ciphers supported for SSH session encryption (e.g. aes256-ctr). • `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.
telnet host *address/name*	Opens a telnet session to another host. Parameters include:

Parameter	Description
	• *host* is the name or IP address of the host

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

Section 2.5.9
Specifying a Range

Some CLI commands accept a range of values, such as 3-6, to specify multiple targets. In the following example, a command is applied to ports 1, 2 and 3 on the swport slot:

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

In this example, a command is issued to ports 1, 2 and 4 on the swport slot:

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

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

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

Section 2.5.10
Common Commands

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

CONTENTS

- Section 2.5.10.1, “Basic CLI Commands”
- Section 2.5.10.2, “File Commands”
- Section 2.5.10.3, “Interface and Services Commands”
- Section 2.5.10.4, “Administration Commands”
- Section 2.5.10.5, “Configuration Mode General Commands”

Section 2.5.10.1
Basic CLI Commands

Use the following commands to perform basic CLI functions.

Parameter	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. • `no-confirm` exits from configuration mode without prompting the user to commit any pending changes.

Parameter	Description
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. The message appears in both the CLI and web interface. 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                              SERIAL`
	`SLOT     FIELD     DETECTED MODULE        NUMBER`
	`-------------------------------------------------`
	`swport   SM0001    SM M88E6097F, 4FT 2GP`
	`serport  SER0001   2xRS232/422/485`
	`celport  CELL0001  Cellular Modem`

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`
	` 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`
	• `history` displays the CLI command history.
	• `jobs` displays currently running background jobs. For example:
	`ruggedcom# show jobs`
	` JOB COMMAND`
	` 2  monitor start /tmp/saved`
	• `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.

Parameter	Description
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.

Section 2.5.10.2
File Commands

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

Parameter	Description
file	Performs file operations, including: • **compare-config** • **copy-config** • **delete-config** • **delete-featurekey** • **list-config** • **list-featurekey** • **rename-config** • **rename-featurekey** • **scp-config-from-url** • **scp-config-to-url** • **scp-featurekey-from-url** • **scp-featurekey-to-url** • **scp-log-to-url** • **show-config** • **show-featurekey**

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 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 deleted_users`

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`

Parameter	Description
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 scp-config-from-url *user@host:/path/current-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/current-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:/ruggedcom/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 *current-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.
	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-log-to-url *current-filename 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.

Parameter	Description

scp-log-to-url	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 syslog.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" location Location contact Contact`
	`admin hostname name ruggedcom domain localdomain`
	`admin session-limits max-sessions 50`
	`.`
	`.`
	`.`

Section 2.5.10.3

Interface and Services Commands

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

Parameter	Description
interfaces cellmodem cel-1 lte [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 switch swport *port* clearportstats	Clears statistics for the selected port.
services dhcpserver show-active-leases	Displays active DHCP leases.

Section 2.5.10.4
Administration Commands

Operational mode provides commands for performing device administration tasks.

Parameter	Description
admin acknowledge-all-alarms	Acknowledges all system alarms.
admin clear-all-alarms	Clears all system alarms.
admin delete-all-ssh-known-hosts	Deletes the list of known hosts.
admin delete-ssh-known-hosts	Deletes the host entry from the list of known hosts.
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 restore-factory-defaults	Restores the factory default configuration and settings, but does not erase any files you have saved on the device.
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 Section 4.5, "Shutting Down the Device"
admin software-upgrade decline-upgrade	Cancels (or declines) a recent software upgrade that is waiting for a reboot to the upgraded partition.
admin software-upgrade launch-upgrade	Launches an upgrade in the alternate partition.
admin software-upgrade 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	**CAUTION!** *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.

Parameter	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 Section 2.5.6, "Using Output Redirects". 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 Section 2.5.6, "Using Output Redirects".
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 Section 2.5.10.5, "Configuration Mode General Commands". **IMPORTANT!** *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 blocked from making changes until the session timeout period expires.*

Section 2.5.10.5

Configuration Mode General Commands

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

Parameter	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.

Parameter	Description
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 confirmed 2` To cancel a commit before the time elapses and discard the changes, type: **commit** abort 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.

Parameter	Description
help command	Displays help information for the specified command.
load [merge | override] *filename*	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`
	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 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 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-address-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:

Parameter	Description
	`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 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 configuration`
	` 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 configuration`
	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-configuration-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. 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.

Parameter	Description
wizard [rox_flash | rox_upgrade]	Runs the rox_flash or rox_upgrade wizards. For more information, refer to Section 4.15.5.2, "Downgrading Using ROXflash" and Section 4.15.3, "Upgrading the RUGGEDCOM ROX II Software".

Section 2.6

Configuring the CLI Interface

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

Parameter	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 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.

Section 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.

CONTENTS

- Section 2.7.1, “Managing Maintenance Mode Authorization”
- Section 2.7.2, “Accessing Maintenance Mode”
- Section 2.7.3, “Accessing BIST Mode”
- Section 2.7.4, “Accessing Service Mode”

Section 2.7.1

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.

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

CONTENTS

- Section 2.7.1.1, “Temporarily Enabling Maintenance Mode Authorization”
- Section 2.7.1.2, “Permanently Enabling Maintenance Mode Authorization”
- Section 2.7.1.3, “Disabling Maintenance Mode Authorization”

Section 2.7.1.1

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, refer to Section 4.1, "Displaying Device and Software Information".

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 Section 4.1, "Displaying Device and Software Information".

4. [Optional] Access maintenance mode with the maintenence mode password. For more information, refer to refer to Section 2.7.2, "Accessing Maintenance Mode".

Section 2.7.1.2
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 Section 4.15, "Upgrading/Downgrading the RUGGEDCOM ROX II Software".

For more information restoring the factory default settings for the device, refer to Section 4.7, "Restoring Factory Defaults".

CAUTION!
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 Section 2.7.1.1, "Temporarily Enabling Maintenance Mode Authorization".

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.

Section 2.7.1.3
Disabling Maintenance Mode Authorization

To disable maintenance mode authorization, do the following:

- Type the following:

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

Maintenance mode is disabled.

Section 2.7.2
Accessing Maintenance Mode

Maintenance mode grants access to the Linux shell.

To access maintenance mode, do the following:

CAUTION!
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.

IMPORTANT!
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 Section 2.7.1.1, "Temporarily Enabling Maintenance Mode Authorization".

IMPORTANT!
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.

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To avoid unintended admin users from accessing maintenence mode, make sure the default maintenance mode password has been replaced with a strong password. For information about creating strong passwords, refer to Section 5.9, "Managing Passwords and Passphrases".

1. If the default password has been changed previously, proceed to step Step 2. Otherwise, change the default maintenance mode password to a strong password. For information about setting the maintenance mode password, refer to Section 5.9.4, "Setting the Maintenance Password/Passphrase".
2. Enable maintenance mode authorization. For more information, refer to Section 2.7.1.1, "Temporarily Enabling Maintenance Mode Authorization".
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 2.4.0 (2013-01-24 18:20)) RX1511 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:~#
```

Section 2.7.3

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.

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. Access to BIST mode should be restricted to admin users only.

CAUTION!
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 222.

To access BIST mode normally, do the following:

IMPORTANT!
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 RX1400 through the RS-232 console connection and a terminal application. For more information, refer to Section 3.1.2, "Connecting Directly".
3. Reboot the device. For more information, refer to Section 4.6, "Rebooting the Device".
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 RX1400 through the RS-232 console connection and a terminal application. For more information, refer to Section 3.1.2, "Connecting Directly".
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
```

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. Upon accessing BIST mode on a device that is connected to a network, make sure SSH is disabled. Failure to disable SSH once in BIST mode would allow anyone with remote access to the device and the root password to access the Linux shell.

NOTE
SSH is enabled automatically once the device is rebooted in normal mode. It can also be enabled manually by typing:

```
/etc/init.d/ssh start
```

3. Once the device is rebooted, disable SSH immediately by typing:

```
/etc/init.d/ssh stop
```

4. Connect the device to the network.

Section 2.7.4

Accessing Service Mode

Service mode grants access to the Linux shell.

To access service mode, do the following:

CAUTION!
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.

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. SSH is automatically enabled on port 222 when the device is put in service mode. 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*
- *Disabling SSH via maintenance mode before accessing service mode*

IMPORTANT!
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 Section 3.1.2, "Connecting Directly".
2. Reboot the device. For more information, refer to Section 4.6, "Rebooting the Device".
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 Section 2.1, "Default User Names and Passwords".

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:~#
```

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. Upon accessing service mode on a device that is connected to a network, make sure SSH is disabled. Failure to disable SSH once in service mode would allow anyone with remote access to the device and the root password to access the Linux shell.

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.

CONTENTS

- Section 3.1, "Connecting to RUGGEDCOM ROX II"
- Section 3.2, "Configuring a Basic Network"

Section 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.

CONTENTS

- Section 3.1.1, "Default IP Address"
- Section 3.1.2, "Connecting Directly"
- Section 3.1.3, "Connecting Remotely"

Section 3.1.1

Default IP Address

The default IP address for the device is 192.168.0.2/24.

Section 3.1.2

Connecting Directly

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.

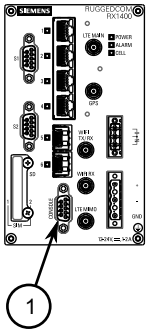


Figure 3: RS-232 Console Port

1. RS-232 Console Port

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 Section 2.2, "Logging In".

Section 3.1.3

Connecting Remotely

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.
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 Section 2.2, "Logging In".

Section 3.2
Configuring a Basic Network

RUGGEDCOM ROX II has the following Internet interfaces configured by default: *dummy0* and *switch.0001*. The default IP addresses for *switch.0001* is configured under the ***ip » switch.0001 » ipv4***. 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

CONTENTS

- Section 3.2.1, "Configuring a Basic IPv4 Network"
- Section 3.2.2, "Configuring a Basic IPv6 Network"

Section 3.2.1
Configuring a Basic IPv4 Network

To configure a basic IPv4 network, do the following:

1. Select two switched Ethernet ports and assign them each a unique VLAN. For more information about assigning VLANs to switched Ethernet ports, refer to Section 8.1.2, "Configuring a Switched Ethernet Port".

   For the purposes of this procedure, the ports will be referred to as VLAN 1 and VLAN 2, respectively.
2. Configure an IPv4 address for the VLAN interface representing each port, making sure the VLAN 2 interface is in a different subnet. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".
3. Connect a computer to the VLAN 1 port.
4. Configure the computer to be on the same subnet as the VLAN 1 interface.
5. Configure the default gateway for the computer to be the same as the VLAN 1 interface's IPv4 address.
6. Connect a switch from an IPv4 capable network to the VLAN 2 port.
7. Configure all computers on the IPv4 network to be on the same subnet as the VLAN 2 interface.
8. Configure the default gateway for all computers on the IPv4 network to be the same as the VLAN 2 interface's IPv4 address.
9. Enable the Brute Force Attack (BFA) protection system on the device. For more information, refer to Section 6.3, "Enabling/Disabling Brute Force Attack Protection".
10. Make sure all computers connected to the device can ping one another.

Section 3.2.2
Configuring a Basic IPv6 Network

To configure a basic IPv6 network, do the following:

1. Select two switched Ethernet ports and assign them each a unique VLAN. For more information about assigning VLANs to switched Ethernet ports, refer to Section 8.1.2, "Configuring a Switched Ethernet Port".

   For the purposes of this procedure, the ports will be referred to as VLAN 1 and VLAN 2, respectively.
2. Configure an IPv6 address for the VLAN interface representing each port, making sure the VLAN 2 interface is in a different subnet. For more information, refer to Section 7.1.4.2, "Adding an IPv6 Address".
3. Connect a computer to the VLAN 1 port.
4. Configure the computer to be on the same subnet as the VLAN 1 interface.
5. Configure the default gateway for the computer to be the same as the VLAN 1 interface's IPv6 address.
6. Connect a switch from an IPv6 capable network to the VLAN 2 port.
7. Configure all computers on the IPv6 network to be on the same subnet as the VLAN 2 interface.
8. Configure the default gateway for all computers on the IPv6 network to be the same as the VLAN 2 interface's IPv6 address.
9. Enable the Brute Force Attack (BFA) protection system on the device. For more information, refer to Section 6.3, "Enabling/Disabling Brute Force Attack Protection".
10. Enable IPv6 Neighbor Discovery. For more information, refer to Section 7.1.5, "Configuring IPv6 Neighbor Discovery".
11. 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.

CONTENTS

- Section 4.1, "Displaying Device and Software Information"
- Section 4.2, "Determining the GPS Location of the Device"
- Section 4.3, "Viewing Chassis Information and Status"
- Section 4.4, "Viewing the Parts List"
- Section 4.5, "Shutting Down the Device"
- Section 4.6, "Rebooting the Device"
- Section 4.7, "Restoring Factory Defaults"
- Section 4.8, "Decommissioning the Device"
- Section 4.9, "Viewing a List of Line Module Configurations"
- Section 4.10, "Managing Feature Keys"
- Section 4.11, "Managing Files"
- Section 4.12, "Managing Logs"
- Section 4.13, "Managing the Software Configuration"
- Section 4.14, "Managing Automatic Configuration Loading"
- Section 4.15, "Upgrading/Downgrading the RUGGEDCOM ROX II Software"
- Section 4.16, "Monitoring Firmware Integrity"
- Section 4.17, "Managing SFP Transceivers"

Section 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                      RX1400
 software license           "Layer 3 Security Edition"
```

```
mlfb                        6GK60140AM2
rox release                 "ROX 2.13.0-QA2.3 (2019-01-01 08:00)"
system serial number        RUMED22080399
last integrity check        "2019-01-01 09:00"
last integrity check result Success
BootLoader                  2014.04RR31
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 1 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. This parameter is mandatory.
system-serial-number	**Synopsis:** A string 1 to 32 characters long The system serial number on the chassis label. This parameter is mandatory.
last-integrity-check	**Synopsis:** A string 1 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.
BootLoader	**Synopsis:** A string The version of the ROX bootloader software on the installed module. This parameter is mandatory.
maint-mode-status	**Synopsis:** A string The maintenance mode status (enabled or disabled).

Section 4.2

Determining the GPS Location of the Device

With GPS enabled, the physical location of the device can be determined via RUGGEDCOM ROX II.

To determine the GPS location of the device, type:

```
interfaces cellmodem port lte gps-location
```

Where:

- *port* is the port number for the module

The GPS location of the device is displayed. For example:

```
ruggedcom# interfaces cellmodem cel-1 lte gps-location
gps_location_reply
```

```
UTC time:  2015-03-18 19:25:20 UTC
Localtime: 2015-03-18 15:25:20 EDT
Latitude: 43 deg. 48.4717 min. N
Longitude: 079 deg. 32.4272 min. W
Number of satellites in view: 8
```

Section 4.3
Viewing Chassis Information and Status

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

CONTENTS

- Section 4.3.1, "Viewing the Slot Hardware"
- Section 4.3.2, "Viewing Flash Card Storage Utilization"
- Section 4.3.3, "Viewing CPU/RAM Utilization"
- Section 4.3.4, "Viewing the Slot Status"
- Section 4.3.5, "Viewing the Slot Sensor Status"

Section 4.3.1
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                              SERIAL
SLOT      FIELD     DETECTED MODULE          NUMBER
-------------------------------------------------
swport    SM0001    SM M88E6097F, 4FT 2GP
serport   SER0001   2xRS232/422/485
celport   CELL0001  1x Cell LTE EU
```

Section 4.3.2
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                "Flash"
  total capacity              994896
  current partition           "Partition #1"
  current partition capacity  490496
  secondary partition capacity 490496
  current partition usage     67
```

This table or list provides the following information:

Parameter	Description
storage-name	**Synopsis:** A string 0 to 32 characters long The type of storage.
total-capacity	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total capacity of the flash storage in KB. This parameter is mandatory.
current-partition	**Synopsis:** A string 0 to 32 characters long The partition ROX is currently running on and booted from. This parameter is mandatory.
current-partition-capacity	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The capacity of the current partition in KB. This parameter is mandatory.
secondary-partition-capacity	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The capacity of the secondary partition in KB. This parameter is mandatory.
current-partition-usage	**Synopsis:** A 32-bit signed integer between 0 and 100 The %usage of the current partition. This parameter is mandatory.

Section 4.3.3
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
                                          RAM
                                CPU   RAM   AVAIL
SLOT  DETECTED MODULE           LOAD  AVAIL LOW
-----------------------------------------------------

cm    CM TI-AM5726 variant 0001  4     122   121
```

This 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 1 to 60 characters long The installed module's type specifier. This parameter is mandatory.
cpu-load	**Synopsis:** A 32-bit signed integer between 0 and 100 The CPU load, in percent, on the installed module.
ram-avail	**Synopsis:** A 32-bit signed integer between 0 and 100 The proportion of memory (RAM) currently unused, in percent, on the installed module.
ram-avail-low	**Synopsis:** A 32-bit signed integer between 0 and 100 The lowest proportion of unused memory (RAM), in percent, recorded for the installed module since start-up.

Section 4.3.4
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
-------------------------------------------------------------------------------------------
cm    CM TI-AM5726 variant 0001  operating  Normal  0D 0hr 0min 0sec  2015-01-06Z  16:36:20Z
```

This 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 1 to 60 characters long The installed module's type specifier. This parameter is mandatory.
state	**Synopsis:** { unknown, empty, disabled, resetting, operating, failed, disconnected } The current state of the installed module. This parameter is mandatory.
status-string	**Synopsis:** A string The runtime status of the installed module. This parameter is mandatory.
uptime	**Synopsis:** A string The total time elapsed since the start-up of the installed module. This parameter is mandatory.
start-date	**Synopsis:** A string The date on which the installed module was started up.

Parameter	Description
	This parameter is mandatory.
start-time	**Synopsis:** A string The time at which the installed module was started up. This parameter is mandatory.

Section 4.3.5
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:

```
show chassis sensors
sensors
SLOT  DETECTED MODULE                                    TEMPERATURE  CURRENT  VOLTAGE
-------------------------------------------------------------------------------------
cm    CM TI-AM5726 variant 0001                          38
wlanport 1x WLAN 802.11 US
```

This 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 1 to 60 characters long The installed module's type specifier. This parameter is mandatory.
temperature	**Synopsis:** A 32-bit signed 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. This parameter is mandatory.

Section 4.4
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
-------------------------------------------------------------------------------
RX1400  CELL0001    CELL-LTE-0.001  1x Cell LTE EU

                    DB-CELL-LTE-1.
```

```
                    001
RX1400  CELL0002    CELL-LTE-0.001  1x Cell LTE NAM A/R/B/T

                    DB-CELL-LTE-1.
                    002
RX1400  CELL0003    CELL-LTE-0.001  1x Cell LTE NAM V/S

                    DB-CELL-LTE-1.
                    003
RX1400  CELL0004    CELL-LTE-0.001  1x Cell LTE APAC

                    DB-CELL-LTE-1.
                    004
RX1400  CELL0005    CELL-LTE-0.001  1x Cell LTE Japan

                    DB-CELL-LTE-1.
                    005
RX1400  CM0001      BACKPLANE.001   CM TI-AM5726 variant 0001
RX1400  CM0001      CM-AM5726-0.00  CM TI-AM5726 variant 0001
                    1
RX1400  PM0001      PM-24VDC.001    12-24VDC Unmonitored PM
RX1400  PM0002      PM-48VDC.001    48VDC Unmonitored PM
RX1400  PM0003      PM-HI.001       HI AC-DC Unmonitored PM
RX1400  SER0001     SER-TP-0.001    2xRS232/422/485
                    DB-SER-TP-2.00
                    1
RX1400  SM0001      SM-L2-0.001     SM M88E6097F, 4FT 2GP
                    DB-ETH-FT-4.00
                    1
                    DB-ETH-GP-2.00
                    1
.
.
.
```

Section 4.5

Shutting Down the Device

To shut down the device, type:

CAUTION!
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
```

Section 4.6
Rebooting the Device

To reboot the device, type:

```
admin reboot
```

Section 4.7
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	**Synopsis:** { true, false } **Default:** false Delete system logs as well as restoring default settings.
default-both-partitions	**Synopsis:** { true, false } **Default:** false Perform the operation on both partitions.
delete-saved-configurations	**Synopsis:** { true, false } **Default:** false Delete saved configuration files (works with default-both-partitions option).
shutdown	**Synopsis:** { true, false } **Default:** false Shutdown rather than reboot after restoring factory defaults.

Section 4.8
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.

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 Section 2.7.2, “Accessing Maintenance Mode”.
3. Delete the current boot password/passphrase by typing:

   ```
   rox-delete-bootpwd --force
   ```
4. Type **exit** and press **Enter**.
5. Log in to RUGGEDCOM ROX II. For more information, refer to Section 2.2, “Logging In”.

6. Flash the RUGGEDCOM ROX II firmware obtained in Step 1 to the inactive partition and reboot the device. For more information, refer to Section 4.15.5.2, "Downgrading Using ROXflash".
7. Repeat Step 5 and Step 6 to flash the RUGGEDCOM ROX II firmware obtained in Step 1 to the other partition and reboot the device.
8. Shut down the device. For more information, refer to Section 4.5, "Shutting Down the Device".

Section 4.9
Viewing a List of Line Module Configurations

To view a list of line module configurations, type:

NOTE
Line module configurations are not configurable.

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

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

```
show running-config chassis line-modules | tab
chassis
 line-modules
  line-module
                                    ADMIN    ADMIN
SLOT      MODULE TYPE               ENABLED  BYPASS
-------------------------------------------------------
swport    SM M88E6097F, 4FT 2GP     X        -
serport   2xRS232/422/485           X        -
celport   1x Cell LTE NAM A/R/B/T   X        -
wlanport  1x WLAN 802.11 US         X        -

 !
!
```

Section 4.10
Managing Feature Keys

RUGGEDCOM ROX II can be enhanced with additional features at any time by adding feature levels. Feature levels are encoded in feature keys that can be loaded on a device. At the time of ordering, a device feature key is encoded into the electronic signature of the device. Additional file-based feature keys can be added as needed.

NOTE
Some RUGGEDCOM ROX II features are only available through the purchase of feature levels. For more information about the available feature levels, refer to the product data sheet for the device available at https://www.siemens.com/ruggedcom or contact a Siemens Sales representative.

When ordering feature levels, 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 on how to determine the *main* serial number, refer to Section 4.1, "Displaying Device and Software Information".

CONTENTS

- Section 4.10.1, "Viewing the Contents of a Feature Key"
- Section 4.10.2, "Installing Feature Keys"

Section 4.10.1

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+G5kdYj1ACfecKysp3DK3QBsP87I/
   gXgi92cwAAnjqrsgdqwaCczY4ghWrR0ELkr2TK
   ```

Section 4.10.2

Installing Feature Keys

When installing a new feature key, RUGGEDCOM ROX II evaluates the new file-based feature key and the device feature key and enables the most capable feature level described by the keys.

Feature keys can be installed from a host computer or microSD/microSDHC drive.

» Installing From a Host Computer

NOTE

Before installing a feature key from a host computer, the following information is required:

- *The file name of the feature key*
- *The user name and password required to log into the host computer where the feature key is stored*
- *The host name or IP address of the computer where the feature key is stored*

1. Make sure the CLI is in Operational mode.
2. 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_cmRUMHD06096338.key
    L3SE_cmRUMHD06096338.key
   ```

3. 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 a MicroSD Card

1. Make sure the CLI is in Operational mode.
2. Insert the microSD/microSDHC drive into the microSD/microSDHC drive slot on the device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
3. Install the feature key by typing:

   ```
   file scp-featurekey-from-url usb:///path/current-filename new-filename
   ```

   Where:

   - *path* is the directory path to the feature key file on the USB Mass Storage drive.
   - *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 usb://repository/keys/L3SE_cmRUMHD06096338.key
    L3SE_cmRUMHD06096338.key
   ```

   The system uploads the feature key file:

   ```
    ruggedcom# file scp-featurekey-from-url usb://repository/keys/
   L3SE_cmRUMHD06096338.key L3SE_cmRUMHD06096338.key
   L3SE_cmRUMHD06096338.key               100%  192     0.2KB/s   00:00
   ```

Section 4.11
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 microSD/SDHC card or from a remote server using a file transfer protocol, such as FTP.
- **Backup**
  Allows users to download files to a microSD/SDHC card or to a remote server using a file transfer protocol, such as FTP.

CONTENTS

- Section 4.11.1, “Installing Files”
- Section 4.11.2, “Backing Up Files”

Section 4.11.1
Installing Files

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

IMPORTANT!
A microSD/microSDHC drive must be installed if the file type is a virtual machine image. Virtual machine images are saved to the microSD/microSDHC drive when installed.

1. If the source of the file is a microSD/microSDHC drive, insert the drive in the microSD/microSDHC port on the device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
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.

Parameter	Description
file-type { file-type }	**Synopsis:** { config, featurekey, vmfile } The file types to be copied. This parameter is mandatory.
url { url }	**Synopsis:** A string 1 to 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. This parameter is mandatory.

3. If the VPE feature key (VIRTUALM) was installed, reboot the device to reveal the virtualization features. For more information, refer to Section 4.6, "Rebooting the Device".

Section 4.11.2
Backing Up Files

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

1. If the file's destination is a microSD/microSDHC drive, insert the drive in the microSD/microSDHC port on the device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
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.

Parameter	Description
file-type { file-type }	**Synopsis:** { config, featurekey, logfiles, rollbacks, licenses, logarchive } The file types to copy. This parameter is mandatory.
file { file }	**Synopsis:** A string 1 to 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. This parameter is mandatory.
timestamp	**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 1 to 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. This parameter is mandatory.

Section 4.12
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 Section 4.12.1, "Viewing Logs".
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.

CONTENTS

• Section 4.12.1, "Viewing Logs"
• Section 4.12.2, "Deleting Logs"
• Section 4.12.3, "Configuring Secure Remote Syslog"
• Section 4.12.4, "Managing Diagnostic Logs"
• Section 4.12.5, "Managing Remote Syslog Servers"
• Section 4.12.6, "Managing Remote Server Selectors"

Section 4.12.1

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 Section 4.11.2, "Backing Up Files".

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)
.
.
.
```

Section 4.12.2
Deleting Logs

To delete all logs stored on the device, type:

```
admin delete-logs
```

Section 4.12.3
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).

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

CONTENTS

- Section 4.12.3.1, "Enabling/Disabling Secure Remote Syslog"
- Section 4.12.3.2, "Viewing a List of Permitted Peers"
- Section 4.12.3.3, "Adding a Permitted Peer"
- Section 4.12.3.4, "Deleting a Permitted Peer"
- Section 4.12.3.5, "Configuring a Source IP Address for Remote Syslog Messages"

Section 4.12.3.1
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
   ```

   IMPORTANT!
   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 Section 6.7.7.3, "Adding a Certificate".

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 Section 4.12.3.3, "Adding a Permitted Peer".

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 4.12.3.2
Viewing a List of Permitted Peers

To view a list of permitted peers, type:

```
show running-config admin logging secure-remote-syslog permitted-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 Section 4.12.3.3, "Adding a Permitted Peer".

Section 4.12.3.3
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 pattern
   ```

   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, or type **revert** and press **Enter** to abort.

Section 4.12.3.4
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, or type **revert** and press **Enter** to abort.

Section 4.12.3.5
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 Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".

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, or type **revert** and press **Enter** to abort.

Section 4.12.4

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

CAUTION!
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.

CONTENTS

- Section 4.12.4.1, “Enabling/Disabling the Developer's Log”
- Section 4.12.4.2, “Enabling/Disabling the SNMP Log”
- Section 4.12.4.3, “Enabling/Disabling the NETCONF Summary Log”
- Section 4.12.4.4, “Enabling/Disabling the NETCONF Trace Log”
- Section 4.12.4.5, “Enabling/Disabling the XPATH Trace Log”
- Section 4.12.4.6, “Enabling/Disabling the WebUI Trace Log”

Section 4.12.4.1

Enabling/Disabling the Developer's Log

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

CAUTION!
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, or type **`revert`** and press **Enter** to abort.

Section 4.12.4.2
Enabling/Disabling the SNMP Log

The SNMP log records all SNMP related events.

CAUTION!
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, or type **`revert`** and press **Enter** to abort.

Section 4.12.4.3
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"
.
.
.
```

CAUTION!
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, or type **`revert`** and press **Enter** to abort.

Section 4.12.4.4
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>
.
.
.
```

CAUTION!
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, or type **revert** and press **Enter** to abort.

Section 4.12.4.5
Enabling/Disabling the XPATH Trace Log

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

CAUTION!
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, or type **revert** and press **Enter** to abort.

Section 4.12.4.6
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.

CAUTION!
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, or type **`revert`** and press **Enter** to abort.

Section 4.12.5
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

CONTENTS

- Section 4.12.5.1, "Viewing a List of Remote Servers"
- Section 4.12.5.2, "Adding a Remote Server"
- Section 4.12.5.3, "Deleting a Remote Server"

Section 4.12.5.1
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 Section 4.12.5.2, "Adding a Remote Server".

Section 4.12.5.2
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:** A 16-bit unsigned integer between 1 and 65535 **Default:** 514 Port number.

4. Configure one or more selectors for the server. For more information, refer to Section 4.12.6.2, "Adding a Remote Server Selector".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 4.12.5.3
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, or type **revert** and press **Enter** to abort.

Section 4.12.6
Managing Remote Server Selectors

Remote server selectors filter the information sent to specific servers.

CONTENTS

- Section 4.12.6.1, "Viewing a List of Remote Server Selectors"
- Section 4.12.6.2, "Adding a Remote Server Selector"
- Section 4.12.6.3, "Deleting a Remote Server Selector"

Section 4.12.6.1
Viewing a List of Remote Server Selectors

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 Section 4.12.6.2, "Adding a Remote Server Selector".

Section 4.12.6.2
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. 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, or type **revert** and press **Enter** to abort.

Section 4.12.6.3
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.

Section 4.13
Managing the Software Configuration

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

CONTENTS

- Section 4.13.1, "Saving the Configuration"
- Section 4.13.2, "Loading a Configuration"

Section 4.13.1
Saving the Configuration

To save the configuration settings for RUGGEDCOM ROX II as a separate file, type:

```
admin full-configuration-save format cli file-name filename
```

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 microSD/microSDHC Flash card. For more information, refer to Section 4.11.2, "Backing Up Files".

Section 4.13.2
Loading a Configuration

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

IMPORTANT!
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 Section 4.11.1, "Installing Files".
2. Load the configuration file by typing:

   ```
   admin full-configuration-load format cli file-name filename
   ```

   Where:

- *filename* is the name of the configuration file

3. A confirmation message appears. Type **yes** to load the file or **no** to abort.

Section 4.14
Managing Automatic Configuration Loading

RUGGEDCOM ROX II supports automatic loading of a configuration file via a microSD card, following a reboot of the device.

Configurations can be saved from one device onto removeable memory, then loaded onto another device or devices as needed. Saved configurations can also be loaded onto new devices to replace factory default settings.

CONTENTS

- Section 4.14.1, "Enabling/Disabling Automatic Configuration Loading"
- Section 4.14.2, "Automatically Loading a Configuration File from a Removable Drive"
- Section 4.14.3, "Overriding Factory Settings Using a Removable Drive"

Section 4.14.1
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, or type **revert** and press **Enter** to abort.

Section 4.14.2
Automatically Loading a Configuration File from a Removable Drive

NOTE
For more information about supported file systems in RUGGEDCOM ROX II, refer to Section 1.6, "Removable Memory".

To automatically load a configuration file from a removable drive following a reboot, do the following:

1. If a VPE is being used, do the following on the source device:

NOTE
For detailed information about managing the Virtual Processing Engine (VPE), refer to Chapter 17, Virtualization.

a. Make sure the VPE feature key (VIRTUALM) is installed.

b. Enable the virtualization service. For more information, refer to Section 17.2, "Enabling/Disabling the Virtualization Service".

c. Enable the virtual machine to be auto started. For more information, refer to Section 17.3, "Configuring Global Settings".

2. Create a configuration file from the desired source device. Name the file *autoload-config.cli*. For more information, refer to Section 4.13.1, "Saving the Configuration".
3. Make sure the desired virtual machine image is installed on the microSD/microSDHC card. For more information, refer to Section 4.11.2, "Backing Up Files".
4. Copy the configuration file to the removable drive. For more information, refer to Section 4.11.2, "Backing Up Files".

IMPORTANT!
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.

5. On the target device, install the VPE feature key (VIRTUALM). For more information about obtaining this feature key, contact a Siemens Sales representative or Customer Support.
6. On the target device, enable the Automatic Configuration Load feature. For more information, refer to Section 4.14.1, "Enabling/Disabling Automatic Configuration Loading".
7. Insert the microSD/microSDHC drive into the microSD/microSDHC drive slot on the target device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
8. Reboot the target device. For more information about rebooting, refer to Section 4.6, "Rebooting the Device".

   The auto-loaded configuration file is loaded to the device. If the VPE service is configured to auto-start, the virtual machine starts.

Section 4.14.3

Overriding Factory Settings Using a Removable Drive

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

NOTE
For more information about supported file systems in RUGGEDCOM ROX II, refer to Section 1.6, "Removable Memory".

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

1. If a VPE is being used, do the following on the source device:

NOTE
For detailed information about managing the Virtual Processing Engine (VPE), refer to Chapter 17, Virtualization.

a. Make sure the VPE feature key (VIRTUALM) is installed.

b. Enable the virtualization service. For more information, refer to Section 17.2, "Enabling/Disabling the Virtualization Service".

c. Enable the virtual machine to be auto started. For more information, refer to Section 17.3, "Configuring Global Settings".

2. Create a configuration file from the desired source device. Name the file *autoload-config.cli*. For more information, refer to Section 4.13.1, "Saving the Configuration".
3. Copy the configuration file to the removable drive. For more information, refer to Section 4.11.2, "Backing Up Files".
4. Make sure the desired virtual machine image is installed on the microSD/microSDHC card. For more information, refer to Section 4.11.2, "Backing Up Files".
5. Insert the microSD/microSDHC drive into the microSD/microSDHC drive slot on the target device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
6. On the target device, install the VPE feature key (VIRTUALM). For more information about obtaining this feature key, contact a Siemens Sales representative or Customer Support.

   Start up and connect to the target device. For more information about connecting to the device, refer to Section 3.1, "Connecting to RUGGEDCOM ROX II".

   The auto-loaded configuration file is loaded to the device. If the VPE service is configured to auto-start, the virtual machine starts.

Section 4.15

Upgrading/Downgrading the RUGGEDCOM ROX II Software

This section describes how to change the version of RUGGEDCOM ROX II running on the device.

CONTENTS

- Section 4.15.1, "Configuring the Upgrade Source"
- Section 4.15.2, "Setting Up an Upgrade Server"
- Section 4.15.3, "Upgrading the RUGGEDCOM ROX II Software"
- Section 4.15.4, "Stopping/Declining a Software Upgrade"
- Section 4.15.5, "Downgrading the RUGGEDCOM ROX II Software"

Section 4.15.1

Configuring the Upgrade Source

Firmware for upgrading or downgrading RUGGEDCOM ROX II can be uploaded from either an upgrade server or a portable microSD/microSDHC drive. For information about setting up an upgrade server, refer to Section 4.15.2, "Setting Up an Upgrade Server".

IMPORTANT!
*A Trusted Root CA (Certified Authority) certificate is required if using HTTPS to upload packages from an upgrade server. The certificate is chosen using the **Server CA** parameter. If a certificate is not available, it must be uploaded to the device. For more information, refer to Section 6.7.4.3, "Adding a CA Certificate and CRL".*

To specify the source of the RUGGEDCOM ROX II software and a specific version, do the following:

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

Parameter	Description
repository-url { repository-url }	**Synopsis:** A string The URL for the upgrade server or file system. Supported URIs are HTTP, HTTPS, FTP, USB and SD. To upgrade from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-repository" or "sd://device-name/path-to-repository". To determine the device name, insert your device and in the web ui, go to "chassis", "storage", "removable", OR, in the cli, type "show chassis". Note that only one single partition is supported for either data medium. For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".
target-version { target-version }	**Synopsis:** A string The target software version. Specify a specific software release in the form of 'rrX.Y.Z' or enter 'current' to upgrade to the latest software release available on the upgrade server.

3. Add the server's SSH/RSA public key to RUGGEDCOM ROX II and add the server to the Known Hosts list. For more information, refer to Section 6.7.8.2, "Adding a Known Host".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 4.15.2
Setting Up an Upgrade Server

An upgrade server containing a software repository can be used to upgrade or downgrade the RUGGEDCOM ROX II software via the network.

The upgrade server must meet the following requirements:

- Each device that will be upgraded/downgraded must have access to a host that acts as a Web server or FTP server.
- The server must have sufficient disk space for at least two full software releases. Each full software release is approximately 75 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 or FTP 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 along 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
Each device should be configured 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 the devices to upgrade at the same time.

CONTENTS

- Section 4.15.2.1, "Configuring the Upgrade Server"
- Section 4.15.2.2, "Adding Software Releases to the Upgrade Server"
- Section 4.15.2.3, "Adding Firmware Releases to the Upgrade Server"

Section 4.15.2.1
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:

  NOTE
  ***2.x.y** represents the RUGGEDCOM ROX II version, where **x** is the major release number and **y** is the minor release number. For example, **2.13.1**.*

File Type	File Name	MIME Type
RUGGEDCOM ROX II Image Archive	imagerr2.x.y-armhf.tar.bz2	application/x-bzip2
RUGGEDCOM ROX II Upgrade Archive	rr2/dists/rr2.x.y/Release (extracted from rr2.x.y.zip)	text/plain
GNU Privacy Guard (GPG)	imagerr2.x.y-armhf.tar.bz2.gpg	text/plain

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

- **Enable Double-Escaping**
  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.

Section 4.15.2.2
Adding Software Releases to the Upgrade Server

Software releases, including updates, can be obtained by submitting a Support Request via the Siemens Industry Online Support [https://support.industry.siemens.com] website. For more information, refer to https://support.industry.siemens.com/My/ww/en/requests.

To add software releases to the upgrade server, do the following:

1. Submit a Support Request to via Siemens Industry Online Support [https://support.industry.siemens.com]. Information will be provided by Siemens Customer Support on how to download the requested software package.
2. Download the software package to the upgrade directory on the upgrade server.

   NOTE
   *Software release filenames take 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.*
3. Extract the compressed ZIP file within the directory. The file will extract to a folder that has the same name as the major release (i.e. /rr2/dists/rr2.13.0). Subsequent releases will also be extracted to this folder (i.e. /rr2/dists/rr2.13.1).

Section 4.15.2.3
Adding Firmware Releases to the Upgrade Server

When configured, RUGGEDCOM ROX II can access the upgrade server to remotely upgrade firmware for the LTE modem. For more information, refer to Section 10.6.9, “Managing Firmware Updates”.

Siemens will provide a compressed ZIP file containing the upgrade package necessary to upgrade the firmware.

To add a firmware release to the upgrade server, do the following:

NOTE
For information about obtaining the ZIP file containing the files necessary to upgrade the firmware, contact Siemens Customer Support.

1. Obtain the compressed ZIP file containing the appropriate firmware release from Siemens.
2. Add the ZIP file to the upgrade directory on the upgrade server.
3. Extract the ZIP file within the directory.

Section 4.15.3
Upgrading the RUGGEDCOM ROX II Software

RUGGEDCOM ROX II software upgrades are managed between two partitions. One partition is always active, while the other is always inactive. Software upgrades are always applied to the inactive partition. This allows the active partition to function normally during a software upgrade and for users to roll back a software upgrade to previous version.

After a successful software upgrade and reboot, the upgraded partition is activated.

IMPORTANT!
When a microSD/microSDHC drive is used, do not remove the drive during the file transfer.

NOTE
All parameters are locked during a software upgrade until the device is rebooted and the upgraded partition is changed to an active state. This prevents post-upgrade configuration changes that are not carried over to the upgraded partition.

If required, the software upgrade can be stopped/declined at any time before the device is rebooted. For more information about stopping/declining a software upgrade, refer to Section 4.15.4, "Stopping/Declining a Software Upgrade".

NOTE
All system configurations and user files (i.e. configuration files, etc.) are carried over to the upgrade partition.

NOTE
If a major system failure is detected upon rebooting with the newly upgraded partition, the device will automatically roll back to the previously active partition.

To upgrade the RUGGEDCOM ROX II software, do the following:

1. If the source of the software is a microSD/microSDHC drive, insert the drive in the microSD/microSDHC port on the device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
2. Make sure the source of the software upgrade has been configured. For more information, refer to Section 4.15.1, "Configuring the Upgrade Source".
3. Make sure the CLI is in Configuration mode.
4. Launch the software upgrade wizard by typing:

```
wizard rox_upgrade
```

The wizard will require 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
The upgrade repository url is set to: http://rceng03/debianppc/rr2
Press <ENTER> to accept this or type a new address to change it:

The software release you are upgrading to is: rr2
Press <ENTER> to accept this or type a different version:

Checking for a more recent version of the upgrade system
Already running the most recent version of the upgrade system
****************************************************************
Launching ROXII Upgrade.......
```

```
Upgrading system to Partition 2
Estimating size of upgrade. This may take a few minutes....
31 packages to install, 20799050 bytes to download
15768 files, 635375611 bytes will be copied to Partition 2
Starting upgrade...

Preparing to transfer files to alternate partition. You may not see activity for a few minutes....

---- File Transfer Phase: 635375611 bytes, 15768 files ----
progress: 100%
File transfer phase complete.

Starting download of packages...

---- Package Download Phase ----
progress: 100%
Download phase complete.

Installing packages...

---- Package Install phase ----
progress: 100%
Package installation complete.

Upgrade to partition 2 completed successfully.
A reboot is required to run the upgraded partition.
```

5. If the software upgrade is successful, reboot the device or decline the software upgrade. For more information, refer to Section 4.6, "Rebooting the Device" or Section 4.15.4, "Stopping/Declining a Software Upgrade".

Section 4.15.4

Stopping/Declining a Software Upgrade

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

IMPORTANT!
A software upgrade can only be declined before the device is rebooted. If the software upgrade has already been activated following a reboot, the previous software version installed on the other partition can be activated. For more information, refer to Section 4.15.5.1, "Rolling Back a Software Upgrade".

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

```
admin software-upgrade decline-upgrade
```

Section 4.15.5

Downgrading the RUGGEDCOM ROX II Software

The RUGGEDCOM ROX II software can be downgraded to a previous release at any time.

CONTENTS

- Section 4.15.5.1, "Rolling Back a Software Upgrade"
- Section 4.15.5.2, "Downgrading Using ROXflash"

Section 4.15.5.1

Rolling Back a Software Upgrade

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

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

   ```
   admin software-upgrade 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.

Section 4.15.5.2

Downgrading Using ROXflash

ROXflash is used to flash any previous version of a RUGGEDCOM ROX II software image to the inactive partition. To obtain a RUGGEDCOM ROX II software image, contact Siemens Customer Support.

After a successful software downgrade and reboot, the downgraded partition is activated.

IMPORTANT!
Use ROXflash only to install earlier versions of the RUGGEDCOM ROX II software. Newer software versions should be installed using the software upgrade functions. For more information about upgrading the RUGGEDCOM ROX II software, refer to Section 4.15.3, "Upgrading the RUGGEDCOM ROX II Software".

IMPORTANT!
When a microSD/microSDHC drive is used, do not remove the drive during the file transfer.

NOTE
If a major system failure is detected upon rebooting with the newly downgraded partition, the device will automatically roll back to the previously active partition.

To flash the inactive partition with an earlier version of the RUGGEDCOM ROX II software, do the following:

1. Contact Siemens Customer Support and obtain the required firmware version. Two tarball files (*.tar.bz2) are provided: the firmware image and a GPG (GNU Private Guard) signature file.
2. Add both files to the upgrade repository or place them on a microSD/microSDHC drive.

3. If the source of the software is a microSD/microSDHC drive, insert the drive in the microSD/microSDHC port on the device. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
4. Make sure the CLI is in Configuration mode.

   IMPORTANT!
   For downgrades via HTTPS (SSL), the server's public key must be signed by a trusted Certificate Authority (CA).

5. 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 configurations 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:password@'.

   Enter url: ftp://root:admin@rceng03/debianppc/rr2/image/imagerr2.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.
   ```

6. If the software downgrade is successful, reboot the device. For more information, refer to Section 4.6, “Rebooting the Device”.

Section 4.16

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.

CAUTION!
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.

IMPORTANT!
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.

CONTENTS

- Section 4.16.1, "Enabling/Disabling the Boot Time Firmware Integrity"
- Section 4.16.2, "Checking the Firmware Integrity"
- Section 4.16.3, "Scheduling a Recurring Firmware Integrity Check"
- Section 4.16.4, "Viewing the Status of the Firmware Integrity Check"

Section 4.16.1
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, or type **`revert`** and press **Enter** to abort.

Section 4.16.2
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 operating system files
 have been modified or tampered with. For assistance, contact Siemens Customer Support.
```

Section 4.16.3
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 Section 5.10, "Scheduling Jobs".

Section 4.16.4
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 1 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 operating system files
 have been modified or tampered with. For assistance, contact Siemens Customer Support.
```

Section 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].

IMPORTANT!
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.

CONTENTS

- Section 4.17.1, "SFP Transceiver Support"
- Section 4.17.2, "Viewing SFP Information"
- Section 4.17.3, "Enabling/Disabling Smart SFP Mode"

Section 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 triggers an alarm and is logged in the syslog.

Smart SFP For Select Transceivers

Smart SFP mode is available for SFP transceivers installed in ports **5** and **6**. 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.

IMPORTANT!
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 Section 4.17.3, "Enabling/Disabling Smart SFP Mode".

Section 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
```

Section 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 SFP transceivers installed in ports 5 and 6.

NOTE
*To determine if an SFP transcever has been marked as **Unidentified**, refer to the `media` parameter under **interfaces » switch » swport » {port}**, where **{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 swport port sfp smart-sfp-mode
   ```

   Disable

   ```
   no interface switch swport 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 Section 8.1.2, "Configuring a Switched Ethernet Port".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

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.

CONTENTS

- Section 5.1, “Configuring the System Name and Location”
- Section 5.2, “Configuring the Host Name”
- Section 5.3, “Customizing the Welcome Screen”
- Section 5.4, “Setting the Maximum Number of Sessions”
- Section 5.5, “Enabling and Configuring WWW Interface Sessions”
- Section 5.6, “Enabling/Disabling Remote Access Through a VRF Interface”
- Section 5.7, “Managing Alarms”
- Section 5.8, “Managing Users”
- Section 5.9, “Managing Passwords and Passphrases”
- Section 5.10, “Scheduling Jobs”

Section 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 1 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 1 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 1 to 255 characters long **Default:** Contact

Parameter	Description
	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, or type **`revert`** and press **Enter** to abort.

Section 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:

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

Parameter	Description
name { name }	**Synopsis:** A string 1 to 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 1 to 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, or type **`revert`** and press **Enter** to abort.

Section 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 welcome message, type:

```
admin authentication banner message
```

Where:

- *`message`* is the custom welcome message

Section 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:** a 32-bit unsigned 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, or type **`revert`** and press **Enter** to abort.

Section 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	**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:** A 16-bit unsigned 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:** a 32-bit unsigned 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	**Synopsis:** { true, false } **Default:** true Redirects traffic from port 80 to port 443. If disabled, port 80 will be closed.
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.

Parameter	Description
	• 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, or type **`revert`** and press **Enter** to abort.

Section 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.

IMPORTANT!
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 Section 12.11.3, "Configuring VRF".
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 Section 14.2.2, "Enabling and Configuring SNMP Sessions".

Parameter	Description
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:** A 32-bit signed 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	**Synopsis:** { true, false } **Default:** true

Parameter	Description
	Enables access to the CLI over the VRF interface.
cli-listen-port { cli-listen-port }	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 22 The port the CLI will listen on for incoming connections over a VRF interface.
snmp-enabled	**Synopsis:** { true, false } **Default:** true Enables SNMP access over the VRF interface.
snmp-listen-port { snmp-listen-port }	**Synopsis:** A 32-bit signed 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, or type **`revert`** and press **Enter** to abort.

> **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 Section 14.2.2, "Enabling and Configuring SNMP Sessions".

Section 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.

Alarm Type	Description
Security	Security alarms are for certificate expiry events. 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 time services, link failover, Dynamic Domain Name Server (DNS) etc.

CONTENTS

- Section 5.7.1, “Pre-Configured Alarms”
- Section 5.7.2, “Viewing a List of Active Alarms”
- Section 5.7.3, “Clearing and Acknowledging Alarms”
- Section 5.7.4, “Configuring an Alarm”

Section 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.

Alarm Type	Alarm	Description	Suggested Resolution
Admin	Featurekey mismatch	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.
Chassis	PM1 bad supply	Input power to the power module is outside nominal operating range.	Make sure the input power operating range meets the device requirements.
Chassis	PM1 MOV protection bad	The Metal Oxide Varistor (MOV) protection component within the PM1 power module is damaged.	Contact Siemens Customer Support to return the power module.
Chassis	Real-time clock battery low	The Real-Time Clock (RTC) battery in the control module is depleted.	Contact Siemens Customer Support to return the device for repair.
Security	Firmware Integrity Check Failed	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.

Section 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
  ACTUATORS
```

```
-------------------------------------------------------------------------------------------------------
switch     1      1      notice    Link-up on port swport/1    Thu Oct  2 09:28:25 2014  clear-or-ack
  none
switch     2      1      warning   Link-down on port swport/4  Thu Oct  2 09:28:23 2014  resolve-or-ack
  resolved
```

For information on how to clear or acknowledge an active alarm, refer to Section 5.7.3, "Clearing and Acknowledging Alarms".

Section 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.

CONTENTS

- Section 5.7.3.1, "Clearing Alarms"
- Section 5.7.3.2, "Acknowledging Alarms"

Section 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

Section 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 acknowledge
```

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.

Section 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. This parameter is mandatory.
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, or type **`revert`** and press **Enter** to abort.

Section 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	×	×	✓

CAUTION!
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 Section 5.9.2, "Setting a User Password/Passphrase".

CONTENTS

- Section 5.8.1, "Viewing a List of Users"
- Section 5.8.2, "Adding a User"
- Section 5.8.3, "Deleting a User"
- Section 5.8.4, "Monitoring Users"

Section 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 Section 5.8.2, "Adding a User".

Section 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 Section 5.9.2, "Setting a User Password/Passphrase".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.
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 Section 6.6.2, "Managing User Authentication Keys".

Section 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, or type **revert** and press **Enter** to abort.

Section 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 message 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
```

CONTENTS

- Section 5.8.4.1, "Kicking Users from the Network"
- Section 5.8.4.2, "Sending Messages to Users"

Section 5.8.4.1

Kicking Users from the Network

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

Section 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

Section 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 Section 2.1, "Default User Names and Passwords".

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 alarm is generated. For example:

```
Error: Supplied password is shorter than the minimum password length: 12
```

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 Section 6.6.3, "Managing RADIUS Authentication" and Section 6.6.4, "Configuring TACACS+ Authentication".

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the device, change the default passwords before commissioning the device.

CAUTION!
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.

CONTENTS

- Section 5.9.1, "Configuring Password/Passphrase Complexity Rules"
- Section 5.9.2, "Setting a User Password/Passphrase"
- Section 5.9.3, "Setting the Boot Password/Passphrase"
- Section 5.9.4, "Setting the Maintenance Password/Passphrase"
- Section 5.9.5, "Resetting the Admin Password/Passphrase"
- Section 5.9.6, "Resetting the Boot Password/Passphrase"
- Section 5.9.7, "Resetting the Maintenance Password/Passphrase"

Section 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:** A 32-bit unsigned integer between 1 and 128 **Default:** 12 Minimum password length.
maximum-length { maximum-length }	**Synopsis:** A 32-bit unsigned integer between 1 and 128 **Default:** 128 Maximum password length.
uppercase-required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one uppercase letter.
lowercase-required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one lowercase letter.
digits-required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one numerical digit.
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, or type **`revert`** and press **Enter** to abort.

Section 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
```

Section 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 Section 2.5.1, "Accessing Different CLI Modes".

CAUTION!
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.

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
```

Section 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 Section 2.5.1, "Accessing Different CLI Modes".

CAUTION!
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
```

Section 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 Section 2.7.4, “Accessing Service Mode”.
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**.

IMPORTANT!
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-password-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-password-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 Section 4.6, "Rebooting the Device".
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 and Step 10 to reset the password/passphrase on the inactive partition and switch back to the original partition.

Section 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 Section 2.7.2, "Accessing Maintenance Mode".

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 Section 5.9.3, "Setting the Boot Password/Passphrase".

Section 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.

CAUTION!
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 Section 5.9.4, "Setting the Maintenance Password/Passphrase".
3. Reboot the device. For more information, refer to Section 4.6, "Rebooting the Device".
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 Section 2.2, "Logging In".
7. Repeat Step 1 and Step 5 to reset the password/passphrase on the inactive partition and switch back to the original partition.

Section 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.

CONTENTS

- Section 5.10.1, "Viewing a List of Scheduled Jobs"
- Section 5.10.2, "Adding a Scheduled Job"
- Section 5.10.3, "Deleting a Scheduled Job"

Section 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 Section 5.10.2, "Adding a Scheduled Job".

Section 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 1 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: • 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 1 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 1 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 1 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. This parameter is not required for configchange jobs.
job-month { job-month }	**Synopsis:** A string 1 to 32 characters long

Parameter	Description
	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 1 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 1 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. This parameter is mandatory.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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, or type **`revert`** and press **Enter** to abort.

6 Security

This chapter describes how to configure and manage the security-related features of RUGGEDCOM ROX II.

CONTENTS

- Section 6.1, "Enabling and Configuring CLI Sessions"
- Section 6.2, "Enabling and Configuring SFTP Sessions"
- Section 6.3, "Enabling/Disabling Brute Force Attack Protection"
- Section 6.4, "Enabling/Disabling SYN Cookies"
- Section 6.5, "Managing Port Security"
- Section 6.6, "Managing User Authentication"
- Section 6.7, "Managing Certificates and Keys"
- Section 6.8, "Managing Firewalls"
- Section 6.9, "Restricting Management Access to Specific Interfaces"

Section 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	**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:** A 16-bit unsigned 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

Parameter	Description
	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.
max-sessions { max-sessions }	**Synopsis:** a 32-bit unsigned 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 1 to 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, or type **`revert`** and press **Enter** to abort.

Section 6.2
Enabling and Configuring SFTP Sessions

To enable and configure SFTP sessions, 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
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:** A 16-bit unsigned 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

Parameter	Description
	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:** a 32-bit unsigned integer **Default:** 10

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.3
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.

IMPORTANT!
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), 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.

IMPORTANT!
Enabling, disabling or making a configuration change to the firewall will reset – but not disable – the BFA protection mechanism. Any hosts that were previously blocked will be allowed to log in again. If multiple hosts are actively attacking at the time, this could result in reduced system performance.

When BFA protection is started, the following Syslog entry is displayed:

```
Jun  5 09:36:34 ruggedcom firewallmgr[3644]: Enabling Brute Force Attack Protection
```

When a host fails to login, an entry is logged in `auth.log`. For example:

```
Jun  5 10:12:52 ruggedcom confd[3386]: audit user: admin/0 Provided bad password
Jun  5 10:12:52 ruggedcom rmfmgr[3512]: login failed, reason='Bad password', user ipaddr='172.11.150.1'
Jun  5 10:12:52 ruggedcom confd[3386]: audit user: admin/0 Failed to login over ssh: Bad password
```

`Auth.log` also details which IP addresses are currently being blocked:

```
Jun 5 14:43:04 ruggedrouter sshguard[24720]: Blocking 172.59.9.1:4 for >630secs: 60 danger in 5 attacks
over 70 seconds (all: 60d in 1 abuses over 70s).
```

NOTE
For information about how to view `auth.log`*, refer to Section 4.12.1, "Viewing Logs".*

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, or type **revert** and press **Enter** to abort.
4. [Optional] Enable or disable the default alarm for brute force attacks. For more information, refer to Section 5.7.4, "Configuring an Alarm".

Section 6.4

Enabling/Disabling SYN Cookies

RUGGEDCOM ROX II can be configured to transmit SYN cookies when the SYN backlog queue of a socket begins to overflow. This is a technique used to resist SYN flood attacks.

To enable or disable the transmission of SYN cookies, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 6.5

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 PEAP, EAP-TLS and EAP-MD5. PEAP and EAP-TLS are more secure and are recommended over EAP-MD5.

IMPORTANT!
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.

CONTENTS

- Section 6.5.1, “Port Security Concepts”
- Section 6.5.2, “Configuring Port Security”
- Section 6.5.3, “Viewing the Security Status of Switched Ethernet Ports”

Section 6.5.1

Port Security Concepts

This section describes some of the concepts important to the implementation of port security in RUGGEDCOM ROX II.

CONTENTS

- Section 6.5.1.1, “Static MAC Address-Based Authentication”
- Section 6.5.1.2, “IEEE 802.1x Authentication”
- Section 6.5.1.3, “IEEE 802.1X Authentication with MAC Address-Based Authentication”
- Section 6.5.1.4, “Assigning VLANS with Tunnel Attributes”

Section 6.5.1.1
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.

Section 6.5.1.2
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.

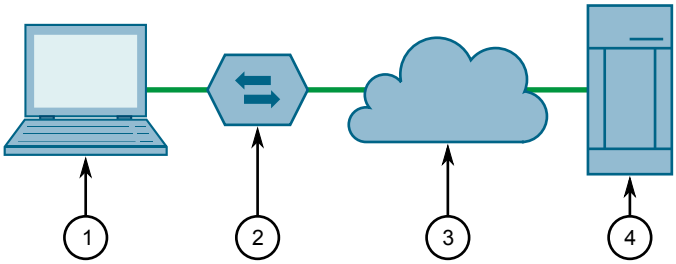


Figure 4: IEEE 802.1x General Topology

1. Supplicant **2.** Authenticator Device **3.** LAN **4.** Authentication Server

IMPORTANT!
RUGGEDCOM ROX II supports Protected Extensible Authentication Protocol (PEAP), EAP Transport Layer Security (EAP-TLS) and EAP-MD5. PEAP and EAP-TLS are more secure and are 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 Section 6.6.3.3, “Configuring RADIUS Authentication for Switched Ethernet Ports”.

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.

Section 6.5.1.3
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.

Section 6.5.1.4
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.

Section 6.5.2
Configuring Port Security

To configure port security for a switched Ethernet port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » switch » swport » {port} » port-security***, where *{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.

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
auto-learn { auto-learn }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed integer between 1 and 65535 **Default:** 30

Parameter	Description
	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:** A 32-bit signed 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.
reauth-period { reauth-period }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed 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 Section 6.6.3.3, "Configuring RADIUS Authentication for Switched Ethernet Ports".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.5.3

Viewing the Security Status of Switched Ethernet Ports

To view the port security status of all switched Ethernet ports, type:

```
show interfaces switch swport port-security
```

For example:

```
show interfaces switch swport port-security
SLOT    PORT  STATUS
------------------------
swport  1     Unsecure
swport  2     Unsecure
swport  3     Unsecure
swport  4     Unsecure
swport  5     Unsecure
swport  6     Unsecure
```

To view the port security status of a specific switched Ethernet port, type:

```
show interfaces switch swport port port-security
```

Where:

- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

For example:

```
show interfaces switch swport 1 port-security
port-security
 status Unsecure
```

Section 6.6

Managing User Authentication

This section describes the various methods for authenticating users.

CONTENTS

- Section 6.6.1, “Setting the User Authentication Mode”
- Section 6.6.2, “Managing User Authentication Keys”
- Section 6.6.3, “Managing RADIUS Authentication”
- Section 6.6.4, “Configuring TACACS+ Authentication”

Section 6.6.1

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.

To set the authentication mode, type:

```
admin authentication mode [ localonly | radius_local | radius_only | radius_then_local |
tacacsplus_local | tacacsplus_only ]
```

- 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.

Section 6.6.2
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.

IMPORTANT!
RUGGEDCOM ROX II only accepts SSH2 RSA public keys. SSH1 or DSA keys are not supported.

CONTENTS

- Section 6.6.2.1, “Determining Which Keys are Associated to a User”
- Section 6.6.2.2, “Adding a User Authentication Key”
- Section 6.6.2.3, “Deleting a User Authentication Key”
- Section 6.6.2.4, “Associating/Disassociating a User Authentication Key”

Section 6.6.2.1
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 authorized-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 Section 6.6.2.4, “Associating/Disassociating a User Authentication Key”.

Section 6.6.2.2
Adding a User Authentication Key

To add a user authentication key to the device, do the following:

CAUTION!
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.

IMPORTANT!
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 Section 2.2, "Logging In".
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, or type **`revert`** and press **Enter** to abort.
9. Associate the new authentication key with one or more user accounts. For more information, refer to Section 6.6.2.4, "Associating/Disassociating a User Authentication Key".

Section 6.6.2.3
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 Section 6.6.2.4, "Associating/Disassociating a User Authentication Key".
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, or type **revert** and press **Enter** to abort.

Section 6.6.2.4
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.

IMPORTANT!
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 Section 2.2, "Logging In".
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, or type **revert** and press **Enter** to abort.

» 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 Section 2.2, "Logging In".
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, or type **revert** and press **Enter** to abort.

Section 6.6.3

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].

IMPORTANT!
*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 Section 6.6.1, "Setting the User Authentication Mode".*

IMPORTANT!
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 Section 4.12.1, "Viewing Logs".*

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.

CONTENTS

- Section 6.6.3.1, "Configuring RADIUS Authentication for LOGIN Services"
- Section 6.6.3.2, "Configuring RADIUS Authentication for PPP Services"
- Section 6.6.3.3, "Configuring RADIUS Authentication for Switched Ethernet Ports"

Section 6.6.3.1
Configuring RADIUS Authentication for LOGIN Services

To configure RADIUS authentication for LOGIN services, do the following:

IMPORTANT!
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 7 to 15 characters long or a string 6 to 40 characters long The NAS-IP-Address. Set this to the primary IP address of the unit.
nas-identifier { nas-identifier }	**Synopsis:** A string 1 to 64 characters long

Parameter	Description
	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 7 to 15 characters long or a string 6 to 40 characters long The IP address of the server.
port-udp { port-udp }	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 1812 The network port of the server.
password { password }	**Synopsis:** A string The password of the RADIUS server.

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.6.3.2
Configuring RADIUS Authentication for PPP Services

To configure RADIUS authentication for PPP services, do the following:

IMPORTANT!
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 7 to 15 characters long The IPv4 address of the server.
port-udp { port-udp }	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 1812
password { password }	**Synopsis:** A string

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.6.3.3
Configuring RADIUS Authentication for Switched Ethernet Ports

To configure RADIUS authentication for switched Ethernet ports, do the following:

IMPORTANT!
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 7 to 15 characters long The IPv4 address of the server.
port-udp { port-udp }	**Synopsis:** A 32-bit signed 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, or type **revert** and press **Enter** to abort.

Section 6.6.4
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.

IMPORTANT!
*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 Section 6.6.1, "Setting the User Authentication Mode".*

To configure TACACS+ authentication, do the following:

IMPORTANT!
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 1 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 1 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 1 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 7 to 15 characters long or a string 6 to 40 characters long The IP address of the TACACS+ server.
port-tcp { port-tcp }	**Synopsis:** A 32-bit signed 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, or type **`revert`** and press **Enter** to abort.

Section 6.7

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.

CONTENTS

- Section 6.7.1, “Viewing the Local Host SSH/RSA Public Key”
- Section 6.7.2, “Managing the Trusted Certificate Store”

- Section 6.7.3, "Managing CA Certificates for the Trusted Certificate Store"
- Section 6.7.4, "Managing CA Certificates and CRLs"
- Section 6.7.5, "Managing Private Keys"
- Section 6.7.6, "Managing Public Keys"
- Section 6.7.7, "Managing Certificates"
- Section 6.7.8, "Managing Known Hosts"

Section 6.7.1

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 AAAAB3NzaC1yc2EAAAADAQABAAABAQC0De8wvPyFpUGph9mwNXPcY3/
dwmQxIelGZe5Pt4laOZpeGOtuMSKqN15jcx29RcBasSdui5muLq8o+iBfDwjJw2q5WBBqyweXHgGYQGC58e7PQ5eYWIvu2L/
cgTpR3rCs4xTUh+URJYCTGEhh1V6jGOjuY8M3pO/iLPrwtZ066uyCqNoJLoptYnLfRDJu8AdWNdxLfXQsSv4XOB8hzYKekyg8bqsE/
w6b5MyE60Xc51f413PMicZz6WhBcuaqvutHxoIqCR6oI7fkLGGyWaeCzWUO02FplVfiJe1vTwAaa5+JAoSdPNzTJKrHvFE18SdEAlwpj4PMVIA7c
```

Section 6.7.2

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 Section 6.7.2.3, "List of Root Certificates in the Trusted Certificate Store".

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 Section 6.7.7.3, "Adding a Certificate".

CONTENTS

- Section 6.7.2.1, "Configuring the Trusted Certificate Store"
- Section 6.7.2.2, "Enabling/Disabling the Trusted Certificate Store"
- Section 6.7.2.3, "List of Root Certificates in the Trusted Certificate Store"

Section 6.7.2.1
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 Section 6.7.4.3, "Adding a CA Certificate and CRL".
2. Enable the Trusted Certificate Store. For more information, refer to Section 6.7.2.2, "Enabling/Disabling the Trusted Certificate Store".
3. Add CA certificates to the Store to validate the authenticity of the root certificates. For more information, refer to Section 6.7.3.2, "Adding a CA Certificate to the Trusted Certificate Store".

Section 6.7.2.2
Enabling/Disabling the Trusted Certificate Store

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, or type **`revert`** and press **Enter** to abort.

Section 6.7.2.3
List of Root Certificates in the Trusted Certificate Store

The Trusted Certificate Store adds the following X.509 v3 root certificates when enabled:

- **spi-cacert-2008.crt**
  Subject Name: /C=US/ST=Indiana/L=Indianapolis/O=Software in the Public Interest/OU=hostmaster/CN=Certificate Authority/emailAddress=hostmaster@spi-inc.org
  Fingerprint: AF:70:88:43:83:82:02:15:CD:61:C6:BC:EC:FD:37:24:A9:90:43:1C
  Issued: May 13 08:07:56 2008 GMT
  Expires: May 11 08:07:56 2018 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: 27:96:BA:E6:3F:18:01:E2:77:26:1B:A0:D7:77:70:02:8F:20:EE:E4
  Issued: Jun 29 17:06:20 2004 GMT
  Expires: Jun 29 17:06:20 2034 GMT
- **Staat_der_Nederlanden_EV_Root_CA**
  Subject Name: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden EV Root CA

Fingerprint: 76:E2:7E:C1:4F:DB:82:C1:C0:A6:75:B5:05:BE:3D:29:B4:ED:DB:BB

Issued: Dec 8 11:19:29 2010 GMT

Expires: Dec 8 11:10:28 2022 GMT

- **Certinomis_-_Root_CA**
  Subject Name: /C=FR/O=Certinomis/OU=0002 433998903/CN=Certinomis - Root CA

  Fingerprint: 9D:70:BB:01:A5:A4:A0:18:11:2E:F7:1C:01:B9:32:C5:34:E7:88:A8

  Issued: Oct 21 09:17:18 2013 GMT

  Expires: Oct 21 09:17:18 2033 GMT
- **OISTE_WISeKey_Global_Root_GB_CA**
  Subject Name: /C=CH/O=WISeKey/OU=OISTE Foundation Endorsed/CN=OISTE WISeKey Global Root GB CA

  Fingerprint: 0F:F9:40:76:18:D3:D7:6A:4B:98:F0:A8:35:9E:0C:FD:27:AC:CC:ED

  Issued: Dec 1 15:00:32 2014 GMT

  Expires: Dec 1 15:10:31 2039 GMT
- **QuoVadis_Root_CA**
  Subject Name: /C=BM/O=QuoVadis Limited/OU=Root Certification Authority/CN=QuoVadis Root Certification Authority

  Fingerprint: DE:3F:40:BD:50:93:D3:9B:6C:60:F6:DA:BC:07:62:01:00:89:76:C9

  Issued: Mar 19 18:33:33 2001 GMT

  Expires: Mar 17 18:33:33 2021 GMT
- **DigiCert_Global_Root_G2**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2

  Fingerprint: DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT
- **Entrust.net_Premium_2048_Secure_Server_CA**
  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: 50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31

  Issued: Dec 24 17:50:51 1999 GMT

  Expires: Jul 24 14:15:12 2029 GMT
- **TÃœRKTRUST_Elektronik_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±_H5**
  Subject Name: /C=TR/L=Ankara/O=TxC3x9CRKTRUST Bilgi xC4xB0letixC5x9Fim ve BilixC5x9Fim GxC3xBCvenlixC4x9Fi Hizmetleri A.xC5x9E./CN=TxC3x9CRKTRUST Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1 H5

  Fingerprint: C4:18:F6:4D:46:D1:DF:00:3D:27:30:13:72:43:A9:12:11:C6:75:FB

  Issued: Apr 30 08:07:01 2013 GMT

  Expires: Apr 28 08:07:01 2023 GMT

- **Verisign_Class_2_Public_Primary_Certification_Authority_-_G2**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 2 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network

  Fingerprint: B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D

  Issued: May 18 00:00:00 1998 GMT

  Expires: Aug 1 23:59:59 2028 GMT
- **UTN_USERFirst_Email_Root_CA**
  Subject Name: /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Client Authentication and Email

  Fingerprint: B1:72:B1:A5:6D:95:F9:1F:E5:02:87:E1:4D:37:EA:6A:44:63:76:8A

  Issued: Jul 9 17:28:50 1999 GMT

  Expires: Jul 9 17:36:58 2019 GMT
- **AC_RaÃz_CerticÃ¡mara_S.A.**
  Subject Name: /C=CO/O=Sociedad Cameral de CertificacixC3xB3n Digital - CerticxC3xA1mara S.A./CN=AC RaxC3xADz CerticxC3xA1mara S.A.

  Fingerprint: CB:A1:C5:F8:B0:E3:5E:B8:B9:45:12:D3:F9:34:A2:E9:06:10:D3:36

  Issued: Nov 27 20:46:29 2006 GMT

  Expires: Apr 2 21:42:02 2030 GMT
- **IGC_A**
  Subject Name: /C=FR/ST=France/L=Paris/O=PM/SGDN/OU=DCSSI/CN=IGC/A/emailAddress=igca@sgdn.pm.gouv.fr

  Fingerprint: 60:D6:89:74:B5:C2:65:9E:8A:0F:C1:88:7C:88:D2:46:69:1B:18:2C

  Issued: Dec 13 14:29:23 2002 GMT

  Expires: Oct 17 14:29:22 2020 GMT
- **Verisign_Class_1_Public_Primary_Certification_Authority**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority

  Fingerprint: CE:6A:64:A3:09:E4:2F:BB:D9:85:1C:45:3E:64:09:EA:E8:7D:60:F1

  Issued: Jan 29 00:00:00 1996 GMT

  Expires: Aug 2 23:59:59 2028 GMT
- **AffirmTrust_Premium_ECC**
  Subject Name: /C=US/O=AffirmTrust/CN=AffirmTrust Premium ECC

  Fingerprint: B8:23:6B:00:2F:1D:16:86:53:01:55:6C:11:A4:37:CA:EB:FF:C3:BB

  Issued: Jan 29 14:20:24 2010 GMT

  Expires: Dec 31 14:20:24 2040 GMT
- **Staat_der_Nederlanden_Root_CA_-_G3**
  Subject Name: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA - G3

  Fingerprint: D8:EB:6B:41:51:92:59:E0:F3:E7:85:00:C0:3D:B6:88:97:C9:EE:FC

Issued: Nov 14 11:28:42 2013 GMT

Expires: Nov 13 23:00:00 2028 GMT

- **Swisscom_Root_CA_1**
  Subject Name: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root CA 1

  Fingerprint: 5F:3A:FC:0A:8B:64:F6:86:67:34:74:DF:7E:A9:A2:FE:F9:FA:7A:51

  Issued: Aug 18 12:06:20 2005 GMT

  Expires: Aug 18 22:06:20 2025 GMT
- **ComSign_CA**
  Subject Name: /CN=ComSign CA/O=ComSign/C=IL

  Fingerprint: E1:A4:5B:14:1A:21:DA:1A:79:F4:1A:42:A9:61:D6:69:CD:06:34:C1

  Issued: Mar 24 11:32:18 2004 GMT

  Expires: Mar 19 15:02:18 2029 GMT
- **Sonera_Class_2_Root_CA**
  Subject Name: /C=FI/O=Sonera/CN=Sonera Class2 CA

  Fingerprint: 37:F7:6D:E6:07:7C:90:C5:B1:3E:93:1A:B7:41:10:B4:F2:E4:9A:27

  Issued: Apr 6 07:29:40 2001 GMT

  Expires: Apr 6 07:29:40 2021 GMT
- **GeoTrust_Primary_Certification_Authority_-_G3**
  Subject Name: /C=US/O=GeoTrust Inc./OU=(c) 2008 GeoTrust Inc. - For authorized use only/CN=GeoTrust Primary Certification Authority - G3

  Fingerprint: 03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD

  Issued: Apr 2 00:00:00 2008 GMT

  Expires: Dec 1 23:59:59 2037 GMT
- **Comodo_AAA_Services_root**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services

  Fingerprint: D1:EB:23:A4:6D:17:D6:8F:D9:25:64:C2:F1:F1:60:17:64:D8:E3:49

  Issued: Jan 1 00:00:00 2004 GMT

  Expires: Dec 31 23:59:59 2028 GMT
- **DigiCert_Global_Root_G3**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G3

  Fingerprint: 7E:04:DE:89:6A:3E:66:6D:00:E6:87:D3:3F:FA:D9:3B:E8:3D:34:9E

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT
- **DST_ACES_CA_X6**
  Subject Name: /C=US/O=Digital Signature Trust/OU=DST ACES/CN=DST ACES CA X6

  Fingerprint: 40:54:DA:6F:1C:3F:40:74:AC:ED:0F:EC:CD:DB:79:D1:53:FB:90:1D

Issued: Nov 20 21:19:58 2003 GMT

Expires: Nov 20 21:19:58 2017 GMT

- **Deutsche_Telekom_Root_CA_2**
  Subject Name: /C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2

  Fingerprint: 85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF

  Issued: Jul 9 12:11:00 1999 GMT

  Expires: Jul 9 23:59:00 2019 GMT
- **TeliaSonera_Root_CA_v1**
  Subject Name: /O=TeliaSonera/CN=TeliaSonera Root CA v1

  Fingerprint: 43:13:BB:96:F1:D5:86:9B:C1:4E:6A:92:F6:CF:F6:34:69:87:82:37

  Issued: Oct 18 12:00:50 2007 GMT

  Expires: Oct 18 12:00:50 2032 GMT
- **DST_Root_CA_X3**
  Subject Name: /O=Digital Signature Trust Co./CN=DST Root CA X3

  Fingerprint: DA:C9:02:4F:54:D8:F6:DF:94:93:5F:B1:73:26:38:CA:6A:D7:7C:13

  Issued: Sep 30 21:12:19 2000 GMT

  Expires: Sep 30 14:01:15 2021 GMT
- **Comodo_Secure_Services_root**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=Secure Certificate Services

  Fingerprint: 4A:65:D5:F4:1D:EF:39:B8:B8:90:4A:4A:D3:64:81:33:CF:C7:A1:D1

  Issued: Jan 1 00:00:00 2004 GMT

  Expires: Dec 31 23:59:59 2028 GMT
- **TURKTRUST_Certificate_Services_Provider_Root_2007**
  Subject Name: /CN=TxC3x9CRKTRUST Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1/C=TR/L=Ankara/O=TxC3x9CRKTRUST Bilgi xC4xB0letixC5x9Fim ve BilixC5x9Fim GxC3xBCvenlixC4x9Fi Hizmetleri A.xC5x9E. (c) AralxC4xB1k 2007

  Fingerprint: F1:7F:6F:B6:31:DC:99:E3:A3:C8:7F:FE:1C:F1:81:10:88:D9:60:33

  Issued: Dec 25 18:37:19 2007 GMT

  Expires: Dec 22 18:37:19 2017 GMT
- **Certplus_Class_2_Primary_CA**
  Subject Name: /C=FR/O=Certplus/CN=Class 2 Primary CA

  Fingerprint: 74:20:74:41:72:9C:DD:92:EC:79:31:D8:23:10:8D:C2:81:92:E2:BB

  Issued: Jul 7 17:05:00 1999 GMT

  Expires: Jul 6 23:59:59 2019 GMT

- **IdenTrust_Public_Sector_Root_CA_1**
  Subject Name: /C=US/O=IdenTrust/CN=IdenTrust Public Sector Root CA 1

  Fingerprint: BA:29:41:60:77:98:3F:F4:F3:EF:F2:31:05:3B:2E:EA:6D:4D:45:FD

  Issued: Jan 16 17:53:32 2014 GMT

  Expires: Jan 16 17:53:32 2034 GMT
- **EE_Certification_Centre_Root_CA**
  Subject Name: /C=EE/O=AS Sertifitseerimiskeskus/CN=EE Certification Centre Root CA/emailAddress=pki@sk.ee

  Fingerprint: C9:A8:B9:E7:55:80:5E:58:E3:53:77:A7:25:EB:AF:C3:7B:27:CC:D7

  Issued: Oct 30 10:10:30 2010 GMT

  Expires: Dec 17 23:59:59 2030 GMT
- **Staat_der_Nederlanden_Root_CA**
  Subject Name: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA

  Fingerprint: 10:1D:FA:3F:D5:0B:CB:BB:9B:B5:60:0C:19:55:A4:1A:F4:73:3A:04

  Issued: Dec 17 09:23:49 2002 GMT

  Expires: Dec 16 09:15:38 2015 GMT
- **S-TRUST_Universal_Root_CA**
  Subject Name: /C=DE/O=Deutscher Sparkassen Verlag GmbH/OU=S-TRUST Certification Services/CN=S-TRUST Universal Root CA

  Fingerprint: 1B:3D:11:14:EA:7A:0F:95:58:54:41:95:BF:6B:25:82:AB:40:CE:9A

  Issued: Oct 22 00:00:00 2013 GMT

  Expires: Oct 21 23:59:59 2038 GMT
- **DigiCert_Global_Root_CA**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA

  Fingerprint: A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36

  Issued: Nov 10 00:00:00 2006 GMT

  Expires: Nov 10 00:00:00 2031 GMT
- **DigiCert_Assured_ID_Root_CA**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root CA

  Fingerprint: 05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43

  Issued: Nov 10 00:00:00 2006 GMT

  Expires: Nov 10 00:00:00 2031 GMT
- **GlobalSign_ECC_Root_CA_-_R4**
  Subject Name: /OU=GlobalSign ECC Root CA - R4/O=GlobalSign/CN=GlobalSign

  Fingerprint: 69:69:56:2E:40:80:F4:24:A1:E7:19:9F:14:BA:F3:EE:58:AB:6A:BB

  Issued: Nov 13 00:00:00 2012 GMT

  Expires: Jan 19 03:14:07 2038 GMT

- **AffirmTrust_Premium**
  Subject Name: /C=US/O=AffirmTrust/CN=AffirmTrust Premium

  Fingerprint: D8:A6:33:2C:E0:03:6F:B1:85:F6:63:4F:7D:6A:06:65:26:32:28:27

  Issued: Jan 29 14:10:36 2010 GMT

  Expires: Dec 31 14:10:36 2040 GMT
- **USERTrust_RSA_Certification_Authority**
  Subject Name: /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

  Fingerprint: 2B:8F:1B:57:33:0D:BB:A2:D0:7A:6C:51:F7:0E:E9:0D:DA:B9:AD:8E

  Issued: Feb 1 00:00:00 2010 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **certSIGN_ROOT_CA**
  Subject Name: /C=RO/O=certSIGN/OU=certSIGN ROOT CA

  Fingerprint: FA:B7:EE:36:97:26:62:FB:2D:B0:2A:F6:BF:03:FD:E8:7C:4B:2F:9B

  Issued: Jul 4 17:20:04 2006 GMT

  Expires: Jul 4 17:20:04 2031 GMT
- **ACCVRAIZ1**
  Subject Name: /CN=ACCVRAIZ1/OU=PKIACCV/O=ACCV/C=ES

  Fingerprint: 93:05:7A:88:15:C6:4F:CE:88:2F:FA:91:16:52:28:78:BC:53:64:17

  Issued: May 5 09:37:37 2011 GMT

  Expires: Dec 31 09:37:37 2030 GMT
- **TÃœBÄ°TAK_UEKAE_KÃ¶k_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±_-_SÃ¼rÃ¼m_3**
  Subject Name: /C=TR/L=Gebze - Kocaeli/O=TxC3xBCrkiye Bilimsel ve Teknolojik AraxC5x9FtxC4xB1rma Kurumu - TxC3x9CBxC4xB0TAK/OU=Ulusal Elektronik ve Kriptoloji AraxC5x9FtxC4xB1rma EnstitxC3xBCsxC3xBC - UEKAE/OU=Kamu Sertifikasyon Merkezi/CN=TxC3x9CBxC4xB0TAK UEKAE KxC3xB6k Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1 - SxC3xBCrxC3xBCm 3

  Fingerprint: 1B:4B:39:61:26:27:6B:64:91:A2:68:6D:D7:02:43:21:2D:1F:1D:96

  Issued: Aug 24 11:37:07 2007 GMT

  Expires: Aug 21 11:37:07 2017 GMT
- **AddTrust_Qualified_Certificates_Root**
  Subject Name: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Qualified CA Root

  Fingerprint: 4D:23:78:EC:91:95:39:B5:00:7F:75:8F:03:3B:21:1E:C5:4D:8B:CF

  Issued: May 30 10:44:50 2000 GMT

  Expires: May 30 10:44:50 2020 GMT
- **AffirmTrust_Commercial**
  Subject Name: /C=US/O=AffirmTrust/CN=AffirmTrust Commercial

  Fingerprint: F9:B5:B6:32:45:5F:9C:BE:EC:57:5F:80:DC:E9:6E:2C:C7:B2:78:B7

Issued: Jan 29 14:06:06 2010 GMT

Expires: Dec 31 14:06:06 2030 GMT

- **UTN_USERFirst_Hardware_Root_CA**
  Subject Name: /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware

  Fingerprint: 04:83:ED:33:99:AC:36:08:05:87:22:ED:BC:5E:46:00:E3:BE:F9:D7

  Issued: Jul 9 18:10:42 1999 GMT

  Expires: Jul 9 18:19:22 2019 GMT
- **Visa_eCommerce_Root**
  Subject Name: /C=US/O=VISA/OU=Visa International Service Association/CN=Visa eCommerce Root

  Fingerprint: 70:17:9B:86:8C:00:A4:FA:60:91:52:22:3F:9F:3E:32:BD:E0:05:62

  Issued: Jun 26 02:18:36 2002 GMT

  Expires: Jun 24 00:16:12 2022 GMT
- **AddTrust_Public_Services_Root**
  Subject Name: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Public CA Root

  Fingerprint: 2A:B6:28:48:5E:78:FB:F3:AD:9E:79:10:DD:6B:DF:99:72:2C:96:E5

  Issued: May 30 10:41:50 2000 GMT

  Expires: May 30 10:41:50 2020 GMT
- **thawte_Primary_Root_CA**
  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: 91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81

  Issued: Nov 17 00:00:00 2006 GMT

  Expires: Jul 16 23:59:59 2036 GMT
- **StartCom_Certification_Authority**
  Subject Name: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority

  Fingerprint: 3E:2B:F7:F2:03:1B:96:F3:8C:E6:C4:D8:A8:5D:3E:2D:58:47:6A:0F

  Issued: Sep 17 19:46:36 2006 GMT

  Expires: Sep 17 19:46:36 2036 GMT
- **StartCom_Certification_Authority_2**
  Subject Name: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority

  Fingerprint: A3:F1:33:3F:E2:42:BF:CF:C5:D1:4E:8F:39:42:98:40:68:10:D1:A0

  Issued: Sep 17 19:46:37 2006 GMT

  Expires: Sep 17 19:46:36 2036 GMT

- **Go_Daddy_Root_Certificate_Authority_-_G2**
  Subject Name: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2

  Fingerprint: 47:BE:AB:C9:22:EA:E8:0E:78:78:34:62:A7:9F:45:C2:54:FD:E6:8B

  Issued: Sep 1 00:00:00 2009 GMT

  Expires: Dec 31 23:59:59 2037 GMT
- **DigiCert_Trusted_Root_G4**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Trusted Root G4

  Fingerprint: DD:FB:16:CD:49:31:C9:73:A2:03:7D:3F:C8:3A:4D:7D:77:5D:05:E4

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT
- **Equifax_Secure_eBusiness_CA_1**
  Subject Name: /C=US/O=Equifax Secure Inc./CN=Equifax Secure eBusiness CA-1

  Fingerprint: DA:40:18:8B:91:89:A3:ED:EE:AE:DA:97:FE:2F:9D:F5:B7:D1:8A:41

  Issued: Jun 21 04:00:00 1999 GMT

  Expires: Jun 21 04:00:00 2020 GMT
- **China_Internet_Network_Information_Center_EV_Certificates_Root**
  Subject Name: /C=CN/O=China Internet Network Information Center/CN=China Internet Network Information Center EV Certificates Root

  Fingerprint: 4F:99:AA:93:FB:2B:D1:37:26:A1:99:4A:CE:7F:F0:05:F2:93:5D:1E

  Issued: Aug 31 07:11:25 2010 GMT

  Expires: Aug 31 07:11:25 2030 GMT
- **GeoTrust_Universal_CA_2**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Universal CA 2

  Fingerprint: 37:9A:19:7B:41:85:45:35:0C:A6:03:69:F3:3C:2E:AF:47:4F:20:79

  Issued: Mar 4 05:00:00 2004 GMT

  Expires: Mar 4 05:00:00 2029 GMT
- **Certinomis_-_AutoritÃ©_Racine**
  Subject Name: /C=FR/O=Certinomis/OU=0002 433998903/CN=Certinomis - AutoritxC3xA9 Racine

  Fingerprint: 2E:14:DA:EC:28:F0:FA:1E:8E:38:9A:4E:AB:EB:26:C0:0A:D3:83:C3

  Issued: Sep 17 08:28:59 2008 GMT

  Expires: Sep 17 08:28:59 2028 GMT
- **NetLock_Notary_=Class_A=_Root**
  Subject Name: /C=HU/ST=Hungary/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado

  Fingerprint: AC:ED:5F:65:53:FD:25:CE:01:5F:1F:7A:48:3B:6A:74:9F:61:78:C6

  Issued: Feb 24 23:14:47 1999 GMT

Expires: Feb 19 23:14:47 2019 GMT

- **WoSign_China**
  Subject Name: /C=CN/O=WoSign CA Limited/CN=CA xE6xB2x83xE9x80x9AxE6xA0xB9xE8xAFx81xE4xB9xA6

  Fingerprint: 16:32:47:8D:89:F9:21:3A:92:00:85:63:F5:A4:A7:D3:12:40:8A:D6

  Issued: Aug 8 01:00:01 2009 GMT

  Expires: Aug 8 01:00:01 2039 GMT
- **AffirmTrust_Networking**
  Subject Name: /C=US/O=AffirmTrust/CN=AffirmTrust Networking

  Fingerprint: 29:36:21:02:8B:20:ED:02:F5:66:C5:32:D1:D6:ED:90:9F:45:00:2F

  Issued: Jan 29 14:08:24 2010 GMT

  Expires: Dec 31 14:08:24 2030 GMT
- **D-TRUST_Root_Class_3_CA_2_2009**
  Subject Name: /C=DE/O=D-Trust GmbH/CN=D-TRUST Root Class 3 CA 2 2009

  Fingerprint: 58:E8:AB:B0:36:15:33:FB:80:F7:9B:1B:6D:29:D3:FF:8D:5F:00:F0

  Issued: Nov 5 08:35:58 2009 GMT

  Expires: Nov 5 08:35:58 2029 GMT
- **COMODO_Certification_Authority**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO Certification Authority

  Fingerprint: 66:31:BF:9E:F7:4F:9E:B6:C9:D5:A6:0C:BA:6A:BE:D1:F7:BD:EF:7B

  Issued: Dec 1 00:00:00 2006 GMT

  Expires: Dec 31 23:59:59 2029 GMT
- **CA_Disig_Root_R1**
  Subject Name: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig Root R1

  Fingerprint: 8E:1C:74:F8:A6:20:B9:E5:8A:F4:61:FA:EC:2B:47:56:51:1A:52:C6

  Issued: Jul 19 09:06:56 2012 GMT

  Expires: Jul 19 09:06:56 2042 GMT
- **thawte_Primary_Root_CA_-_G3**
  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: F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2

  Issued: Apr 2 00:00:00 2008 GMT

  Expires: Dec 1 23:59:59 2037 GMT
- **AddTrust_External_Root**
  Subject Name: /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

  Fingerprint: 02:FA:F3:E2:91:43:54:68:60:78:57:69:4D:F5:E4:5B:68:85:18:68

Issued: May 30 10:48:38 2000 GMT

Expires: May 30 10:48:38 2020 GMT

- **ACEDICOM_Root**
  Subject Name: /CN=ACEDICOM Root/OU=PKI/O=EDICOM/C=ES

  Fingerprint: E0:B4:32:2E:B2:F6:A5:68:B6:54:53:84:48:18:4A:50:36:87:43:84

  Issued: Apr 18 16:24:22 2008 GMT

  Expires: Apr 13 16:24:22 2028 GMT
- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5**
  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: 4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5

  Issued: Nov 8 00:00:00 2006 GMT

  Expires: Jul 16 23:59:59 2036 GMT
- **IdenTrust_Commercial_Root_CA_1**
  Subject Name: /C=US/O=IdenTrust/CN=IdenTrust Commercial Root CA 1

  Fingerprint: DF:71:7E:AA:4A:D9:4E:C9:55:84:99:60:2D:48:DE:5F:BC:F0:3A:25

  Issued: Jan 16 18:12:23 2014 GMT

  Expires: Jan 16 18:12:23 2034 GMT
- **Juur-SK**
  Subject Name: /emailAddress=pki@sk.ee/C=EE/O=AS Sertifitseerimiskeskus/CN=Juur-SK

  Fingerprint: 40:9D:4B:D9:17:B5:5C:27:B6:9B:64:CB:98:22:44:0D:CD:09:B8:89

  Issued: Aug 30 14:23:01 2001 GMT

  Expires: Aug 26 14:23:01 2016 GMT
- **GlobalSign_Root_CA_-_R3**
  Subject Name: /OU=GlobalSign Root CA - R3/O=GlobalSign/CN=GlobalSign

  Fingerprint: D6:9B:56:11:48:F0:1C:77:C5:45:78:C1:09:26:DF:5B:85:69:76:AD

  Issued: Mar 18 10:00:00 2009 GMT

  Expires: Mar 18 10:00:00 2029 GMT
- **Security_Communication_EV_RootCA1**
  Subject Name: /C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication EV RootCA1

  Fingerprint: FE:B8:C4:32:DC:F9:76:9A:CE:AE:3D:D8:90:8F:FD:28:86:65:64:7D

  Issued: Jun 6 02:12:32 2007 GMT

  Expires: Jun 6 02:12:32 2037 GMT
- **Microsec_e-Szigno_Root_CA_2009**
  Subject Name: /C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009/emailAddress=info@e-szigno.hu

  Fingerprint: 89:DF:74:FE:5C:F4:0F:4A:80:F9:E3:37:7D:54:DA:91:E1:01:31:8E

Issued: Jun 16 11:30:18 2009 GMT

Expires: Dec 30 11:30:18 2029 GMT

- **QuoVadis_Root_CA_3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 3

  Fingerprint: 1F:49:14:F7:D8:74:95:1D:DD:AE:02:C0:BE:FD:3A:2D:82:75:51:85

  Issued: Nov 24 19:11:23 2006 GMT

  Expires: Nov 24 19:06:44 2031 GMT
- **COMODO_RSA_Certification_Authority**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority

  Fingerprint: AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4

  Issued: Jan 19 00:00:00 2010 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **TC_TrustCenter_Class_3_CA_II**
  Subject Name: /C=DE/O=TC TrustCenter GmbH/OU=TC TrustCenter Class 3 CA/CN=TC TrustCenter Class 3 CA II

  Fingerprint: 80:25:EF:F4:6E:70:C8:D4:72:24:65:84:FE:40:3B:8A:8D:6A:DB:F5

  Issued: Jan 12 14:41:57 2006 GMT

  Expires: Dec 31 22:59:59 2025 GMT
- **T-TeleSec_GlobalRoot_Class_2**
  Subject Name: /C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 2

  Fingerprint: 59:0D:2D:7D:88:4F:40:2E:61:7E:A5:62:32:17:65:CF:17:D8:94:E9

  Issued: Oct 1 10:40:14 2008 GMT

  Expires: Oct 1 23:59:59 2033 GMT
- **CNNIC_ROOT**
  Subject Name: /C=CN/O=CNNIC/CN=CNNIC ROOT

  Fingerprint: 8B:AF:4C:9B:1D:F0:2A:92:F7:DA:12:8E:B9:1B:AC:F4:98:60:4B:6F

  Issued: Apr 16 07:09:14 2007 GMT

  Expires: Apr 16 07:09:14 2027 GMT
- **COMODO_ECC_Certification_Authority**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Certification Authority

  Fingerprint: 9F:74:4E:9F:2B:4D:BA:EC:0F:31:2C:50:B6:56:3B:8E:2D:93:C3:11

  Issued: Mar 6 00:00:00 2008 GMT

  Expires: Jan 18 23:59:59 2038 GMT

- **Trustis_FPS_Root_CA**
  Subject Name: /C=GB/O=Trustis Limited/OU=Trustis FPS Root CA

  Fingerprint: 3B:C0:38:0B:33:C3:F6:A6:0C:86:15:22:93:D9:DF:F5:4B:81:C0:04

  Issued: Dec 23 12:14:06 2003 GMT

  Expires: Jan 21 11:36:54 2024 GMT
- **Starfield_Services_Root_Certificate_Authority_-_G2**
  Subject Name: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services Root Certificate Authority - G2

  Fingerprint: 92:5A:8F:8D:2C:6D:04:E0:66:5F:59:6A:FF:22:D8:63:E8:25:6F:3F

  Issued: Sep 1 00:00:00 2009 GMT

  Expires: Dec 31 23:59:59 2037 GMT
- **Hellenic_Academic_and_Research_Institutions_RootCA_2011**
  Subject Name: /C=GR/O=Hellenic Academic and Research Institutions Cert. Authority/CN=Hellenic Academic and Research Institutions RootCA 2011

  Fingerprint: FE:45:65:9B:79:03:5B:98:A1:61:B5:51:2E:AC:DA:58:09:48:22:4D

  Issued: Dec 6 13:49:52 2011 GMT

  Expires: Dec 1 13:49:52 2031 GMT
- **RSA_Security_2048_v3**
  Subject Name: /O=RSA Security Inc/OU=RSA Security 2048 V3

  Fingerprint: 25:01:90:19:CF:FB:D9:99:1C:B7:68:25:74:8D:94:5F:30:93:95:42

  Issued: Feb 22 20:39:23 2001 GMT

  Expires: Feb 22 20:39:23 2026 GMT
- **DigiCert_Assured_ID_Root_G3**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root G3

  Fingerprint: F5:17:A2:4F:9A:48:C6:C9:F8:A2:00:26:9F:DC:0F:48:2C:AB:30:89

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT
- **NetLock_Arany_=Class_Gold=_FÅ‘tanÃºsÃtvÃ¡ny**
  Subject Name: /C=HU/L=Budapest/O=NetLock Kft./OU=TanxC3xBAsxC3xADtvxC3xA1nykiadxC3xB3k (Certification Services)/CN=NetLock Arany (Class Gold) FxC5x91tanxC3xBAsxC3xADtvxC3xA1ny

  Fingerprint: 06:08:3F:59:3F:15:A1:04:A0:69:A4:6B:A9:03:D0:06:B7:97:09:91

  Issued: Dec 11 15:08:21 2008 GMT

  Expires: Dec 6 15:08:21 2028 GMT
- **Sonera_Class_1_Root_CA**
  Subject Name: /C=FI/O=Sonera/CN=Sonera Class1 CA

  Fingerprint: 07:47:22:01:99:CE:74:B9:7C:B0:3D:79:B2:64:A2:C8:55:E9:33:FF

Issued: Apr 6 10:49:13 2001 GMT

Expires: Apr 6 10:49:13 2021 GMT

- **GeoTrust_Primary_Certification_Authority_-_G2**
  Subject Name: /C=US/O=GeoTrust Inc./OU=(c) 2007 GeoTrust Inc. - For authorized use only/CN=GeoTrust Primary Certification Authority - G2

  Fingerprint: 8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0

  Issued: Nov 5 00:00:00 2007 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **Entrust_Root_Certification_Authority_-_EC1**
  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: 20:D8:06:40:DF:9B:25:F5:12:25:3A:11:EA:F7:59:8A:EB:14:B5:47

  Issued: Dec 18 15:25:36 2012 GMT

  Issued: Dec 18 15:55:36 2037 GMT
- **Starfield_Class_2_CA**
  Subject Name: /C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority

  Fingerprint: AD:7E:1C:28:B0:64:EF:8F:60:03:40:20:14:C3:D0:E3:37:0E:B5:8A

  Issued: Jun 29 17:39:16 2004 GMT

  Expires: Jun 29 17:39:16 2034 GMT
- **Staat_der_Nederlanden_Root_CA_-_G2**
  Subject Name: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA - G2

  Fingerprint: 59:AF:82:79:91:86:C7:B4:75:07:CB:CF:03:57:46:EB:04:DD:B7:16

  Issued: Mar 26 11:18:17 2008 GMT

  Expires: Mar 25 11:03:10 2020 GMT
- **Entrust_Root_Certification_Authority_-_G2**
  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: 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4

  Issued: Jul 7 17:25:54 2009 GMT

  Expires: Dec 7 17:55:54 2030 GMT
- **Camerfirma_Global_Chambersign_Root**
  Subject Name: /C=EU/O=AC Camerfirma SA CIF A82743287/OU=http://www.chambersign.org/CN=Global Chambersign Root

  Fingerprint: 33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9

  Issued: Sep 30 16:14:18 2003 GMT

  Expires: Sep 30 16:14:18 2037 GMT

- **S-TRUST_Authentication_and_Encryption_Root_CA_2005_PN**
  Subject Name: /C=DE/ST=Baden-Wuerttemberg (BW)/L=Stuttgart/O=Deutscher Sparkassen Verlag GmbH/CN=S-TRUST Authentication and Encryption Root CA 2005:PN

  Fingerprint: BE:B5:A9:95:74:6B:9E:DF:73:8B:56:E6:DF:43:7A:77:BE:10:6B:81

  Issued: Jun 22 00:00:00 2005 GMT

  Expires: Jun 21 23:59:59 2030 GMT
- **NetLock_Business_=Class_B=_Root**
  Subject Name: /C=HU/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Uzleti (Class B) Tanusitvanykiado

  Fingerprint: 87:9F:4B:EE:05:DF:98:58:3B:E3:60:D6:33:E7:0D:3F:FE:98:71:AF

  Issued: Feb 25 14:10:22 1999 GMT

  Expires: Feb 20 14:10:22 2019 GMT
- **Baltimore_CyberTrust_Root**
  Subject Name: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root

  Fingerprint: D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74

  Issued: May 12 18:46:00 2000 GMT

  Expires: May 12 23:59:00 2025 GMT
- **Verisign_Class_1_Public_Primary_Certification_Authority_-_G3**
  Subject Name: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 1999 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 1 Public Primary Certification Authority - G3

  Fingerprint: 20:42:85:DC:F7:EB:76:41:95:57:8E:13:6B:D4:B7:D1:E9:8E:46:A5

  Issued: Oct 1 00:00:00 1999 GMT

  Expires: Jul 16 23:59:59 2036 GMT
- **ApplicationCA_-_Japanese_Government**
  Subject Name: /C=JP/O=Japanese Government/OU=ApplicationCA

  Fingerprint: 7F:8A:B0:CF:D0:51:87:6A:66:F3:36:0F:47:C8:8D:8C:D3:35:FC:74

  Issued: Dec 12 15:00:00 2007 GMT

  Expires: Dec 12 15:00:00 2017 GMT
- **TÃœRKTRUST_Elektronik_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±_H6**
  Subject Name: /C=TR/L=Ankara/O=TxC3x9CRKTRUST Bilgi xC4xB0letixC5x9Fim ve BilixC5x9Fim GxC3xBCvenlixC4x9Fi Hizmetleri A.xC5x9E./CN=TxC3x9CRKTRUST Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1 H6

  Fingerprint: 8A:5C:8C:EE:A5:03:E6:05:56:BA:D8:1B:D4:F6:C9:B0:ED:E5:2F:E0

  Issued: Dec 18 09:04:10 2013 GMT

  Expires: Dec 16 09:04:10 2023 GMT
- **CA_Disig_Root_R2**
  Subject Name: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig Root R2

  Fingerprint: B5:61:EB:EA:A4:DE:E4:25:4B:69:1A:98:A5:57:47:C2:34:C7:D9:71

Issued: Jul 19 09:15:30 2012 GMT

Expires: Jul 19 09:15:30 2042 GMT

- **Chambers_of_Commerce_Root_-_2008**
  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: 78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C

  Issued: Aug 1 12:29:50 2008 GMT

  Expires: Jul 31 12:29:50 2038 GMT
- **DigiCert_Assured_ID_Root_G2**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root G2

  Fingerprint: A1:4B:48:D9:43:EE:0A:0E:40:90:4F:3C:E0:A4:C0:91:93:51:5D:3F

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT
- **E-Tugra_Certification_Authority**
  Subject Name: /C=TR/L=Ankara/O=E-TuxC4x9Fra EBG BilixC5x9Fim Teknolojileri ve Hizmetleri A.xC5x9E./OU=E-Tugra Sertifikasyon Merkezi/CN=E-Tugra Certification Authority

  Fingerprint: 51:C6:E7:08:49:06:6E:F3:92:D4:5C:A0:0D:6D:A3:62:8F:C3:52:39

  Issued: Mar 5 12:09:48 2013 GMT

  Expires: Mar 3 12:09:48 2023 GMT
- **thawte_Primary_Root_CA_-_G2**
  Subject Name: /C=US/O=thawte, Inc./OU=(c) 2007 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA - G2

  Fingerprint: AA:DB:BC:22:23:8F:C4:01:A1:27:BB:38:DD:F4:1D:DB:08:9E:F0:12

  Issued: Nov 5 00:00:00 2007 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **WoSign**
  Subject Name: /C=CN/O=WoSign CA Limited/CN=Certification Authority of WoSign

  Fingerprint: B9:42:94:BF:91:EA:8F:B6:4B:E6:10:97:C7:FB:00:13:59:B6:76:CB

  Issued: Aug 8 01:00:01 2009 GMT

  Expires: Aug 8 01:00:01 2039 GMT
- **Equifax_Secure_Global_eBusiness_CA**
  Subject Name: /C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1

  Fingerprint: 7E:78:4A:10:1C:82:65:CC:2D:E1:F1:6D:47:B4:40:CA:D9:0A:19:45

  Issued: Jun 21 04:00:00 1999 GMT

  Expires: Jun 21 04:00:00 2020 GMT

- **Actalis_Authentication_Root_CA**
  Subject Name: /C=IT/L=Milan/O=Actalis S.p.A./03358520967/CN=Actalis Authentication Root CA

  Fingerprint: F3:73:B3:87:06:5A:28:84:8A:F2:F3:4A:CE:19:2B:DD:C7:8E:9C:AC

  Issued: Sep 22 11:22:02 2011 GMT

  Expires: Sep 22 11:22:02 2030 GMT
- **Camerfirma_Chambers_of_Commerce_Root**
  Subject Name: /C=EU/O=AC Camerfirma SA CIF A82743287/OU=http://www.chambersign.org/CN=Chambers of Commerce Root

  Fingerprint: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1

  Issued: Sep 30 16:13:43 2003 GMT

  Expires: Sep 30 16:13:44 2037 GMT
- **QuoVadis_Root_CA_1_G3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 1 G3

  Fingerprint: 1B:8E:EA:57:96:29:1A:C9:39:EA:B8:0A:81:1A:73:73:C0:93:79:67

  Issued: Jan 12 17:27:44 2012 GMT

  Expires: Jan 12 17:27:44 2042 GMT
- **Certum_Trusted_Network_CA**
  Subject Name: /C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Trusted Network CA

  Fingerprint: 07:E0:32:E0:20:B7:2C:3F:19:2F:06:28:A2:59:3A:19:A7:0F:06:9E

  Issued: Oct 22 12:07:37 2008 GMT

  Expires: Dec 31 12:07:37 2029 GMT
- **D-TRUST_Root_Class_3_CA_2_EV_2009**
  Subject Name: /C=DE/O=D-Trust GmbH/CN=D-TRUST Root Class 3 CA 2 EV 2009

  Fingerprint: 96:C9:1B:0B:95:B4:10:98:42:FA:D0:D8:22:79:FE:60:FA:B9:16:83

  Issued: Nov 5 08:50:46 2009 GMT

  Expires: Nov 5 08:50:46 2029 GMT
- **NetLock_Qualified_=Class_QA=_Root**
  Subject Name: /C=HU/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/emailAddress=info@netlock.hu

  Fingerprint: 01:68:97:E1:A0:B8:F2:C3:B1:34:66:5C:20:A7:27:B7:A1:58:E2:8F

  Issued: Mar 30 01:47:11 2003 GMT

  Expires: Dec 15 01:47:11 2022 GMT
- **StartCom_Certification_Authority_G2**
  Subject Name: /C=IL/O=StartCom Ltd./CN=StartCom Certification Authority G2

  Fingerprint: 31:F1:FD:68:22:63:20:EE:C6:3B:3F:9D:EA:4A:3E:53:7C:7C:39:17

  Issued: Jan 1 01:00:01 2010 GMT

Expires: Dec 31 23:59:01 2039 GMT

- **Buypass_Class_2_CA_1**
  Subject Name: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 CA 1

  Fingerprint: A0:A1:AB:90:C9:FC:84:7B:3B:12:61:E8:97:7D:5F:D3:22:61:D3:CC

  Issued: Oct 13 10:25:09 2006 GMT

  Expires: Oct 13 10:25:09 2016 GMT
- **CA_WoSign_ECC_Root**
  Subject Name: /C=CN/O=WoSign CA Limited/CN=CA WoSign ECC Root

  Fingerprint: D2:7A:D2:BE:ED:94:C0:A1:3C:C7:25:21:EA:5D:71:BE:81:19:F3:2B

  Issued: Nov 8 00:58:58 2014 GMT

  Expires: Nov 8 00:58:58 2044 GMT
- **XRamp_Global_CA_Root**
  Subject Name: /C=US/OU=www.xrampsecurity.com/O=XRamp Security Services Inc/CN=XRamp Global Certification Authority

  Fingerprint: B8:01:86:D1:EB:9C:86:A5:41:04:CF:30:54:F3:4C:52:B7:E5:58:C6

  Issued: Nov 1 17:14:04 2004 GMT

  Expires: Jan 1 05:37:19 2035 GMT
- **Swisscom_Root_CA_2**
  Subject Name: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root CA 2

  Fingerprint: 77:47:4F:C6:30:E4:0F:4C:47:64:3F:84:BA:B8:C6:95:4A:8A:41:EC

  Issued: Jun 24 08:38:14 2011 GMT

  Expires: Jun 25 07:38:14 2031 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_2**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

  Fingerprint: A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B

  Issued: Jan 29 00:00:00 1996 GMT

  Expires: Aug 2 23:59:59 2028 GMT
- **TWCA_Root_Certification_Authority**
  Subject Name: /C=TW/O=TAIWAN-CA/OU=Root CA/CN=TWCA Root Certification Authority

  Fingerprint: CF:9E:87:6D:D3:EB:FC:42:26:97:A3:B5:A3:7A:A0:76:A9:06:23:48

  Issued: Aug 28 07:24:33 2008 GMT

  Expires: Dec 31 15:59:59 2030 GMT
- **GeoTrust_Universal_CA**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Universal CA

  Fingerprint: E6:21:F3:35:43:79:05:9A:4B:68:30:9D:8A:2F:74:22:15:87:EC:79

  Issued: Mar 4 05:00:00 2004 GMT

Expires: Mar 4 05:00:00 2029 GMT

- **VeriSign_Universal_Root_Certification_Authority**
  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: 36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54

  Issued: Apr 2 00:00:00 2008 GMT

  Expires: Dec 1 23:59:59 2037 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_-_G2**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network

  Fingerprint: 85:37:1C:A6:E5:50:14:3D:CE:28:03:47:1B:DE:3A:09:E8:F8:77:0F

  Issued: May 18 00:00:00 1998 GMT

  Expires: Aug 1 23:59:59 2028 GMT
- **Buypass_Class_3_Root_CA**
  Subject Name: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 3 Root CA

  Fingerprint: DA:FA:F7:FA:66:84:EC:06:8F:14:50:BD:C7:C2:81:A5:BC:A9:64:57

  Issued: Oct 26 08:28:58 2010 GMT

  Expires: Oct 26 08:28:58 2040 GMT
- **GlobalSign_Root_CA**
  Subject Name: /C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA

  Fingerprint: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

  Issued: Sep 1 12:00:00 1998 GMT

  Expires: Jan 28 12:00:00 2028 GMT
- **Verisign_Class_2_Public_Primary_Certification_Authority_-_G3**
  Subject Name: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 1999 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 2 Public Primary Certification Authority - G3

  Fingerprint: 61:EF:43:D7:7F:CA:D4:61:51:BC:98:E0:C3:59:12:AF:9F:EB:63:11

  Issued: Oct 1 00:00:00 1999 GMT

  Expires: Jul 16 23:59:59 2036 GMT
- **PSCProcert**
  Subject Name: /emailAddress=contacto@procert.net.ve/L=Chacao/ST=Miranda/OU=Proveedor de Certificados PROCERT/O=Sistema Nacional de Certificacion Electronica/C=VE/CN=PSCProcert

  Fingerprint: 70:C1:8D:74:B4:28:81:0A:E4:FD:A5:75:D7:01:9F:99:B0:3D:50:74

  Issued: Dec 28 16:51:00 2010 GMT

  Expires: Dec 25 23:59:59 2020 GMT
- **QuoVadis_Root_CA_2**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2

Fingerprint: CA:3A:FB:CF:12:40:36:4B:44:B2:16:20:88:80:48:39:19:93:7C:F7

Issued: Nov 24 18:27:00 2006 GMT

Expires: Nov 24 18:23:33 2031 GMT

- **T-TeleSec_GlobalRoot_Class_3**
  Subject Name: /C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 3

  Fingerprint: 55:A6:72:3E:CB:F2:EC:CD:C3:23:74:70:19:9D:2A:BE:11:E3:81:D1

  Issued: Oct 1 10:29:56 2008 GMT

  Expires: Oct 1 23:59:59 2033 GMT
- **SwissSign_Platinum_CA_-_G2**
  Subject Name: /C=CH/O=SwissSign AG/CN=SwissSign Platinum CA - G2

  Fingerprint: 56:E0:FA:C0:3B:8F:18:23:55:18:E5:D3:11:CA:E8:C2:43:31:AB:66

  Issued: Oct 25 08:36:00 2006 GMT

  Expires: Oct 25 08:36:00 2036 GMT
- **Certum_Root_CA**
  Subject Name: /C=PL/O=Unizeto Sp. z o.o./CN=Certum CA

  Fingerprint: 62:52:DC:40:F7:11:43:A2:2F:DE:9E:F7:34:8E:06:42:51:B1:81:18

  Issued: Jun 11 10:46:39 2002 GMT

  Expires: Jun 11 10:46:39 2027 GMT
- **EBG_Elektronik_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±**
  Subject Name: /CN=EBG Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1/O=EBG BilixC5x9Fim Teknolojileri ve Hizmetleri A.xC5x9E./C=TR

  Fingerprint: 8C:96:BA:EB:DD:2B:07:07:48:EE:30:32:66:A0:F3:98:6E:7C:AE:58

  Issued: Aug 17 00:21:09 2006 GMT

  Expires: Aug 14 00:31:09 2016 GMT
- **Certigna**
  Subject Name: /C=FR/O=Dhimyotis/CN=Certigna

  Fingerprint: B1:2E:13:63:45:86:A4:6F:1A:B2:60:68:37:58:2D:C4:AC:FD:94:97

  Issued: Jun 29 15:13:05 2007 GMT

  Expires: Jun 29 15:13:05 2027 GMT
- **SecureTrust_CA**
  Subject Name: /C=US/O=SecureTrust Corporation/CN=SecureTrust CA

  Fingerprint: 87:82:C6:C3:04:35:3B:CF:D2:96:92:D2:59:3E:7D:44:D9:34:FF:11

  Issued: Nov 7 19:31:18 2006 GMT

  Expires: Dec 31 19:40:55 2029 GMT
- **SwissSign_Silver_CA_-_G2**
  Subject Name: /C=CH/O=SwissSign AG/CN=SwissSign Silver CA - G2

Fingerprint: 9B:AA:E5:9F:56:EE:21:CB:43:5A:BE:25:93:DF:A7:F0:40:D1:1D:CB

Issued: Oct 25 08:32:46 2006 GMT

Expires: Oct 25 08:32:46 2036 GMT

- **Taiwan_GRCA**
  Subject Name: /C=TW/O=Government Root Certification Authority

  Fingerprint: F4:8B:11:BF:DE:AB:BE:94:54:20:71:E6:41:DE:6B:BE:88:2B:40:B9

  Issued: Dec 5 13:23:33 2002 GMT

  Expires: Dec 5 13:23:33 2032 GMT
- **WellsSecure_Public_Root_Certificate_Authority**
  Subject Name: /C=US/O=Wells Fargo WellsSecure/OU=Wells Fargo Bank NA/CN=WellsSecure Public Root Certificate Authority

  Fingerprint: E7:B4:F6:9D:61:EC:90:69:DB:7E:90:A7:40:1A:3C:F4:7D:4F:E8:EE

  Issued: Dec 13 17:07:54 2007 GMT

  Expires: Dec 14 00:07:54 2022 GMT
- **AddTrust_Low-Value_Services_Root**
  Subject Name: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Class 1 CA Root

  Fingerprint: CC:AB:0E:A0:4C:23:01:D6:69:7B:DD:37:9F:CD:12:EB:24:E3:94:9D

  Issued: May 30 10:38:31 2000 GMT

  Expires: May 30 10:38:31 2020 GMT
- **DigiCert_High_Assurance_EV_Root_CA**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA

  Fingerprint: 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25

  Issued: Nov 10 00:00:00 2006 GMT

  Expires: Nov 10 00:00:00 2031 GMT
- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4**
  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: 22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A

  Issued: Nov 5 00:00:00 2007 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **Verisign_Class_1_Public_Primary_Certification_Authority_-_G2**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network

  Fingerprint: 27:3E:E1:24:57:FD:C4:F9:0C:55:E8:2B:56:16:7F:62:F5:32:E5:47

  Issued: May 18 00:00:00 1998 GMT

  Expires: Aug 1 23:59:59 2028 GMT

- **CFCA_EV_ROOT**
  Subject Name: /C=CN/O=China Financial Certification Authority/CN=CFCA EV ROOT

  Fingerprint: E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83

  Issued: Aug 8 03:07:01 2012 GMT

  Expires: Dec 31 03:07:01 2029 GMT
- **TWCA_Global_Root_CA**
  Subject Name: /C=TW/O=TAIWAN-CA/OU=Root CA/CN=TWCA Global Root CA

  Fingerprint: 9C:BB:48:53:F6:A4:F6:D3:52:A4:E8:32:52:55:60:13:F5:AD:AF:65

  Issued: Jun 27 06:28:33 2012 GMT

  Expires: Dec 31 15:59:59 2030 GMT
- **SecureSign_RootCA11**
  Subject Name: /C=JP/O=Japan Certification Services, Inc./CN=SecureSign RootCA11

  Fingerprint: 3B:C4:9F:48:F8:F3:73:A0:9C:1E:BD:F8:5B:B1:C3:65:C7:D8:11:B3

  Issued: Apr 8 04:56:47 2009 GMT

  Expires: Apr 8 04:56:47 2029 GMT
- **GeoTrust_Primary_Certification_Authority**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Primary Certification Authority

  Fingerprint: 32:3C:11:8E:1B:F7:B8:B6:52:54:E2:E2:10:0D:D6:02:90:37:F0:96

  Issued: Nov 27 00:00:00 2006 GMT

  Expires: Jul 16 23:59:59 2036 GMT
- **Equifax_Secure_CA**
  Subject Name: /C=US/O=Equifax/OU=Equifax Secure Certificate Authority

  Fingerprint: D2:32:09:AD:23:D3:14:23:21:74:E4:0D:7F:9D:62:13:97:86:63:3A

  Issued: Aug 22 16:41:51 1998 GMT

  Expires: Aug 22 16:41:51 2018 GMT
- **Entrust_Root_Certification_Authority**
  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: B3:1E:B1:B7:40:E3:6C:84:02:DA:DC:37:D4:4D:F5:D4:67:49:52:F9

  Issued: Nov 27 20:23:42 2006 GMT

  Expires: Nov 27 20:53:42 2026 GMT
- **Network_Solutions_Certificate_Authority**
  Subject Name: /C=US/O=Network Solutions L.L.C./CN=Network Solutions Certificate Authority

  Fingerprint: 74:F8:A3:C3:EF:E7:B3:90:06:4B:83:90:3C:21:64:60:20:E5:DF:CE

  Issued: Dec 1 00:00:00 2006 GMT

  Expires: Dec 31 23:59:59 2029 GMT

- **QuoVadis_Root_CA_3_G3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 3 G3

  Fingerprint: 48:12:BD:92:3C:A8:C4:39:06:E7:30:6D:27:96:E6:A4:CF:22:2E:7D

  Expires: Jan 12 20:26:32 2012 GMT

  Issued: Jan 12 20:26:32 2042 GMT
- **Security_Communication_Root_CA**
  Subject Name: /C=JP/O=SECOM Trust.net/OU=Security Communication RootCA1

  Fingerprint: 36:B1:2B:49:F9:81:9E:D7:4C:9E:BC:38:0F:C6:56:8F:5D:AC:B2:F7

  Issued: Sep 30 04:20:49 2003 GMT

  Expires: Sep 30 04:20:49 2023 GMT
- **Starfield_Root_Certificate_Authority_-_G2**
  Subject Name: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Root Certificate Authority - G2

  Fingerprint: B5:1C:06:7C:EE:2B:0C:3D:F8:55:AB:2D:92:F4:FE:39:D4:E7:0F:0E

  Issued: Sep 1 00:00:00 2009 GMT

  Expires: Dec 31 23:59:59 2037 GMT
- **Cybertrust_Global_Root**
  Subject Name: /O=Cybertrust, Inc/CN=Cybertrust Global Root

  Fingerprint: 5F:43:E5:B1:BF:F8:78:8C:AC:1C:C7:CA:4A:9A:C6:22:2B:CC:34:C6

  Issued: Dec 15 08:00:00 2006 GMT

  Expires: Dec 15 08:00:00 2021 GMT
- **Global_Chambersign_Root_-_2008**
  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: 4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C

  Issued: Aug 1 12:31:40 2008 GMT

  Expires: Jul 31 12:31:40 2038 GMT
- **Comodo_Trusted_Services_root**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=Trusted Certificate Services

  Fingerprint: E1:9F:E3:0E:8B:84:60:9E:80:9B:17:0D:72:A8:C5:BA:6E:14:09:BD

  Issued: Jan 1 00:00:00 2004 GMT

  Expires: Dec 31 23:59:59 2028 GMT
- **Secure_Global_CA**
  Subject Name: /C=US/O=SecureTrust Corporation/CN=Secure Global CA

  Fingerprint: 3A:44:73:5A:E5:81:90:1F:24:86:61:46:1E:3B:9C:C4:5F:F5:3A:1B

  Issued: Nov 7 19:42:28 2006 GMT

Expires: Dec 31 19:52:06 2029 GMT

- **SwissSign_Gold_CA_-_G2**
  Subject Name: /C=CH/O=SwissSign AG/CN=SwissSign Gold CA - G2

  Fingerprint: D8:C5:38:8A:B7:30:1B:1B:6E:D4:7A:E6:45:25:3A:6F:9F:1A:27:61

  Issued: Oct 25 08:30:35 2006 GMT

  Expires: Oct 25 08:30:35 2036 GMT
- **NetLock_Express_=Class_C=_Root**
  Subject Name: /C=HU/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Expressz (Class C) Tanusitvanykiado

  Fingerprint: E3:92:51:2F:0A:CF:F5:05:DF:F6:DE:06:7F:75:37:E1:65:EA:57:4B

  Issued: Feb 25 14:08:11 1999 GMT

  Expires: Feb 20 14:08:11 2019 GMT
- **GlobalSign_ECC_Root_CA_-_R5**
  Subject Name: /OU=GlobalSign ECC Root CA - R5/O=GlobalSign/CN=GlobalSign

  Fingerprint: 1F:24:C6:30:CD:A4:18:EF:20:69:FF:AD:4F:DD:5F:46:3A:1B:69:AA

  Issued: Nov 13 00:00:00 2012 GMT

  Expires: Jan 19 03:14:07 2038 GMT
- **Atos_TrustedRoot_2011**
  Subject Name: /CN=Atos TrustedRoot 2011/O=Atos/C=DE

  Fingerprint: 2B:B1:F5:3E:55:0C:1D:C5:F1:D4:E6:B7:6A:46:4B:55:06:02:AC:21

  Issued: Jul 7 14:58:30 2011 GMT

  Expires: Dec 31 23:59:59 2030 GMT
- **Root_CA_Generalitat_Valenciana**
  Subject Name: /C=ES/O=Generalitat Valenciana/OU=PKIGVA/CN=Root CA Generalitat Valenciana

  Fingerprint: A0:73:E5:C5:BD:43:61:0D:86:4C:21:13:0A:85:58:57:CC:9C:EA:46

  Issued: Jul 6 16:22:47 2001 GMT

  Expires: Jul 1 15:22:47 2021 GMT
- **Hongkong_Post_Root_CA_1**
  Subject Name: /C=HK/O=Hongkong Post/CN=Hongkong Post Root CA 1

  Fingerprint: D6:DA:A8:20:8D:09:D2:15:4D:24:B5:2F:CB:34:6E:B2:58:B2:8A:58

  Issued: May 15 05:13:14 2003 GMT

  Expires: May 15 04:52:29 2023 GMT
- **Security_Communication_RootCA2**
  Subject Name: /C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication RootCA2

  Fingerprint: 5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74

  Issued: May 29 05:00:39 2009 GMT

Expires: May 29 05:00:39 2029 GMT

- **QuoVadis_Root_CA_2_G3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2 G3

  Fingerprint: 09:3C:61:F3:8B:8B:DC:7D:55:DF:75:38:02:05:00:E1:25:F5:C8:36

  Issued: Jan 12 18:59:32 2012 GMT

  Expires: Jan 12 18:59:32 2042 GMT
- **OISTE_WISeKey_Global_Root_GA_CA**
  Subject Name: /C=CH/O=WISeKey/OU=Copyright (c) 2005/OU=OISTE Foundation Endorsed/CN=OISTE WISeKey Global Root GA CA

  Fingerprint: 59:22:A1:E1:5A:EA:16:35:21:F8:98:39:6A:46:46:B0:44:1B:0F:A9

  Issued: Dec 11 16:03:44 2005 GMT

  Expires: Dec 11 16:09:51 2037 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

  Fingerprint: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2

  Issued: Jan 29 00:00:00 1996 GMT

  Expires: Aug 1 23:59:59 2028 GMT
- **Microsec_e-Szigno_Root_CA**
  Subject Name: /C=HU/L=Budapest/O=Microsec Ltd./OU=e-Szigno CA/CN=Microsec e-Szigno Root CA

  Fingerprint: 23:88:C9:D3:71:CC:9E:96:3D:FF:7D:3C:A7:CE:FC:D6:25:EC:19:0D

  Issued: Apr 6 12:28:44 2005 GMT

  Expires: Apr 6 12:28:44 2017 GMT
- **Izenpe.com**
  Subject Name: /C=ES/O=IZENPE S.A./CN=Izenpe.com

  Fingerprint: 2F:78:3D:25:52:18:A7:4A:65:39:71:B5:2C:A2:9C:45:15:6F:E9:19

  Issued: Dec 13 13:08:28 2007 GMT

  Expires: Dec 13 08:27:25 2037 GMT
- **Buypass_Class_2_Root_CA**
  Subject Name: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 Root CA

  Fingerprint: 49:0A:75:74:DE:87:0A:47:FE:58:EE:F6:C7:6B:EB:C6:0B:12:40:99

  Issued: Oct 26 08:38:03 2010 GMT

  Expires: Oct 26 08:38:03 2040 GMT
- **GeoTrust_Global_CA**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

  Fingerprint: DE:28:F4:A4:FF:E5:B9:2F:A3:C5:03:D1:A3:49:A7:F9:96:2A:82:12

  Issued: May 21 04:00:00 2002 GMT

Expires: May 21 04:00:00 2022 GMT

- **GlobalSign_Root_CA_-_R2**
  Subject Name: /OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign

  Fingerprint: 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE

  Issued: Dec 15 08:00:00 2006 GMT

  Expires: Dec 15 08:00:00 2021 GMT
- **Certification_Authority_of_WoSign_G2**
  Subject Name: /C=CN/O=WoSign CA Limited/CN=Certification Authority of WoSign G2

  Fingerprint: FB:ED:DC:90:65:B7:27:20:37:BC:55:0C:9C:56:DE:BB:F2:78:94:E1

  Issued: Nov 8 00:58:58 2014 GMT

  Expires: Nov 8 00:58:58 2044 GMT
- **Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068**
  Subject Name: /C=ES/CN=Autoridad de Certificacion Firmaprofesional CIF A62634068

  Fingerprint: AE:C5:FB:3F:C8:E1:BF:C4:E5:4F:03:07:5A:9A:E8:00:B7:F7:B6:FA

  Issued: May 20 08:38:15 2009 GMT

  Expires: Dec 31 08:38:15 2030 GMT
- **EC-ACC**
  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: 28:90:3A:63:5B:52:80:FA:E6:77:4C:0B:6D:A7:D6:BA:A6:4A:F2:E8

  Issued: Jan 7 23:00:00 2003 GMT

  Expires: Jan 7 22:59:59 2031 GMT
- **USERTrust_ECC_Certification_Authority**
  Subject Name: /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust ECC Certification Authority

  Fingerprint: D1:CB:CA:5D:B2:D5:2A:7F:69:3B:67:4D:E5:F0:5A:1D:0C:95:7D:F0

  Issued: Feb 1 00:00:00 2010 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **Swisscom_Root_EV_CA_2**
  Subject Name: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root EV CA 2

  Fingerprint: E7:A1:90:29:D3:D5:52:DC:0D:0F:C6:92:D3:EA:88:0D:15:2E:1A:6B

  Issued: Jun 24 09:45:08 2011 GMT

  Expires: Jun 25 08:45:08 2031 GMT
- **CA_Disig**
  Subject Name: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig

  Fingerprint: 2A:C8:D5:8B:57:CE:BF:2F:49:AF:F2:FC:76:8F:51:14:62:90:7A:41

Issued: Mar 22 01:39:34 2006 GMT

Expires: Mar 22 01:39:34 2016 GMT

- **ePKI_Root_Certification_Authority**
  Subject Name: /C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certification Authority

  Fingerprint: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0

  Issued: Dec 20 02:31:27 2004 GMT

  Expires: Dec 20 02:31:27 2034 GMT
- **GeoTrust_Global_CA_2**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA 2

  Fingerprint: A9:E9:78:08:14:37:58:88:F2:05:19:B0:6D:2B:0D:2B:60:16:90:7D

  Issued: Mar 4 05:00:00 2004 GMT

  Expires: Mar 4 05:00:00 2019 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_-_G3**
  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: 13:2D:0D:45:53:4B:69:97:CD:B2:D5:C3:39:E2:55:76:60:9B:5C:C6

  Issued: Oct 1 00:00:00 1999 GMT

  Expires: Jul 16 23:59:59 2036 GMT

Section 6.7.3

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.

CONTENTS

- Section 6.7.3.1, “Viewing a List of CA Certificates Added to the Trusted Certificate Store”
- Section 6.7.3.2, “Adding a CA Certificate to the Trusted Certificate Store”
- Section 6.7.3.3, “Deleting a CA Certificate from the Trusted Certificate Store”

Section 6.7.3.1

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 Section 6.7.3.2, "Adding a CA Certificate to the Trusted Certificate Store".

Section 6.7.3.2
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 certificate
   ```

   Where *certificate* is the chosen CA certificate.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.7.3.3
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 static VLAN by typing:

   ```
   no admin system-ca-certificates configured-cas certificate
   ```

   Where *certificate* is the chosen CA certificate.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.7.4
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.

CONTENTS

- Section 6.7.4.1, "Viewing a List of CA Certificates and CRLs"
- Section 6.7.4.2, "Viewing the Status of a CA Certificate and CRL"
- Section 6.7.4.3, "Adding a CA Certificate and CRL"
- Section 6.7.4.4, "Deleting a CA Certificate and CRL"

Section 6.7.4.1
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
 "{--contents--}" ! ! !
```

If no certificates have been configured, add certificates as needed. For more information, refer to Section 6.7.4.3, "Adding a CA Certificate and CRL".

Section 6.7.4.2
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-certificate-status
```

Where:

- *certificate* is the name of the certificate

This 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-certificate-status
```

Where:

- *certificate* is the name of the certificate

This 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

Parameter	Description
	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

This 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 certificate must be updated by this date and time.

Section 6.7.4.3
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-certificate 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, or type **revert** and press **Enter** to abort.

Section 6.7.4.4
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, or type **revert** and press **Enter** to abort.

Section 6.7.5
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.

CONTENTS

- Section 6.7.5.1, “Viewing a List of Private Keys”
- Section 6.7.5.2, “Adding a Private Key”

- Section 6.7.5.3, "Deleting a Private Key"

Section 6.7.5.1
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 Section 6.7.5.2, "Adding a Private Key".

Section 6.7.5.2
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.

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 } The type of key. This parameter is mandatory.
contents { contents }	**Synopsis:** A string 1 to 8192 characters long

Parameter	Description
	The contents of the unsigned private key. This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.7.5.3
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, or type **revert** and press **Enter** to abort.

Section 6.7.6
Managing Public Keys

This section describes how to manage public keys on the device.

CONTENTS

- Section 6.7.6.1, "Viewing a List of Public Keys"
- Section 6.7.6.2, "Adding a Public Key"
- Section 6.7.6.3, "Adding an IPSec-Formatted Public Key"
- Section 6.7.6.4, "Deleting a Public Key"

Section 6.7.6.1
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 Section 6.7.6.2, "Adding a Public Key".

Section 6.7.6.2
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 Section 6.7.5.2, "Adding a Private Key".
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.*

Parameter	Description
algorithm { algorithm }	**Synopsis:** { rsa, dsa, ssh-rsa } The algorithm of the key. This parameter is mandatory.
contents { contents }	**Synopsis:** A string 1 to 8192 characters long The contents of the key. This parameter is mandatory.
private-key-name { private-key-name }	**Synopsis:** A string The private key name associated with this public key.

6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.7.6.3
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 Section 6.7.6.2, "Adding a Public Key".
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-formatted-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, or type **`revert`** and press **Enter** to abort.

Section 6.7.6.4
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, or type **`revert`** and press **Enter** to abort.

Section 6.7.7
Managing Certificates

This section describes how to manage certificates on the device.

CONTENTS

- Section 6.7.7.1, "Viewing a List of Certificates"
- Section 6.7.7.2, "Viewing the Status of a Certificate"
- Section 6.7.7.3, "Adding a Certificate"

- Section 6.7.7.4, "Deleting a Certificate"

Section 6.7.7.1
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 Section 6.7.7.3, "Adding a Certificate".

Section 6.7.7.2
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.localdomain
 subject    /C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=localhost.localdomain
 not before 2017-01-06T18:45:49-00:00
 not after  2037-01-03T18:45:49-00:00
```

This 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.

Section 6.7.7.3
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 Section 6.7.4.3, "Adding a CA Certificate and CRL"
   - For more information about adding private keys, refer to Section 6.7.5.2, "Adding a Private Key"
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 1 to 8192 characters long The contents of the certificate. This parameter is mandatory.
private-key-name { private-key-name }	**Synopsis:** A string The private key associated with this certificate.
ca-name { ca-name }	**Synopsis:** A string The optional CA certificate for this certificate.

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.7.7.4
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, or type **revert** and press **Enter** to abort.

Section 6.7.8
Managing Known Hosts

RUGGEDCOM ROX II maintains a Known Hosts list for defining each SSH (SCP) server the device pulls updates or files from. Servers are identified by their host name or IP address. Users can further define a specific port on the server designated for SSH communications and/or an SSH/RSA public key.

Servers can also be enabled or disabled.

CONTENTS

- Section 6.7.8.1, “Viewing a List of Known Hosts”
- Section 6.7.8.2, “Adding a Known Host”
- Section 6.7.8.3, “Deleting a Known Host”

Section 6.7.8.1
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 Section 6.7.8.2, “Adding a Known Host”.

Section 6.7.8.2
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 Section 6.7.6, “Managing Public Keys”.
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
   enabled
   ```

   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, or type **revert** and press **Enter** to abort.

Section 6.7.8.3
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, or type **revert** and press **Enter** to abort.

Section 6.8
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:

a. A rule for the TCP and UDP protocols is applied.

b. The router sees both TCP and UDP traffic that qualifies for NAT.

c. The rule is then modified to allow only UDP.

d. 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 Section 6.8.1, "Firewall Concepts".

CONTENTS

- Section 6.8.1, "Firewall Concepts"
- Section 6.8.2, "Viewing a List of Firewalls"
- Section 6.8.3, "Adding a Firewall"
- Section 6.8.4, "Deleting a Firewall"
- Section 6.8.5, "Working with Multiple Firewall Configurations"
- Section 6.8.6, "Configuring the Firewall for a VPN"
- Section 6.8.7, "Configuring the Firewall for a VPN in a DMZ"
- Section 6.8.8, "Configuring Netfilter"
- Section 6.8.9, "Managing Zones"
- Section 6.8.10, "Managing Interfaces"
- Section 6.8.11, "Managing Hosts"
- Section 6.8.12, "Managing Policies"
- Section 6.8.13, "Managing Network Address Translation Settings"
- Section 6.8.14, "Managing Masquerade and SNAT Settings"
- Section 6.8.15, "Managing Rules"
- Section 6.8.16, "Validating a Firewall Configuration"
- Section 6.8.17, "Enabling/Disabling a Firewall"

Section 6.8.1

Firewall Concepts

This section describes some of the concepts important to the implementation of firewalls in RUGGEDCOM ROX II.

CONTENTS

- Section 6.8.1.1, "Stateless vs. Stateful Firewalls"
- Section 6.8.1.2, "Linux netfilter"
- Section 6.8.1.3, "Network Address Translation"
- Section 6.8.1.4, "Port Forwarding"
- Section 6.8.1.5, "Protecting Against a SYN Flood Attack"
- Section 6.8.1.6, "Protecting Against IP Spoofing"

Section 6.8.1.1

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.

Section 6.8.1.2
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.

Section 6.8.1.3
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: 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.

Section 6.8.1.4
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.

Section 6.8.1.5
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.

Section 6.8.1.6
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 Section 6.8.10.2, "Adding an Interface".

Section 6.8.2
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 Section 6.8.3, "Adding a Firewall".

Section 6.8.3
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 Section 6.8.10.2, "Adding an Interface".
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 Section 6.8.9.2, "Adding a Zone".
6. Associate an interface with each zone. For more information about associating interfaces with zones, refer to Section 6.8.10.3, "Associating an Interface with a Zone".
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 Section 6.8.12, "Managing Policies".
8. Configure the network address translation (NAT), masquerading or static network address translation (SNAT) settings. For more information about configuring NAT settings, refer to Section 6.8.13, "Managing Network Address Translation Settings". For more information about configuring masquerading and/or SNAT settings, refer to Section 6.8.14, "Managing Masquerade and SNAT Settings".

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 Section 6.8.11, "Managing Hosts".
10. If required, configure rules that override the default policies. For more information about configuring rules, refer to Section 6.8.15, "Managing Rules".
11. If required, configure support for a VPN. For more information, refer to:
    - Section 6.8.6, "Configuring the Firewall for a VPN"
    - Section 6.8.7, "Configuring the Firewall for a VPN in a DMZ"
12. Validate the configuration. For more information about validating a firewall configuration, refer to Section 6.8.16, "Validating a Firewall Configuration".
13. Enable the firewall. For more information, refer to Section 6.8.17, "Enabling/Disabling a Firewall".
14. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.8.4
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, or type **revert** and press **Enter** to abort.

Section 6.8.5
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, or type **revert** and press **Enter** to abort.

Section 6.8.6

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 Section 6.8.3, "Adding a Firewall".
2. Make sure zones for local, network and VPN traffic have been configured. For more information about managing zones, refer to Section 6.8.9, "Managing Zones".
3. Make sure a zone called *Any* exists and is of the type IPsec . For more information about managing zones, refer to Section 6.8.9, "Managing Zones".
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 Section 6.8.10.3, "Associating an Interface with a Zone".
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 Section 6.8.11, "Managing Hosts".
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 Section 6.8.11, "Managing Hosts".

   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 Section 6.8.15, "Managing Rules".
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 Section 6.8.15, "Managing Rules".

Section 6.8.7
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), 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 Section 6.8.3, "Adding a Firewall".
2. Make sure a zone called *dmz* exists. For more information about managing zones, refer to Section 6.8.9, "Managing Zones".
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 Section 6.8.15, "Managing Rules".

Section 6.8.8
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, or type **revert** and press **Enter** to abort.

Section 6.8.9
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.

CONTENTS

- Section 6.8.9.1, “Viewing a List of Zones”
- Section 6.8.9.2, “Adding a Zone”
- Section 6.8.9.3, “Deleting a Zone”

Section 6.8.9.1
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 Section 6.8.9.2, "Adding a Zone".

Section 6.8.9.2
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.
type46 { type46 }	**Synopsis:** { ip, ipsec, firewall } **Default:** ip Zone types applying to both IPv4 and IPv6: plain IP, firewall, or IPSec
type6 { type6 }	**Synopsis:** { ipv6, ipsec, firewall } **Default:** ipv6 Zone types are plain IPv6, firewall, or IPSec
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, or type **revert** and press **Enter** to abort.

Section 6.8.9.3
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, or type **revert** and press **Enter** to abort.

Section 6.8.10

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.

Table: Example

Interface	Zone
Switch.0001	Loc
Switch.0002	Loc
Switch.0003	Any
Switch.0004	DMZ
W1ppp	net

CONTENTS

- Section 6.8.10.1, “Viewing a List of Interfaces”
- Section 6.8.10.2, “Adding an Interface”
- Section 6.8.10.3, “Associating an Interface with a Zone”
- Section 6.8.10.4, “Configuring a Broadcast Address”
- Section 6.8.10.5, “Deleting an Interface”

Section 6.8.10.1

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 Section 6.8.10.2, "Adding an Interface".

Section 6.8.10.2
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

Parameter	Description
arp_filter	IPv4 ONLY- See additional info. Responds only to ARP requests for configured IP addresses (This is permanently enabled system wide since ROX 2.3.0, and this option no longer has any effect).
routeback	IPv4 and IPv6 - Interface traffic routed back out that same interface.
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.
norfc1918	Not currently implemented
routefilter	IPv4 and IPv6 - Enables /rpfilter/ spoofing protection

Parameter	Description
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 Section 6.8.10.3, "Associating an Interface with a Zone".
7. Configure a broadcast address for the interface. For more information configuring a broadcast address, refer to Section 6.8.10.4, "Configuring a Broadcast Address".
8. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.10.3
Associating an Interface with a Zone

To associate an interface with a pre-defined 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 the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	**Synopsis:** A string A pre-defined zone
undefined-zone	This is used in conjunction with hosts definitions.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.10.4
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 the following parameter(s) as required:

Parameter	Description
ipv4-address { ipv4-address }	**Synopsis:** A string An IPv4 address for a broadcast address.
detect	Automatic detection of the broadcast address(es).

Parameter	Description
none	The default.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.8.10.5
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, or type **revert** and press **Enter** to abort.

Section 6.8.11
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.

Table: Example

Zone	Interface	IP Address or Network
Local	Switch.0003	10.0.0.0/8
Guests	Switch.0003	192.168.0.0/24

CONTENTS

- Section 6.8.11.1, “Viewing a List of Hosts”
- Section 6.8.11.2, “Adding a Host”
- Section 6.8.11.3, “Deleting a Host”

Section 6.8.11.1
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 Section 6.8.11.2, "Adding a Host".

Section 6.8.11.2

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	**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 A pre-defined zone This parameter is mandatory.
interface { interface }	**Synopsis:** A string A pre-defined interface to which optional IPs and/or networks can be added. This parameter is mandatory.
ipaddress { ipaddress }	**Synopsis:** A string

Parameter	Description
	Additional IP addresses or networks - comma separated, or a range in the form of low.address-high.address
description { description }	**Synopsis:** A string (Optional) The description string for this host.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.8.11.3
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, or type **revert** and press **Enter** to abort.

Section 6.8.12
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 Section 6.8.9, "Managing Zones".

NOTE
Policies for specific hosts or types of traffic can be overridden by rules. For more information about rules, refer to Section 6.8.15, "Managing Rules".

CONTENTS

- Section 6.8.12.1, "Viewing a List of Policies"
- Section 6.8.12.2, "Adding a Policy"
- Section 6.8.12.3, "Configuring the Source Zone"
- Section 6.8.12.4, "Configuring the Destination Zone"
- Section 6.8.12.5, "Deleting a Policy"

Section 6.8.12.1
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 Section 6.8.12.2, "Adding a Policy".

Section 6.8.12.2
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 policy
   ```

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-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.
description { description }	**Synopsis:** A string (Optional) The description string for this policy.

4. Configure the source zone for the policy. For more information, refer to Section 6.8.12.3, "Configuring the Source Zone".
5. Configure the destination zone for the policy. For more information, refer to Section 6.8.12.4, "Configuring the Destination Zone".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.12.3
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 the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	**Synopsis:** A string
all	

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.12.4
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. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	**Synopsis:** A string
all	

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.12.5
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, or type **`revert`** and press **Enter** to abort.

Section 6.8.13
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 Section 6.8.15, "Managing Rules".

CONTENTS

- Section 6.8.13.1, "Viewing a List of NAT Settings"
- Section 6.8.13.2, "Adding a NAT Setting"
- Section 6.8.13.3, "Deleting a NAT Setting"

Section 6.8.13.1
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 Section 6.8.13.2, “Adding a NAT Setting”.

Section 6.8.13.2

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. This parameter is mandatory.
interface { interface }	**Synopsis:** A string An interface that has an external IP address. This parameter is mandatory.
ipalias	Create IP Alias for NAT rule.

Parameter	Description
internal-addr { internal-addr }	**Synopsis:** A string The internal IP address. The address must not be a DNS Name. This parameter is mandatory.
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, or type **`revert`** and press **Enter** to abort.

Section 6.8.13.3
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, or type **`revert`** and press **Enter** to abort.

Section 6.8.14
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.

CONTENTS

- Section 6.8.14.1, “Viewing a List of Masquerade and SNAT Settings”
- Section 6.8.14.2, “Adding Masquerade or SNAT Settings”
- Section 6.8.14.3, “Deleting a Masquerade or SNAT Setting”

Section 6.8.14.1
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 Section 6.8.14.2, "Adding Masquerade or SNAT Settings".

Section 6.8.14.2

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

Parameter	Description
	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. This parameter is mandatory.
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) This parameter is mandatory.
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, or type **`revert`** and press **Enter** to abort.

Section 6.8.14.3
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, or type **`revert`** and press **Enter** to abort.

Section 6.8.15
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.

CONTENTS

- Section 6.8.15.1, "Viewing a List of Rules"

- Section 6.8.15.2, "Adding a Rule"
- Section 6.8.15.3, "Configuring the Source Zone"
- Section 6.8.15.4, "Configuring the Destination Zone"
- Section 6.8.15.5, "Deleting a Rule"

Section 6.8.15.1
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 Section 6.8.15.2, "Adding a Rule".

Section 6.8.15.2
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:

a. A rule for the TCP and UDP protocols is applied.

b. The router sees both TCP and UDP traffic that qualifies for NAT.

c. The rule is then modified to allow only UDP.

d. 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. • 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:** { tcp, udp, icmp, all } or a string **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
original-destination { original-destination }	**Synopsis:** { None } or a string

Parameter	Description
	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. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.15.3
Configuring the Source Zone

To configure the source 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} » source-zone***, where *{firewall}* is the name of the firewall and *{rule}* is the name of the rule.
3. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	**Synopsis:** A string A predefined zone
other { other }	**Synopsis:** A string Type a custom definition - this can be a comma-separated list of zones.
all	All zones

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 6.8.15.4
Configuring the Destination Zone

To configure the destination zone for a firewall rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	**Synopsis:** A string A pre-defined zone
other { other }	**Synopsis:** A string An undefined zone (string).
all	All zones

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 6.8.15.5
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, or type **revert** and press **Enter** to abort.

Section 6.8.16
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.

Section 6.8.17
Enabling/Disabling a Firewall

To enable or disable the firewall, do the following:

IMPORTANT!
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, or type **revert** and press **Enter** to abort.

Section 6.9

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.

CAUTION!
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.

IMPORTANT!
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 Chapter 6, Security.

```
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 Chapter 6, *Security*.

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 Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".

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 Section 6.8.3, "Adding a Firewall".

IP Address Assignment

This chapter describes features related to the assignment of IP addresses, such as DHCP and DNS.

CONTENTS

- Section 7.1, "Managing IP Addresses for Routable Interfaces"
- Section 7.2, "Managing the DHCP Relay Agent"
- Section 7.3, "Managing the DHCP Server"
- Section 7.4, "Managing Static DNS"
- Section 7.5, "Managing Dynamic DNS"

Section 7.1

Managing IP Addresses for Routable Interfaces

This section describes how to manage IP address for routable interfaces.

CONTENTS

- Section 7.1.1, "Configuring Costing for Routable Interfaces"
- Section 7.1.2, "Viewing Statistics for Routable Interfaces"
- Section 7.1.3, "Managing IPv4 Addresses"
- Section 7.1.4, "Managing IPv6 Addresses"
- Section 7.1.5, "Configuring IPv6 Neighbor Discovery"
- Section 7.1.6, "Managing IPv6 Network Prefixes"

Section 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, or type **revert** and press **Enter** to abort.

Section 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
.
.
.
```

This 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. This parameter is mandatory.
state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down. This parameter is mandatory.
pointopoint	**Synopsis:** { true, false } The point-to-point link. This parameter is mandatory.
bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes received. This parameter is mandatory.
packets	**Synopsis:** A 64-bit unsigned integer The number of packets received. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of error packets received.

Parameter	Description
	This parameter is mandatory.
dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the receiving device. This parameter is mandatory.
bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes transmitted. This parameter is mandatory.
packets	**Synopsis:** A 64-bit unsigned integer The number of packets transmitted. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of error packets transmitted. This parameter is mandatory.
dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the transmitting device. This parameter is mandatory.
collisions	**Synopsis:** A 32-bit unsigned integer The number of collisions detected on the port. This parameter is mandatory.

Section 7.1.3
Managing IPv4 Addresses

This section describes how to manage IPv4 addresses for a routable interface.

CONTENTS

- Section 7.1.3.1, “Viewing a List of IPv4 Addresses”
- Section 7.1.3.2, “Adding an IPv4 Address”
- Section 7.1.3.3, “Deleting an IPv4 Address”

Section 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 Section 7.1.3.2, "Adding an IPv4 Address".

Section 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 7.1.4
Managing IPv6 Addresses

This section describes how to manage IPv6 addresses for a routable interface.

CONTENTS

- Section 7.1.4.1, "Viewing a List of IPv6 Addresses"
- Section 7.1.4.2, "Adding an IPv6 Address"
- Section 7.1.4.3, "Deleting an IPv6 Address"

Section 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 Section 7.1.4.2, "Adding an IPv6 Address".

Section 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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 with for various purposes including:

- Find a link-layer address of a neighbor
- Discover neighbor routers
- Determine any change in the link-layer address
- Determine when a neighbor is down
- Send 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-lifetime }	**Synopsis:** A 32-bit unsigned 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-preference }	**Synopsis:** A 32-bit unsigned 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.
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-lifetime }	**Synopsis:** A 32-bit unsigned 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:** A 32-bit unsigned 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:** A 32-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.1.6.1, "Adding an IPv6 Network Prefix"
- Section 7.1.6.2, "Deleting an IPv6 Network Prefix"

Section 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:** { infinite } or a 32-bit unsigned integer between 0 and 4294967295 The length of time in seconds during which time the prefix is valid for the purpose of on-link determination.
preferred { preferred }	**Synopsis:** { infinite } or a 32-bit unsigned integer between 0 and 4294967295 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.2.1, "Configuring the DHCP Relay Agent"

- Section 7.2.2, "Assigning a DHCP Server Address"
- Section 7.2.3, "Viewing a List of DHCP Client Ports"
- Section 7.2.4, "Adding a DHCP Client Port"
- Section 7.2.5, "Deleting a DHCP Client Port"
- Section 7.2.6, "Example: Configuring the Device as a Relay Agent"

Section 7.2.1
Configuring the DHCP Relay Agent

To configure 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 Section 7.2.4, "Adding a DHCP Client Port".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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 Section 7.2.4, "Adding a DHCP Client Port".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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 swport 1
 !
!
```

If no client ports have been configured, add client ports as needed. For more information, refer to Section 7.2.4, "Adding a DHCP Client Port".

Section 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

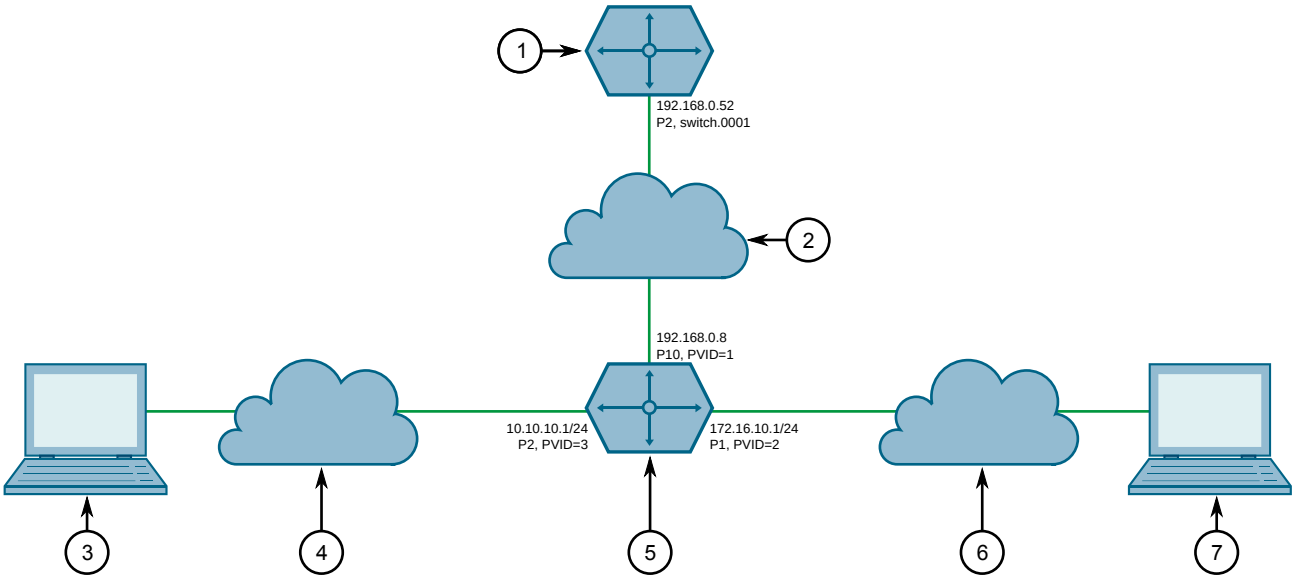


Figure 5: Topology – Device as a Relay Agent

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

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 Section 8.5.5.2, "Adding a Static VLAN".
   b. Assign IP address *192.168.0.8* to VLAN 1. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
   c. Change the PVID of port 1 to PVID 2, and change the PVID of port 2 to PVID 3. Refer to Section 8.1.2, "Configuring a Switched Ethernet Port" 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 Section 7.3.19, "Example: Configuring the Device as a DHCP Server to Support a Relay Agent" 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
 !
```

Section 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.

CONTENTS

- Section 7.3.1, "Viewing a List of Active Leases"
- Section 7.3.2, "Configuring the DHCP Server"
- Section 7.3.3, "Enabling/Disabling the DHCP Server"
- Section 7.3.4, "Configuring DHCP Server Options"
- Section 7.3.5, "Managing DHCP Client Configuration Options"
- Section 7.3.6, "Managing DHCP Listen Interfaces"
- Section 7.3.7, "Managing Shared Networks"
- Section 7.3.8, "Managing Subnets"
- Section 7.3.9, "Managing Host Groups"
- Section 7.3.10, "Managing DHCP Hosts"
- Section 7.3.11, "Managing Address Pools (IPv4)"
- Section 7.3.12, "Managing Address Pools (IPv6)"
- Section 7.3.13, "Managing IP Ranges (IPv4)"
- Section 7.3.14, "Managing IP Ranges (IPv6)"
- Section 7.3.15, "Managing IPv6 Prefixes"
- Section 7.3.16, "Managing Temporary Subnets"
- Section 7.3.17, "Managing IPv6 Subnets"
- Section 7.3.18, "Managing Option 82 Classes for Address Pools"
- Section 7.3.19, "Example: Configuring the Device as a DHCP Server to Support a Relay Agent"

Section 7.3.1
Viewing a List of Active Leases

RUGGEDCOM ROX II can generate a list of active leases. The list includes the start and end times, hardware Ethernet address, and client host name for each lease.

To view a list of active leases, do the following:

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;
}
```

Section 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 Section 7.3.19, "Example: Configuring the Device as a DHCP Server to Support a Relay Agent".

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 Section 7.2.6, "Example: Configuring the Device as a Relay Agent" for more information.
2. Enable the DHCP server. For more information, refer to Section 7.3.3, "Enabling/Disabling the DHCP Server".
3. Add a DHCP listen interface. For more information, refer to Section 7.3.6.2, "Adding a DHCP Listen Interface".
4. Assign an IP address to the listen interface. For more information, refer to Section 7.3.8.2, "Adding a Subnet".
5. Create a shared network and enable Option82. For more information, refer to Section 7.3.7.2, "Adding a Shared Network" and Section 7.3.7.3, "Configuring Shared Network Options".
6. Create a subnet for each LAN that has DHCP clients. For more information about creating subnets, refer to Section 7.3.8.2, "Adding a Subnet".

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 Section 7.3.8.2, "Adding a Subnet".
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 Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".

      For more information about IP ranges, refer to Section 7.3.13.2, "Adding an IP Range (IPv4)" or Section 7.3.14.2, "Adding an IP Range (IPv6)".

   b. [Optional] Configure the option82 class on the relay agent, if used. For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".
9. [Optional] Add and configure hosts and host-groups. For more information, refer to Section 7.3.10.2, "Adding a Host".

Section 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, or type **`revert`** and press **Enter** to abort.

Section 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:

> **IMPORTANT!**
> ***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 Section 7.3.8.3, "Configuring Subnet Options".*

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 Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)"
- Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)"
- Section 7.3.5.3, "Viewing a List of Custom DHCP Client Configuration Options"
- Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option"
- Section 7.3.5.5, "Deleting a Custom DHCP Client Configuration Option"

Section 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 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.
subnetmask { subnetmask }	**Synopsis:** A string 7 to 15 characters long Subnet mask
default-route { default-route }	**Synopsis:** A string 7 to 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 7 to 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 1 to 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 7 to 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 7 to 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 7 to 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 1 to 253 characters long

Parameter	Description
	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 1 to 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 1 to 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 Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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 1 to 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 6 to 87 characters long The domain name server that the server offers to the client when it issues the lease to the client.

Parameter	Description
domain-search { domain-search }	**Synopsis:** A string 1 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 6 to 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 1 to 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 Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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 Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option".

Section 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 }	**Synopsis:** A 32-bit signed integer
{ value }	**Synopsis:** A 32-bit signed integer The value of the custom option.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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 number
     ```

   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, or type **revert** and press **Enter** to abort.

Section 7.3.6

Managing DHCP Listen Interfaces

DHCP listen interfaces specify the IP interface to which the client sends a request.

CONTENTS

- Section 7.3.6.1, “Viewing a List of DHCP Listen Interfaces”
- Section 7.3.6.2, “Adding a DHCP Listen Interface”
- Section 7.3.6.3, “Deleting a DHCP Listen Interface”

Section 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 Section 7.3.6.2, "Adding a DHCP Listen Interface".

Section 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.7.1, "Viewing a List of Shared Networks"
- Section 7.3.7.2, "Adding a Shared Network"
- Section 7.3.7.3, "Configuring Shared Network Options"
- Section 7.3.7.4, "Deleting a Shared Network"

Section 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 Section 7.3.7.2, "Adding a Shared Network".

Section 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 Section 7.3.7.3, "Configuring Shared Network Options".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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 following parameter(s) as required:

IMPORTANT!
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 Section 7.3.8.3, "Configuring Subnet Options".

Parameter	Description
unknown-client { unknown-client }	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients

Parameter	Description
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 configuration options for DHCP clients at the shared network level. For more information, refer to refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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, or type **`revert`** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.8.1, "Viewing a List of Subnets"
- Section 7.3.8.2, "Adding a Subnet"
- Section 7.3.8.3, "Configuring Subnet Options"
- Section 7.3.8.4, "Deleting a Subnet"

Section 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 Section 7.3.8.2, "Adding a Subnet".

Section 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 Section 7.3.7.2, "Adding a Shared Network".

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 9 to 18 characters long The network IP address for this subnet. This parameter is mandatory.
shared-network { shared-network }	**Synopsis:** A string

Parameter	Description
	The shared-network that this host belongs to.

Parameter	Description
network-ip { network-ip }	**Synopsis:** A string 4 to 43 characters long The network IPv6 address for this subnet. This parameter is mandatory.
shared-network { shared-network }	**Synopsis:** A string The shared-network that this host belongs to.

4. Configure the options for the subnet. For more information, refer to Section 7.3.8.3, "Configuring Subnet Options".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

   - **For IPv6:**

Parameter	Description
default { default }	**Synopsis:** A 32-bit unsigned integer **Default:** 600

Parameter	Description
	The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned 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):

> **IMPORTANT!**
> ***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 Section 7.3.5.1, “Configuring Standard DHCP Client Configuration Options (IPv4)” or Section 7.3.5.2, “Configuring Standard DHCP Client Configuration Options (IPv6)”.
6. Configure one or more address pools to the subnet. For more information, refer to Section 7.3.11.2, “Adding an Address Pool (IPv4)” or Section 7.3.12.2, “Adding an Address Pool (IPv6)”.
7. Configure one or more IP ranges to the subnet. For more information, refer to Section 7.3.13.2, “Adding an IP Range (IPv4)” or Section 7.3.14.2, “Adding an IP Range (IPv6)”.

8. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.9.1, “Viewing a List of Host Groups”
- Section 7.3.9.2, “Adding a Host Group”
- Section 7.3.9.3, “Configuring Host Group Options”
- Section 7.3.9.4, “Deleting a Host Group”

Section 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 Section 7.3.9.2, "Adding a Host Group".

Section 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 }	**Synopsis:** A string 1 to 32 characters long The description of the host groups.

4. Configure the options for the host group. For more information, refer to Section 7.3.9.3, "Configuring Host Group Options".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

   - **For IPv6:**

Parameter	Description
default { default }	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned 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 The shared-network that this host belongs to.
subnet { subnet }	**Synopsis:** A string 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 The shared-network that this host belongs to.
subnet6 { subnet6 }	**Synopsis:** A string

Parameter	Description
	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 Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
7. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 7.3.10
Managing DHCP Hosts

Host entries assign settings to a specific client based on its Ethernet MAC address.

CONTENTS

- Section 7.3.10.1, "Viewing a List of Hosts"
- Section 7.3.10.2, "Adding a Host"
- Section 7.3.10.3, "Configuring Host Options"
- Section 7.3.10.4, "Deleting Hosts"

Section 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 Section 7.3.10.2, "Adding a Host".

Section 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 Section 7.3.10.3, "Configuring Host Options".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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 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. This parameter is mandatory.

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

Parameter	Description
default { default }	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned 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 7 to 15 characters long The IP address that the server assigns to the matching client. This parameter is mandatory.
unknown-client { unknown-client }	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
shared-network { shared-network }	**Synopsis:** A string The shared-network that this host belongs to.
subnet { subnet }	**Synopsis:** A string The subnet that this host belongs to.
host-groups { host-groups }	**Synopsis:** A string

Parameter	Description
	The host groups that this host belongs to.

- **For IPv6**

Parameter	Description
fixed-ip { fixed-ip }	**Synopsis:** A string 6 to 40 characters long The IPv6 address that the server assigns to the matching client.
fixed-prefix6 { fixed-prefix6 }	**Synopsis:** A string 4 to 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 The shared-network that this host belongs to.
subnet6 { subnet6 }	**Synopsis:** A string The subnet that this host belongs to.
host-groups { host-groups }	**Synopsis:** A string 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 Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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, or type **`revert`** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.11.1, "Viewing a List of Address Pools (IPv4)"
- Section 7.3.11.2, "Adding an Address Pool (IPv4)"
- Section 7.3.11.3, "Deleting an Address Pool (IPv4)"

Section 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 ippool
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 Section 7.3.11.2, "Adding an Address Pool (IPv4)".

Section 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:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned 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 7 to 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 Section 7.3.13.2, "Adding an IP Range (IPv4)".
6. Add one or more Option82 classes to the pool. For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".
7. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.12.1, "Viewing a List of Address Pools (IPv6)"
- Section 7.3.12.2, "Adding an Address Pool (IPv6)"
- Section 7.3.12.3, "Deleting an Address Pool (IPv6)"

Section 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 Section 7.3.12.2, "Adding an Address Pool (IPv6)".

Section 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:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum { maximum }	**Synopsis:** A 32-bit unsigned 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 Section 7.3.14.2, "Adding an IP Range (IPv6)".
6. [Optional] Add one or more subnets to the pool. For more information, refer to Section 7.3.17.2, "Adding a IPv6 Subnet".
7. [Optional] Add one or more temporary subnets to the pool. For more information, refer to Section 7.3.16.2, "Adding a Temporary Subnet".
8. [Optional] Add one or more prefixes to the pool. For more information, refer to Section 7.3.15.2, "Adding an IPv6 Prefix".
9. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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 ippool6 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, or type **revert** and press **Enter** to abort.

Section 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).

CONTENTS

- Section 7.3.13.1, "Viewing a List of IP Ranges (IPv4)"
- Section 7.3.13.2, "Adding an IP Range (IPv4)"
- Section 7.3.13.3, "Deleting an IP Range (IPv4)"

Section 7.3.13.1
Viewing a List of IP Ranges (IPv4)

To view a list of IP ranges configured for a DHCP subnet, type:

- **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 Section 7.3.13.2, "Adding an IP Range (IPv4)" or Section 7.3.14.2, "Adding an IP Range (IPv6)".

Section 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. 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

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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. 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 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

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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).

CONTENTS

- Section 7.3.14.1, “Viewing a List of IP Ranges (IPv6)”
- Section 7.3.14.2, “Adding an IP Range (IPv6)”
- Section 7.3.14.3, “Deleting an IP Range (IPv6)”

Section 7.3.14.1
Viewing a List of IP Ranges (IPv6)

To view a list of IP ranges configured for a DHCP subnet, type:

- **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 Section 7.3.14.2, "Adding an IP Range (IPv6)".

Section 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. 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 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.15.1, “Viewing a List of IPv6 Prefixes”
- Section 7.3.15.2, “Adding an IPv6 Prefix”
- Section 7.3.15.3, “Deleting an IPv6 Prefix”

Section 7.3.15.1
Viewing a List of IPv6 Prefixes

To view a list of IP ranges configured for a DHCP subnet, type:

For DHCP IPv6 subnets

```
show running-config services dhcpserver6 subnet6-name name options prefix6
```

Where:

- *name* is the name of the subnet

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 prefix6
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 Section 7.3.15.2, "Adding an IPv6 Prefix".

Section 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. Add the prefix by typing:

   ```
   services dhcpserver6 subnet6-name name options prefix6 prefix
   ```

   Where:

   - *name* is the name of the subnet
   - *prefix* is the starting IPv6 prefix delegation
3. Configure the IPv6 Range Configuration by configuring the following parameter(s) as required:

Parameter	Description
end { end }	**Synopsis:** A string 6 to 40 characters long The ending IPv6 prefix delegation that the server uses to offer to the client. This parameter is mandatory.
bits { bits }	**Synopsis:** An 8-bit unsigned integer between 1 and 64 Prefix delegations of bits length that are offered to the client. This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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:

   ```
   no services dhcpserver6 subnet6-name name options prefix6 prefix
   ```

   Where:

   - *name* is the name of the subnet

- *prefix* is the prefix

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.3.16.1, "Viewing a List of Temporary Subnets"
- Section 7.3.16.2, "Adding a Temporary Subnet"
- Section 7.3.16.3, "Deleting a Temporary Subnet"

Section 7.3.16.1
Viewing a List of Temporary Subnets

To view a list of temporary subnets, type:

For DHCP IPv6 subnets

```
show running-config services dhcpserver6 subnet6-name name options temporarysubnet6
```

Where:

- *name* is the name of the subnet

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 temporarysubnet6
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 Section 7.3.15.2, "Adding an IPv6 Prefix".

Section 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. Add the prefix by typing:

```
services dhcpserver6 subnet6-name name options temporarysubnet6 temporaryname
```

Where:

- *name* is the name of the subnet
- *temporaryname* is the name of the temporary subnet

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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:

```
no services dhcpserver6 subnet6-name name options temporarysubnet6 temporaryname
```

Where:

- *name* is the name of the subnet
- *temporaryname* is the temporary subnet

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 7.3.17
Managing IPv6 Subnets

One or more optional IPv6 subnets can be defined for the server to offer to the client.

CONTENTS

- Section 7.3.17.1, "Viewing a List of IPv6 Subnets"
- Section 7.3.17.2, "Adding a IPv6 Subnet"
- Section 7.3.17.3, "Deleting an IPv6 Subnet"

Section 7.3.17.1
Viewing a List of IPv6 Subnets

To view a list of IPv6 subnets, type:

```
show running-config services dhcpserver6 subnet6-name name options subnet6
```

Where:

- *name* is the name of the subnet

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 subnet6
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 Section 7.3.15.2, "Adding an IPv6 Prefix".

Section 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. Add the IPv6 subnet by typing:

   ```
   services dhcpserver6 subnet6-name name options subnet6 subnet6name
   ```

   Where:

   - *name* is the name of the subnet
   - *subnet6name* is the name of the IPv6 subnet
3. Configure the following parameter(s) as required:

Parameter	Description
{ subnet-number }	**Synopsis:** A string 4 to 43 characters long The IPv6 subnet that the server uses to offer to the client. This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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:

   ```
   no services dhcpserver6 subnet6-name name options subnet6 subnet6name
   ```

   Where:

   - *name* is the name of the subnet
   - *subnet6name* is the name of the IPv6 subnet
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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.

IMPORTANT!
For more information about enabling the DHCP server to accept Option 82 information, refer to either Section 7.3.4, "Configuring DHCP Server Options" or Section 7.3.8.3, "Configuring Subnet Options".

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.

CONTENTS

- Section 7.3.18.1, "Viewing a List of Option 82 Classes for Address Pools"
- Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool"
- Section 7.3.18.3, "Deleting an Option 82 Class From an Address Pool"

Section 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, type:

```
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 Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".

Section 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. 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
3. 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 17 characters long Specifies the information relating to the remote host end of the circuit. This parameter is mandatory.
circuit-id { circuit-id }	**Synopsis:** A string 1 to 17 characters long Specifies the local information to which circuit the request came in on (ie. 00:02:03:02) This parameter is mandatory.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 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, or type **`revert`** and press **Enter** to abort.

Section 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.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

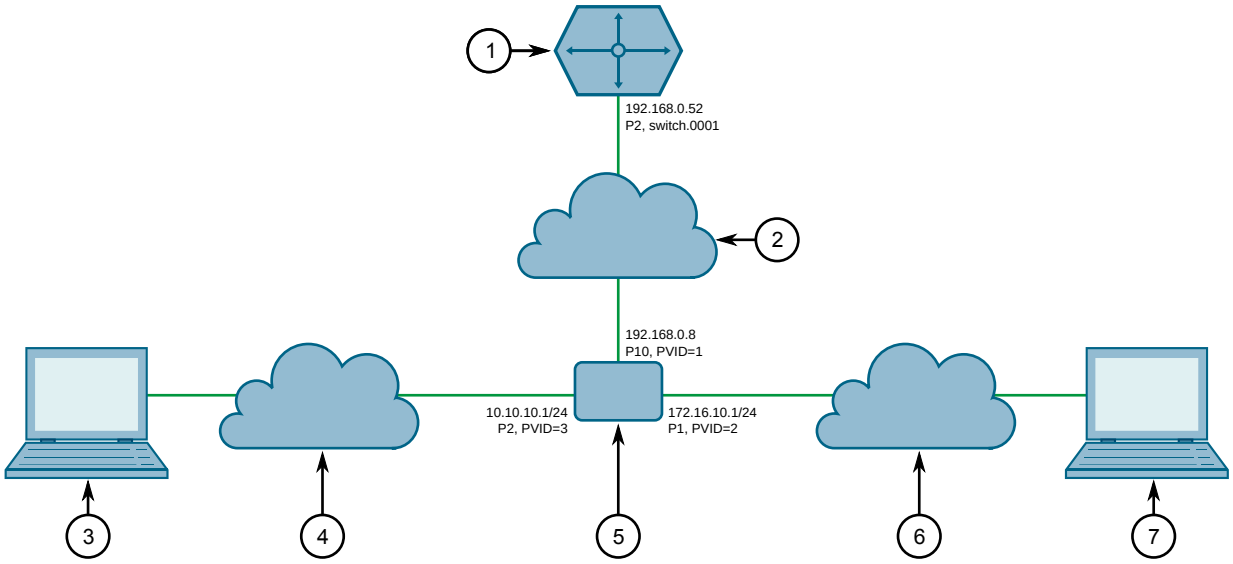


Figure 6: Topology – Device as a DHCP Server

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

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 Section 7.2.6, "Example: Configuring the Device as a Relay Agent" for more information.

2. Enable the DHCP server. For more information, refer to Section 7.3.3, "Enabling/Disabling the DHCP Server".
3. Add the management interface (switch.0001) as a DHCP listen interface. For more information, refer to Section 7.3.6.2, "Adding a DHCP Listen Interface".
4. Assign IP address *192.168.0.52* to switch.0001 on the DHCP server. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
5. Create a shared network named *LAN.10-LAN.172* and enable Option82. For more information, refer to Section 7.3.7.3, "Configuring Shared Network Options".
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 Section 7.3.8.2, "Adding a Subnet".

7. [Optional] For the LAN A-172 subnet, configure *172.16.10.1* as a default route for clients. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)".
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 Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".

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 Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".

10. [Optional] For the LAN B-10 subnet, configure *10.10.10.1* as a default route for clients. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)".
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 Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".

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 Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".

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
```

Section 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.

CONTENTS

- Section 7.4.1, "Managing Domain Names"
- Section 7.4.2, "Managing Domain Name Servers"

Section 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).

CONTENTS

- Section 7.4.1.1, "Viewing a List of Domain Names"
- Section 7.4.1.2, "Adding a Domain Name"
- Section 7.4.1.3, "Deleting a Domain Name"

Section 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 Section 7.4.1.2, "Adding a Domain Name".

Section 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.4.2.1, “Viewing a List of Domain Name Servers”
- Section 7.4.2.2, “Adding a Domain Name Server”
- Section 7.4.2.3, “Deleting a Domain Name Server”

Section 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 Section 7.4.2.2, "Adding a Domain Name Server".

Section 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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 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 Section 5.7.4, "Configuring an Alarm".

CONTENTS

- Section 7.5.1, "Enabling and Configuring Dynamic DNS"
- Section 7.5.2, "Managing Dynamic DNS Servers"
- Section 7.5.3, "Managing Dynamic DNS Server Host Names"

Section 7.5.1

Enabling and Configuring Dynamic DNS

To enable and configure dynamic DNS, do the following:

IMPORTANT!
Update requests are sent to the selected service provider via HTTPS. As such, before enabling Dynamic DNS, the Trusted Certificate Store must be enabled. For more information, refer to Section 6.7.2.2, "Enabling/Disabling the Trusted Certificate Store".

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:** A 32-bit unsigned 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:** A 32-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 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.

CONTENTS

- Section 7.5.2.1, "Viewing a List of Dynamic DNS Servers"
- Section 7.5.2.2, "Viewing the Status of a Dynamic DNS Server"
- Section 7.5.2.3, "Adding a Dynamic DNS Server"
- Section 7.5.2.4, "Deleting a Dynamic DNS Server"

Section 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 Section 7.5.2.3, "Adding a Dynamic DNS Server".

Section 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

Section 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	**Synopsis:** { true, false } **Default:** false Enables / disables DDNS updates for the server
username { username }	**Synopsis:** A string 2 to 24 characters long The username of the DDNS server This parameter is mandatory.
password { password }	**Synopsis:** A string The password of the DDNS server This parameter is mandatory.

4. Define one or more host names for the server. For more information, refer to Section 7.5.3.2, "Adding a Host Name".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

Section 7.5.3
Managing Dynamic DNS Server Host Names

This section describes how to manage host names for the configured dynamic DNS servers.

IMPORTANT!
At least one host name is required for each configured dynamic DNS server.

CONTENTS

- Section 7.5.3.1, "Viewing a List of Host Names"
- Section 7.5.3.2, "Adding a Host Name"
- Section 7.5.3.3, "Deleting a Host Name"

Section 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 Section 7.5.3.2, "Adding a Host Name".

Section 7.5.3.2
Adding a Host Name

To add a host name for a dynamic DNS server, do the following:

IMPORTANT!
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, or type **revert** and press **Enter** to abort.

Section 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, or type **revert** and press **Enter** to abort.

8 Layer 2

This chapter describes the Layer 2, or Data Link Layer (DLL), features of RUGGEDCOM ROX II.

CONTENTS

- Section 8.1, “Managing Switched Ethernet Ports”
- Section 8.2, “Managing Ethernet Trunk Interfaces”
- Section 8.3, “Managing MAC Addresses”
- Section 8.4, “Managing Multicast Filtering”
- Section 8.5, “Managing VLANs”

Section 8.1

Managing Switched Ethernet Ports

This section describes how to configure and manage switched Ethernet ports.

CONTENTS

- Section 8.1.1, “Viewing a List of Switched Ethernet Ports”
- Section 8.1.2, “Configuring a Switched Ethernet Port”
- Section 8.1.3, “Viewing Switched Ethernet Port Statistics”
- Section 8.1.4, “Viewing the Status of a Switched Ethernet Port”
- Section 8.1.5, “Viewing RMON Port Statistics”
- Section 8.1.6, “Clearing Switched Ethernet Port Statistics”
- Section 8.1.7, “Resetting a Switched Ethernet Port”
- Section 8.1.8, “Testing Switched Ethernet Port Cables”

Section 8.1.1

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 swport 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
  !
 !
.
.
.
```

Section 8.1.2

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 » swport » {port}***, where *{port}* is the switched Ethernet port.
3. Configure the port settings by configuring the following parameter(s) as required:

CAUTION!
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.

CAUTION!
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 Section 15.5.2, "Configuring Port Rate Limiting".

Parameter	Description
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:** A string 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. This parameter is mandatory.
speed { speed }	**Synopsis:** A string 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. This parameter is mandatory.
duplex { duplex }	**Synopsis:** A string 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. This parameter is mandatory.
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.
switchport	**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

Parameter	Description
	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:** A 32-bit signed integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
alias { alias }	**Synopsis:** A string 1 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. • 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:** A 32-bit signed integer between 0 and 7 **Default:** 0

Parameter	Description
	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:** A 32-bit signed 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 Section 8.5.4.2, "Configuring VLANs for Switched Ethernet Ports".
9. Configure the port security settings. For more information, refer to Section 6.5.2, "Configuring Port Security".
10. Configure the spanning tree settings. For more information, refer to Section 13.4.5, "Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces".
11. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 8.1.3
Viewing Switched Ethernet Port Statistics

To view statistics collected for a specific switched Ethernet port, type:

```
show interfaces switch swport port port-stats
```

Where:

- *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 swport 1 port-stats
port-stats
 in octets  6820
 out octets 3086
 in pkts    33
 out pkts   18
 error pkts 0
```

This table or list provides the following information:

Parameter	Description
in-octets	**Synopsis:** A 32-bit unsigned integer The number of octets in received good packets. (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
out-octets	**Synopsis:** A 32-bit unsigned integer The number of octets in transmitted good packets. This parameter is mandatory.
in-pkts	**Synopsis:** A 32-bit unsigned integer The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
out-pkts	**Synopsis:** A 32-bit unsigned integer The number of transmitted good packets. This parameter is mandatory.
error-pkts	**Synopsis:** A 32-bit unsigned integer The number of any type of erroneous packets. This parameter is mandatory.

Section 8.1.4
Viewing the Status of a Switched Ethernet Port

To view the current status of a switched Ethernet port, type:

```
show interfaces switch swport port
```

Where:

- *port* is the port number for the switched Ethernet port

A table or list similar to the following example appears:

```
ruggedcom# show interfaces switch swport 1
 name   ge-1-1
 state  up
 media  1000T
 speed  100M
 duplex full
 mtu    1500
 mac    00:0a:dc:f6:c6:21
 .
 .
 .
```

This table or list provides the following information:

Parameter	Description
name	**Synopsis:** A string 1 to 10 characters long A descriptive name that may be used to identify the device connected on that port. This parameter is mandatory.
state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's link status. This parameter is mandatory.
media	**Synopsis:** A string 1 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. This parameter is mandatory.
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) This parameter is mandatory.
duplex	**Synopsis:** { auto, half, full } Duplex Setting: { Auto, Half, Full } This parameter is mandatory.
mtu	**Synopsis:** A 32-bit signed integer The Maximum Transmission Unit of frame (in bytes) permitted on the interface. This parameter is mandatory.
mac	**Synopsis:** A string 17 characters long The MAC Address of this specific port. This parameter is mandatory.

Section 8.1.5
Viewing RMON Port Statistics

To view Remote Network Monitoring (RMON) statistics collected for a specific switched Ethernet port, type:

```
show interfaces switch swport port rmon-stats
```

Where:

- *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 swport 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
```

This table or list provides the following information:

Parameter	Description
in-octets	**Synopsis:** A 64-bit unsigned integer The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
in-pkts	**Synopsis:** A 64-bit unsigned integer The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
in-bcast-pkts	**Synopsis:** A 64-bit unsigned integer The number of good broadcast packets received. This parameter is mandatory.
in-mcast-pkts	**Synopsis:** A 64-bit unsigned integer The number of good multicast packets received. This parameter is mandatory.
total-in-octets	**Synopsis:** A 64-bit unsigned 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. This parameter is mandatory.
total-in-pkts	**Synopsis:** A 64-bit unsigned integer

Parameter	Description
	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. This parameter is mandatory.
out-octets	**Synopsis:** A 64-bit unsigned integer The number of octets in transmitted good packets. This parameter is mandatory.
out-pkts	**Synopsis:** A 64-bit unsigned integer The number of transmitted good packets. This parameter is mandatory.
drop-events	**Synopsis:** A 32-bit unsigned integer The number of received packets that are dropped due to lack of receive buffers. This parameter is mandatory.
out-bcast-pkts	**Synopsis:** A 64-bit unsigned integer The number of transmitted broadcast packets. This parameter is mandatory.
out-mcast-pkts	**Synopsis:** A 64-bit unsigned integer The number of transmitted multicast packets. This does not include broadcast packets. This parameter is mandatory.
crc-align-errors	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
undersize-pkts	**Synopsis:** A 64-bit unsigned 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. This parameter is mandatory.
oversize-pkts	**Synopsis:** A 32-bit unsigned integer The number of packets received with data length greater than 1536 octets and valid CRC. This parameter is mandatory.
fragments	**Synopsis:** A 32-bit unsigned integer The number of packets received which meet all the following conditions: 1. The packet data length is less than 64 octets, or it is a packet without SFD and is less than 64 octets in length. 2. A Collision Event has not been detected. 3. A Late Collision Event has not been detected. 4. The packet has invalid CRC. This parameter is mandatory.
jabbers	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
collisions	**Synopsis:** A 32-bit unsigned integer The number of received packets for which a Collision Event has been detected. This parameter is mandatory.

Parameter	Description
late-collisions	**Synopsis:** A 32-bit unsigned integer The number of received packets for which a Late Collision Event has been detected. This parameter is mandatory.
pkts-64-octets	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
pkts-65to127-octets	**Synopsis:** A 32-bit unsigned 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 This parameter is mandatory.
pkts-128to255-octets	**Synopsis:** A 32-bit unsigned 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 This parameter is mandatory.
pkts-256to511-octets	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
pkts-512to1023-octets	**Synopsis:** A 32-bit unsigned 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 This parameter is mandatory.
pkts-1024to1518-octets	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.

Section 8.1.6
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 swport port clear-port-stats
```

Where:

- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

Section 8.1.7

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 swport port reset-port
```

Where:

- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

Section 8.1.8

Testing Switched Ethernet Port Cables

Diagnostics can be performed on switched Ethernet port cables to assess their overall quality.

CONTENTS

- Section 8.1.8.1, “Running a Cable Diagnostic Test”
- Section 8.1.8.2, “Viewing Cable Diagnostic Statistics”
- Section 8.1.8.3, “Clearing Cable Diagnostic Statistics”

Section 8.1.8.1

Running a Cable Diagnostic Test

To run a cable diagnostic test on a specific port, type:

IMPORTANT!
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 swport port diagnostics start-cable-test run runs calibration calibration
```

Where:

- *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 Section 8.1.8.2, "Viewing Cable Diagnostic Statistics".

Section 8.1.8.2
Viewing Cable Diagnostic Statistics

To view the statistics collected for a switched Ethernet port after a cable diagnostic test, type:

```
show interfaces switch swport port diagnostics cable-diagnostic-results
```

- *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 swport 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
```

This list provides the following information:

Parameter	Description
running	**Synopsis:** { true, false } Whether or not a cable test is currently running on this port This parameter is mandatory.
good	**Synopsis:** A 16-bit unsigned integer The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.

Parameter	Description
	This parameter is mandatory.
open	**Synopsis:** A 16-bit unsigned integer The number of times OPEN is detected on the cable pairs of the selected port. This parameter is mandatory.
short	**Synopsis:** A 16-bit unsigned integer The number of times SHORT is detected on the cable pairs of the selected port. This parameter is mandatory.
imped	**Synopsis:** A 16-bit unsigned integer The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port. This parameter is mandatory.
pass-fail-total	**Synopsis:** A string 1 to 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. • 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. This parameter is mandatory.
run-count	**Synopsis:** A 16-bit unsigned integer Run Count : The total number of iterations This parameter is mandatory.
pass-count	**Synopsis:** A 16-bit unsigned integer Pass Count This parameter is mandatory.
fail-count	**Synopsis:** A 16-bit unsigned integer Failure Count This parameter is mandatory.

Section 8.1.8.3
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:

Where:

- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

Section 8.2

Managing Ethernet Trunk Interfaces

This section describes how to configure and manage Ethernet trunk interfaces.

CONTENTS

- Section 8.2.1, "Viewing a List of Ethernet Trunk Interfaces"
- Section 8.2.2, "Adding an Ethernet Trunk Interface"
- Section 8.2.3, "Deleting an Ethernet Trunk Interface"
- Section 8.2.4, "Managing Ethernet Trunk Ports"

Section 8.2.1

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 swport 1
  !
  trunk-ports swport 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 Section 8.2.2, "Adding an Ethernet Trunk Interface".

Section 8.2.2

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	**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 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:** A 32-bit signed integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
alias { alias }	**Synopsis:** A string 1 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:** A 32-bit signed 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).

Parameter	Description
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:** A 32-bit signed 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. • 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, or type **`revert`** and press **Enter** to abort.

Section 8.2.3
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, or type **`revert`** and press **Enter** to abort.

Section 8.2.4

Managing Ethernet Trunk Ports

This section describes how to manage Ethernet trunk port assignments.

CONTENTS

- Section 8.2.4.1, "Viewing a List of Ethernet Trunk Ports"
- Section 8.2.4.2, "Adding an Ethernet Trunk Port"
- Section 8.2.4.3, "Deleting an Ethernet Trunk Port"

Section 8.2.4.1

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 swport 1
  !
  trunk-ports swport 2
  !
 !
!
```

If no Ethernet trunk ports have been configured, add ports as needed. For more information, refer to Section 8.2.4.2, "Adding an Ethernet Trunk Port".

Section 8.2.4.2

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 swport port
   ```

   Where:

   - *id* is the ID given to the trunk
   - *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.

Section 8.2.4.3
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 swport port
   ```

   Where:

   - *id* is the ID given to the trunk
   - *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.

Section 8.3
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.

CONTENTS

- Section 8.3.1, “Viewing a Dynamic List of MAC Addresses”
- Section 8.3.2, “Purging the Dynamic MAC Address List”
- Section 8.3.3, “Configuring MAC Address Learning Options”
- Section 8.3.4, “Managing Static MAC Addresses”

Section 8.3.1
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
-------------------------------------------------
00:01:c0:0b:b6:58  4    swport  4     dynamic  N/A
00:04:5f:fb:62:36  4    swport  4     dynamic  N/A
00:04:5f:fb:63:8e  4    swport  4     dynamic  N/A
00:06:b5:64:92:75  4    swport  4     dynamic  N/A
00:0a:dc:02:4f:c0  4    swport  4     dynamic  N/A
00:0a:dc:2d:a6:e3  4    swport  4     dynamic  N/A
00:0a:dc:e5:86:ff  4    swport  4     dynamic  N/A
00:0a:dc:e5:a4:ff  4    swport  4     dynamic  N/A
```

This table or list provides the following information:

Parameter	Description
mac	**Synopsis:** A string 17 characters long The MAC address learned by the switch.
vid	**Synopsis:** A 32-bit signed integer The VLAN identifier of the VLAN upon which the MAC address operates. This parameter is mandatory.
slot	**Synopsis:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } The slot containing the module including the port. This parameter is mandatory.
port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port on which the MAC address has been learned. This parameter is mandatory.
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. This parameter is mandatory.
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. This parameter is mandatory.

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 Section 8.3.3, "Configuring MAC Address Learning Options".
- Configure the address on the device as a static MAC address. For more information, refer to Section 8.3.4.2, "Adding a Static MAC Address".

Section 8.3.2

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
```

Section 8.3.3
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:** A 32-bit signed integer between 15 and 800 **Default:** 300 The time a learned MAC address is held before being aged out.
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, or type **`revert`** and press **Enter** to abort.

Section 8.3.4
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.

CONTENTS

- Section 8.3.4.1, “Viewing a List of Static MAC Addresses”
- Section 8.3.4.2, “Adding a Static MAC Address”
- Section 8.3.4.3, “Deleting a Static MAC Address”

Section 8.3.4.1
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  -        swport  2     normal
00:10:94:00:24:01  4084  -        swport  1     normal
00:10:94:00:30:01  1     -        swport  2     normal
00:10:94:00:40:01  4086  -        swport  2     normal

!
```

If no static MAC addresses have been configured, add addreses as needed. For more information, refer to Section 8.3.4.2, “Adding a Static MAC Address”.

Section 8.3.4.2
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.
slot { slot }	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
port { port }	**Synopsis:** A string 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, or type **revert** and press **Enter** to abort.

Section 8.3.4.3
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 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. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 8.4

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).

CONTENTS

- Section 8.4.1, “Multicast Filtering Concepts”
- Section 8.4.2, “Enabling and Configuring GMRP”
- Section 8.4.3, “Managing IGMP Snooping”
- Section 8.4.4, “Managing the Static Multicast Group Table”
- Section 8.4.5, “Managing Egress Ports for Multicast Groups”
- Section 8.4.6, “Viewing a Summary of Multicast Groups”
- Section 8.4.7, “Viewing a List of IP Multicast Groups”

Section 8.4.1

Multicast Filtering Concepts

This section describes some of the concepts important to the implementation of multicast filtering in RUGGEDCOM ROX II.

CONTENTS

- Section 8.4.1.1, “IGMP”
- Section 8.4.1.2, “GMRP (GARP Multicast Registration Protocol)”

Section 8.4.1.1

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.

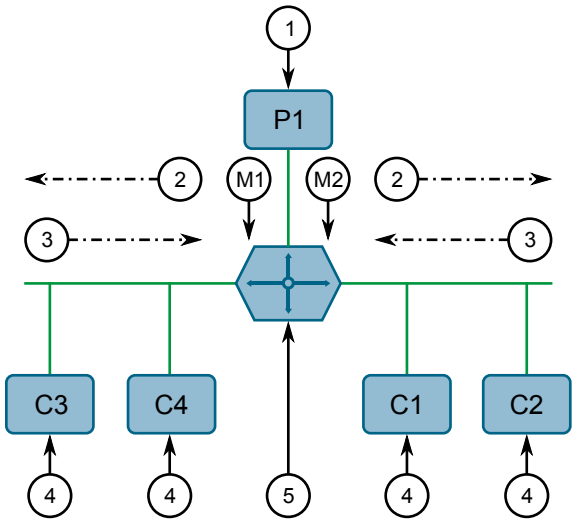


Figure 7: Example – IGMP In Operation

1. Producer **2.** Membership Queries **3.** Membership Reports **4.** Host **5.** Mulicast Router

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.

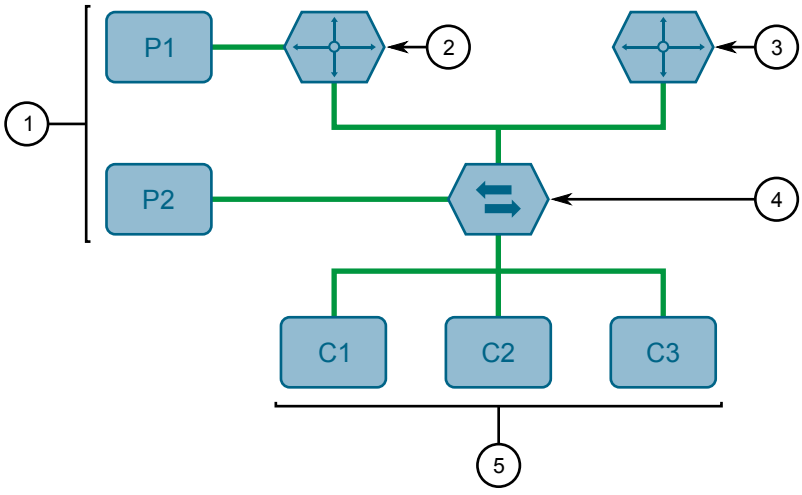


Figure 8: Example – Combined Router and Switch IGMP In Operation

1. Producer **2.** Multicast Router 1 **3.** Multicast Router 2 **4.** Switch **5.** Host

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.

Section 8.4.1.2
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 RX1400, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the RUGGEDCOM RX1400, 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.

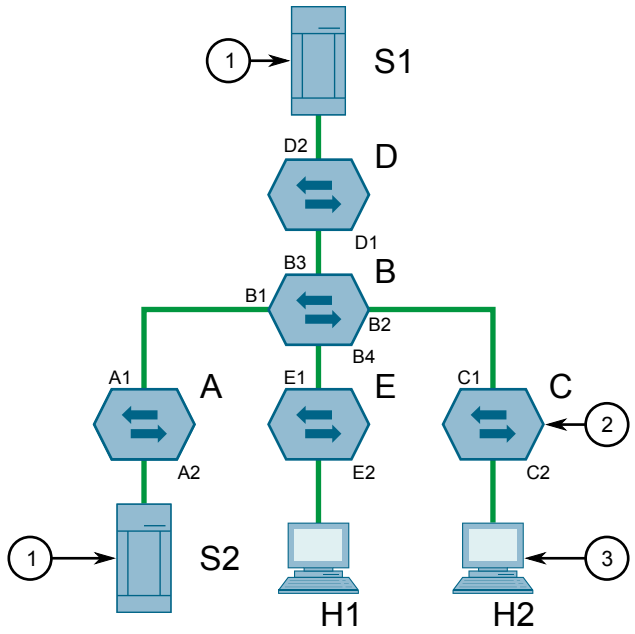


Figure 9: Example – Establishing Membership with GMRP

1. Multicast Source **2.** Switch **3.** Multicast Host

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.

Section 8.4.2
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	**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:** A 32-bit signed 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 Section 8.1.2, "Configuring a Switched Ethernet Port".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 8.4.3
Managing IGMP Snooping

This sections describes how to configure IGMP snooping and manage ports monitored by the service.

CONTENTS

- Section 8.4.3.1, "Configuring IGMP Snooping"
- Section 8.4.3.2, "Viewing a List of Router Ports"
- Section 8.4.3.3, "Adding a Router Port"
- Section 8.4.3.4, "Deleting a Router Port"

Section 8.4.3.1
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:** A 32-bit signed 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.
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 Section 8.4.3.3, "Adding a Router Port".
4. Enable IGMP snooping for the required static VLAN(s). For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 8.4.3.2
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
------------
swport   1

 !
!
```

If no router ports have been configured, add ports as needed. For more information, refer to Section 8.4.3.3, "Adding a Router Port".

Section 8.4.3.3
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 swport port
```

Where:

- *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.

Section 8.4.3.4
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 swport 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, or type **revert** and press **Enter** to abort.

Section 8.4.4
Managing the Static Multicast Group Table

This section describes how to manage entries in the Static Multicast Group table.

CONTENTS

- Section 8.4.4.1, "Viewing a List of Static Multicast Group Entries"
- Section 8.4.4.2, "Adding a Static Multicast Group Entry"
- Section 8.4.4.3, "Deleting a Static Multicast Group Entry"

Section 8.4.4.1
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 Section 8.4.4.2, "Adding a Static Multicast Group Entry".

Section 8.4.4.2
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 address
   ```

   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 Section 8.4.5.2, "Adding an Egress Port".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 8.4.4.3
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 address
   ```

   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, or type **revert** and press **Enter** to abort.

Section 8.4.5
Managing Egress Ports for Multicast Groups

This section describes how to configure and manage egress ports for a multicast group.

CONTENTS

- Section 8.4.5.1, "Viewing a List of Egress Ports"
- Section 8.4.5.2, "Adding an Egress Port"

- Section 8.4.5.3, "Deleting an Egress Port"

Section 8.4.5.1
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 address 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 swport 1
  !
 !
!
```

If no egress ports have been configured, add egress ports as needed. For more information, refer to Section 8.4.5.2, "Adding an Egress Port".

Section 8.4.5.2
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 address egress-ports swport 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
   - *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.

Section 8.4.5.3
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 address egress-ports swport 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
   - *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.

Section 8.4.6
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
-----------------------------------------------------
100  01:00:5e:00:01:01
                        swport  1
                                        swport  none
200  01:00:5e:00:01:02
                        swport  2
                                        swport  none
```

This table or list provides the following information:

Parameter	Description
vid	**Synopsis:** A 32-bit signed integer The VLAN Identifier of the VLAN upon which the multicast group operates.
mac	**Synopsis:** A string 17 characters long The multicast group MAC address.

Section 8.4.7
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
                                    swport      3
                                                      swport      1
200   225.0.1.2   01:00:5e:00:01:02
                                    swport      4
                                                      swport      2
```

This table or list provides the following information:

Parameter	Description
vid	**Synopsis:** A 32-bit signed 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 17 characters long The multicast MAC address corresponding to the group multicast IP address. This parameter is mandatory.
Joined Slot	The name of the module location provided on the silkscreen across the top of the device.
Joined Ports	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	The selected ports on the module installed in the indicated slot.

Section 8.5

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 Section 8.5.5, "Managing Static VLANs".
- **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 Section 8.5.1.7, "GARP VLAN Registration Protocol (GVRP)"

CONTENTS

- Section 8.5.1, "VLAN Concepts"
- Section 8.5.2, "Configuring the Internal VLAN Range"
- Section 8.5.3, "Enabling/Disabling Ingress Filtering"

- Section 8.5.4, “Managing VLANs for Switched Ethernet Ports”
- Section 8.5.5, “Managing Static VLANs”
- Section 8.5.6, “Managing Forbidden Ports”
- Section 8.5.7, “Managing VLANs for Interfaces and Tunnels”

Section 8.5.1

VLAN Concepts

This section describes some of the concepts important to the implementation of VLANs in RUGGEDCOM ROX II.

CONTENTS

- Section 8.5.1.1, “Tagged vs. Untagged Frames”
- Section 8.5.1.2, “Native VLAN”
- Section 8.5.1.3, “Edge and Trunk Port Types”
- Section 8.5.1.4, “Ingress Filtering”
- Section 8.5.1.5, “Forbidden Ports List”
- Section 8.5.1.6, “VLAN-Aware Mode of Operation”
- Section 8.5.1.7, “GARP VLAN Registration Protocol (GVRP)”
- Section 8.5.1.8, “PVLAN Edge”
- Section 8.5.1.9, “VLAN Advantages”

Section 8.5.1.1

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.

Section 8.5.1.2

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.

Section 8.5.1.3
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 Section 8.5.1.5, "Forbidden Ports List".

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.

Section 8.5.1.4
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 Section 8.5.3, "Enabling/Disabling Ingress Filtering".

Section 8.5.1.5
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 Section 8.5.6, "Managing Forbidden Ports".

Section 8.5.1.6
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.

Section 8.5.1.7
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:

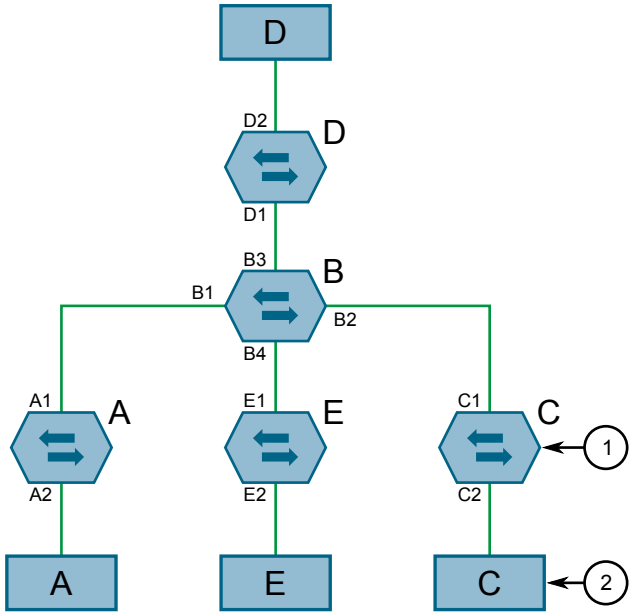


Figure 10: Using GVRP

1. Switch **2.** End Node

- 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

Section 8.5.1.8

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.

Section 8.5.1.9
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.

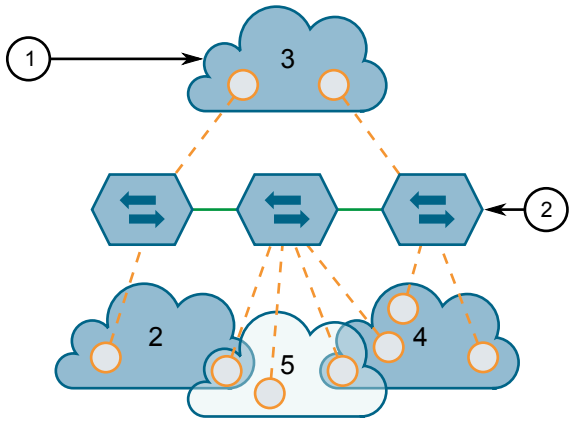


Figure 11: Multiple Overlapping VLANs

1. VLAN **2.** Switch

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.

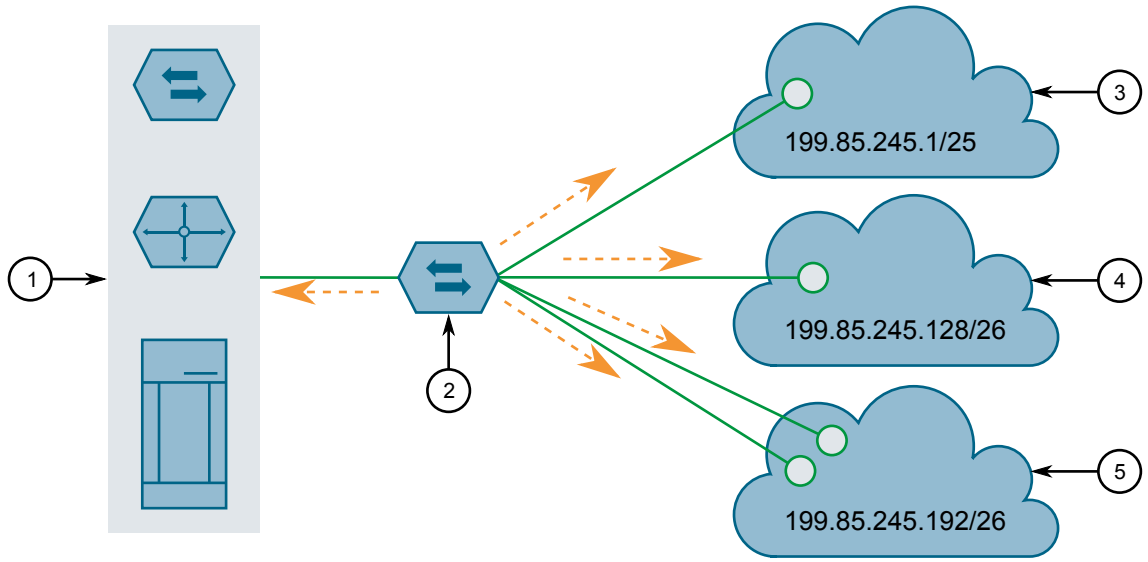


Figure 12: Inter-VLAN Communications

1. Server, Router or Layer 3 Switch **2.** Switch **3.** VLAN 2 **4.** VLAN 3 **5.** VLAN 4

Section 8.5.2

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.

CAUTION!
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.

IMPORTANT!
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.

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** false Enables/disables the Internal VLAN Range settings.
range-start { range-start }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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, or type **`revert`** and press **Enter** to abort.

Section 8.5.3
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

```
no switch vlans ingress-filtering enabled
```

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 8.5.4

Managing VLANs for Switched Ethernet Ports

This section describes how to configure and manage VLANs assigned to switched Ethernet ports.

CONTENTS

- Section 8.5.4.1, "Viewing VLAN Assignments for Switched Ethernet Ports"
- Section 8.5.4.2, "Configuring VLANs for Switched Ethernet Ports"

Section 8.5.4.1

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 | tab
      IGMP            UNTAGD  UNTAGD  TAGGED  TAGGED
VID   SNOOPING  MSTI  SLOT    PORTS   SLOT    PORTS   QOS  INGRESS  MARK
-------------------------------------------------------------------------
1     false     0
                      swport  1,5,6
                                      swport  none
                                                      0    0
                                                      1    0
                                                      2    0
                                                      3    0
                                                      4    0
                                                      5    0
                                                      6    0
                                                      7    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 Section 8.1.2, "Configuring a Switched Ethernet Port".

Section 8.5.4.2
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
{ vid }	**Synopsis:** A 32-bit signed integer between 1 and 4094 The VLAN ID for this routable logical interface.
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. This parameter is mandatory.
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:** A 32-bit signed integer between 68 and 9216 **Default:** 1500 The maximum transmission unit (the largest packet size allowed for this interface).

3. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to Section 15.2.7.2, “Adding a QoS Map”.
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 8.5.5
Managing Static VLANs

This section describes how to configure and manage static VLANs.

CONTENTS

- Section 8.5.5.1, “Viewing a List of Static VLANs”
- Section 8.5.5.2, “Adding a Static VLAN”
- Section 8.5.5.3, “Deleting a Static VLAN”

Section 8.5.5.1
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 Section 8.5.5.2, "Adding a Static VLAN".

Section 8.5.5.2
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 a 32-bit signed 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 Section 8.5.6.2, "Adding a Forbidden Port".
5. Configure the VLAN for the port. For more information, refer to Section 8.5.4.2, "Configuring VLANs for Switched Ethernet Ports".
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 8.5.5.3
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, or type **revert** and press **Enter** to abort.

Section 8.5.6
Managing Forbidden Ports

Static VLANs can be configured to exclude ports from membership in the VLAN using the forbidden ports list.

CONTENTS

- Section 8.5.6.1, "Viewing a List of Forbidden Ports"
- Section 8.5.6.2, "Adding a Forbidden Port"
- Section 8.5.6.3, "Deleting a Forbidden Port"

Section 8.5.6.1
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
     swport  1
     swport  2
60
     swport  2
     swport  3
     swport  4
70
     swport  5

!
```

If no ports have been forbidden, add forbidden ports as needed. For more information, refer to Section 8.5.6.2, "Adding a Forbidden Port".

Section 8.5.6.2
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 swport port
   ```

   Where:

   - *name* is the name of the static VLAN
   - *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.

Section 8.5.6.3
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 swport port
   ```

   Where:

   - *name* is the name of the static VLAN
   - *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, or type **revert** and press **Enter** to abort.

Section 8.5.7
Managing VLANs for Interfaces and Tunnels

This section describes how to view, add and delete tunnels for specific interfaces and tunnels.

- Section 11.1.8, “Managing VLANs for Virtual Switches”
- Section 11.4.6, “Managing VLANs for L2TPv3 Tunnels”

9 Serial Server

This chapter describes how to manage and configure the serial server, including serial ports, protocols, remote hosts and the Device Address Tables.

CONTENTS

- Section 9.1, “Managing Serial Ports”
- Section 9.2, “Managing Serial Port Protocols”
- Section 9.3, “Managing Device Address Tables”
- Section 9.4, “Managing Serial Multicast Streaming”
- Section 9.5, “Managing Remote Hosts”
- Section 9.6, “Managing Local Hosts”
- Section 9.7, “Managing Remote Host Interfaces”
- Section 9.8, “Managing Local Host Interfaces”

Section 9.1

Managing Serial Ports

This section describes how to configure, monitor and manage serial ports on the device.

CONTENTS

- Section 9.1.1, “Viewing a List of Serial Ports”
- Section 9.1.2, “Viewing Serial Port Statistics”
- Section 9.1.3, “Viewing Transport Connection Statistics”
- Section 9.1.4, “Viewing DNP Device Table Statistics”
- Section 9.1.5, “Clearing Serial Port Statistics”
- Section 9.1.6, “Configuring a Serial Port”
- Section 9.1.7, “Restarting the Serial Server”
- Section 9.1.8, “Resetting a Serial Port”

Section 9.1.1

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
-------------------------------------------------------------------------------
serport  1     true     -      9600  8     none    1     none     rs232
serport  2     true     -      9600  8     none    1     none     rs232

!
```

Section 9.1.2

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-1   RS232  9.6K   none      0      0        0      0        0       0       0        0
ser-2   RS232  9.6K   none      0      0        0      0        0       0       0        0
```

This table or list provides the following information:

Parameter	Description
ifname	**Synopsis:** A string 1 to 10 characters long The name of the serial interface.
media	**Synopsis:** A string 1 to 31 characters long The type of port media { RS232 RS422 RS485 }. This parameter is mandatory.
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). This parameter is mandatory.
protocol	**Synopsis:** A string 1 to 31 characters long The serial protocol assigned to this port. This parameter is mandatory.
tx-chars	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted over the serial port. This parameter is mandatory.
tx-packets	**Synopsis:** A 32-bit unsigned integer The number of packets transmitted over the serial port. This parameter is mandatory.
rx-chars	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The number of bytes received by the serial port. This parameter is mandatory.
rx-packets	**Synopsis:** A 32-bit unsigned integer The number of packets received by the serial port. This parameter is mandatory.
packet-errors	**Synopsis:** A 32-bit unsigned integer The number of packet errors on this serial port. This parameter is mandatory.
parity-errors	**Synopsis:** A 32-bit unsigned integer The number of parity errors on this serial port. This parameter is mandatory.
framing-errors	**Synopsis:** A 32-bit unsigned integer The number of framing errors on this serial port. This parameter is mandatory.
overrun-errors	**Synopsis:** A 32-bit unsigned integer The number of overrun errors on this serial port. This parameter is mandatory.

Section 9.1.3
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-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:

These tables or lists provide the following information:

Parameter	Description
index	**Synopsis:** A string 1 to 32 characters long The transport connection index.
remote-ip	**Synopsis:** A string 1 to 32 characters long The IP address of the remote serial server. This parameter is mandatory.
remote-port	**Synopsis:** A 32-bit signed integer

Parameter	Description
	The port of the remote serial server. This parameter is mandatory.
local-port	**Synopsis:** A 32-bit signed integer The local port for the incoming connection. This parameter is mandatory.
transport	**Synopsis:** A string 1 to 8 characters long The transport protocol (UDP or TCP) for this serial port. This parameter is mandatory.
rx-packets	**Synopsis:** A 32-bit unsigned integer The number of packets received from TCP/UDP. This parameter is mandatory.
tx-packets	**Synopsis:** A 32-bit unsigned integer The number of packets transmitted to TCP/UDP. This parameter is mandatory.
target-port	**Synopsis:** A string 1 to 1024 characters long The target serial port. This parameter is mandatory.
status	**Synopsis:** A string 1 to 31 characters long The connection status of the serial port. This parameter is mandatory.

Section 9.1.4
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-1
20       10.200.22.199  -
```

This table or list provides the following information:

Parameter	Description
device-address	**Synopsis:** A string 1 to 32 characters long The DNP device address.
remote-ip	**Synopsis:** A string 1 to 32 characters long The IP address of the remote host that provides a connection to the this DNP device address. This parameter is mandatory.
serial-port	**Synopsis:** A string 1 to 128 characters long

Parameter	Description
	The target serial port. This parameter is mandatory.

Section 9.1.5
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

Section 9.1.6
Configuring a Serial Port

To configure a serial port, do the following:

IMPORTANT!
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
{ 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 }	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
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 1 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:** A 32-bit signed integer between 7 and 8 **Default:** 8 The number of data bits.
parity { parity }	**Synopsis:** { none, even, odd }

Parameter	Description
	Default: none The parity of the serial port.
stop-bits { stop-bits }	**Synopsis:** A 32-bit signed 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 Section 9.2.3, "Adding a Serial Port Protocol".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 9.1.7
Restarting the Serial Server

To restart the serial server, type:

```
interfaces serial restart-serserver
```

Section 9.1.8
Resetting a Serial Port

To reset a serial port, type:

```
interfaces serial port name reset
```

Where:

- *name* is the name assigned to the port

Section 9.2
Managing Serial Port Protocols

This section describes how to configure and manage serial protocols for serial ports.

CONTENTS

- Section 9.2.1, "Serial Port Protocol Concepts"
- Section 9.2.2, "Viewing a List of Serial Port Protocols"
- Section 9.2.3, "Adding a Serial Port Protocol"

- Section 9.2.4, “Configuring the DNP Protocol”
- Section 9.2.5, “Configuring the Modbus TCP Protocol”
- Section 9.2.6, “Configuring the Raw Socket Protocol”
- Section 9.2.7, “Deleting a Serial Port Protocol”

Section 9.2.1

Serial Port Protocol Concepts

This section describes some of the concepts important to the implementation of serial port protocols in RUGGEDCOM ROX II.

CONTENTS

- Section 9.2.1.1, “Raw Socket Applications”
- Section 9.2.1.2, “Modbus TCP Applications”
- Section 9.2.1.3, “DNP Applications”
- Section 9.2.1.4, “Incoming/Outgoing Serial Connections”

Section 9.2.1.1

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).

Section 9.2.1.2
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.

Section 9.2.1.3

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.

Section 9.2.1.4
Incoming/Outgoing Serial Connections

The RUGGEDCOM RX1400 supports up to 32 TCP/UDP connections per serial port, up to a total of 64 TCP/UDP connections to the serial server.

Section 9.2.2
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-1   none
ser-2   none
```

If no serial port protocols have been configured, add protocols as needed. For more information, refer to Section 9.2.3, “Adding a Serial Port Protocol”.

Section 9.2.3
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 serport port protocols protocol
   ```

   Where:

   - *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` and `vmserial`.
3. If `dnp`, `tcpmodbus`, or `rawsocket` was selected, configure the protocol.
   - For information about configuring a DNP protocol, refer to Section 9.2.4, “Configuring the DNP Protocol”.
   - For information about configuring a Modbus TCP protocol, refer to Section 9.2.5, “Configuring the Modbus TCP Protocol”.

- For information about configuring a raw socket protocol, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 9.2.4
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 1 to 15 characters long The interface to learn the RTU address from.
aging-timer { aging-timer }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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 Section 9.3.2, "Adding a Device Address Table".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 9.2.5
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:** A 32-bit signed 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:** A 32-bit signed integer between 5 and 1000 **Default:** 1000

Parameter	Description
	The maximum allowable time to wait for a response to a Modbus request to complete once it has started.
turnaround { turnaround }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed integer between 1 and 32 **Default:** 1 The maximum number of incoming connections.
local-port { local-port }	**Synopsis:** A 32-bit signed 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. This parameter is mandatory.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 9.2.6
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 a 32-bit signed 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:** A 32-bit signed 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 a 32-bit signed integer between 16 and 1400 **Default:** max The maximum number of bytes received from the serial port to be forwarded.
turnaround { turnaround }	**Synopsis:** A 32-bit signed integer between 0 and 1000

Parameter	Description
	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:** A 32-bit signed integer between 1 and 32 **Default:** 1 The maximum number of incoming connections to permit when the call direction is incoming.
remote-ip { remote-ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address used when placing an outgoing connection.
remote-port { remote-port }	**Synopsis:** A 32-bit signed integer between 1024 and 65535 The TCP destination port used in outgoing connections.
local-ip { local-ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 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:** A 32-bit signed 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 Section 9.5.2, "Adding a Remote Host".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 9.2.7
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 serport port protocols protocol
```

Where:

- *`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, or type **`revert`** and press **Enter** to abort.

Section 9.3
Managing Device Address Tables

This section describes how to manage DNP addresses in the local Device Address Table.

CONTENTS

- Section 9.3.1, "Viewing a List of Device Address Tables"
- Section 9.3.2, "Adding a Device Address Table"
- Section 9.3.3, "Deleting a Device Address Table"

Section 9.3.1
Viewing a List of 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 slot/port protocols dnp setdnp device-table
```

Where:

- *slot/port* 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 serport 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 Section 9.3.2, "Adding a Device Address Table".

Section 9.3.2
Adding a 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 serport port protocols dnp setdnp device-table address
```
   Where:
   - *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 7 to 15 characters long or a string 6 to 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, or type **`revert`** and press **Enter** to abort.

Section 9.3.3
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 serport port protocols dnp setdnp device-table address
   ```

   Where:

   - *`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, or type **`revert`** and press **Enter** to abort.

Section 9.4
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.

CONTENTS

- Section 9.4.1, “Understanding Serial Multicast Streaming”
- Section 9.4.2, “Configuring Serial Multicast Streaming”
- Section 9.4.3, “Example: Serial Interfaces Configured as a Sink for Multicast Streams”
- Section 9.4.4, “Example: Serial Interfaces Configured as a Source for Multicast Streams”
- Section 9.4.5, “Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams”

Section 9.4.1

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

CONTENTS

- Section 9.4.1.1, “Sink vs. Source Ports”
- Section 9.4.1.2, “Multicast Streaming Examples”

Section 9.4.1.1

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.

Section 9.4.1.2

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.

Section 9.4.2

Configuring Serial Multicast Streaming

To configure serial multicast streaming, do the following:

1. Add the rawsocket protocol. For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".
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 Section 9.5.2, "Adding a Remote Host" and Section 9.7.2, "Adding a Remote Host Interface".
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 Section 9.6.2, "Adding a Local Host" and Section 9.8.2, "Adding a Local Host Interface".
4. Verify that multicast traffic can be seen on the incoming and outgoing interface(s) by typing:

```
traceserial
```

Section 9.4.3

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.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

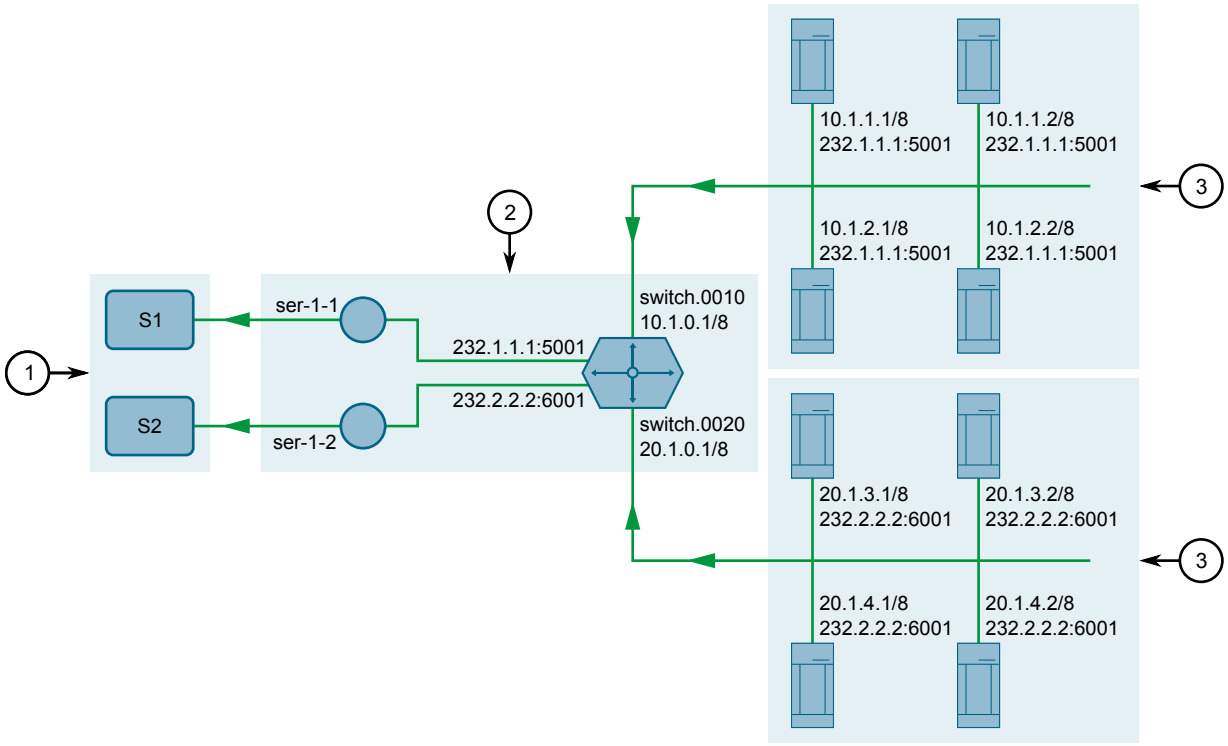


Figure 13: Topology – Serial Interfaces Configured as a Sink for Multicast Streams

1. Serial Devices **2.** Sink Device (RUGGEDCOM RX1400) **3.** Ethernet Network Interfaces

Step 1: Configure ser-1-1

1. Configure IP addresses for the interfaces (switch.0010 and switch.0020). For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".
2. Create a rawsocket connection for ser-1-1:

   ```
   interface serial serport 1 protocols rawsocket
   ```

   For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".
3. Set the rawsocket of the local port to 5001:

   ```
   setrawsocket local-port 5001
   ```

   For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".
4. Set the transport method to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".
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 Section 9.6.2, "Adding a Local Host".
6. Set *switch.0010* as the interface for the local host:

```
interface switch.0010
```

For more information, refer to Section 9.8.2, "Adding a Local Host Interface"

7. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Step 2: Configure ser-1-2

1. Create a raw socket connection for ser-1-2:

```
interface serial serport 2 protocols rawsocket
```

For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".

2. Set the local port for raw socket to 6001:

```
setrawsocket local-port 6001
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

3. Set the transport method for raw socket to *UDP*:

```
setrawsocket transport udp
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

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 Section 9.6.2, "Adding a Local Host".

5. Set *switch.0020* as the interface for the local host:

```
interface switch.0020
```

For more information, refer to Section 9.8.2, "Adding a Local Host Interface"

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 serport 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 serport 2
  no alias
  protocols rawsocket
   setrawsocket local-port 6001
   setrawsocket transport udp
   setrawsocket local-host 232.2.2.2
```

```
    interface switch.0020
```

Section 9.4.4

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.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

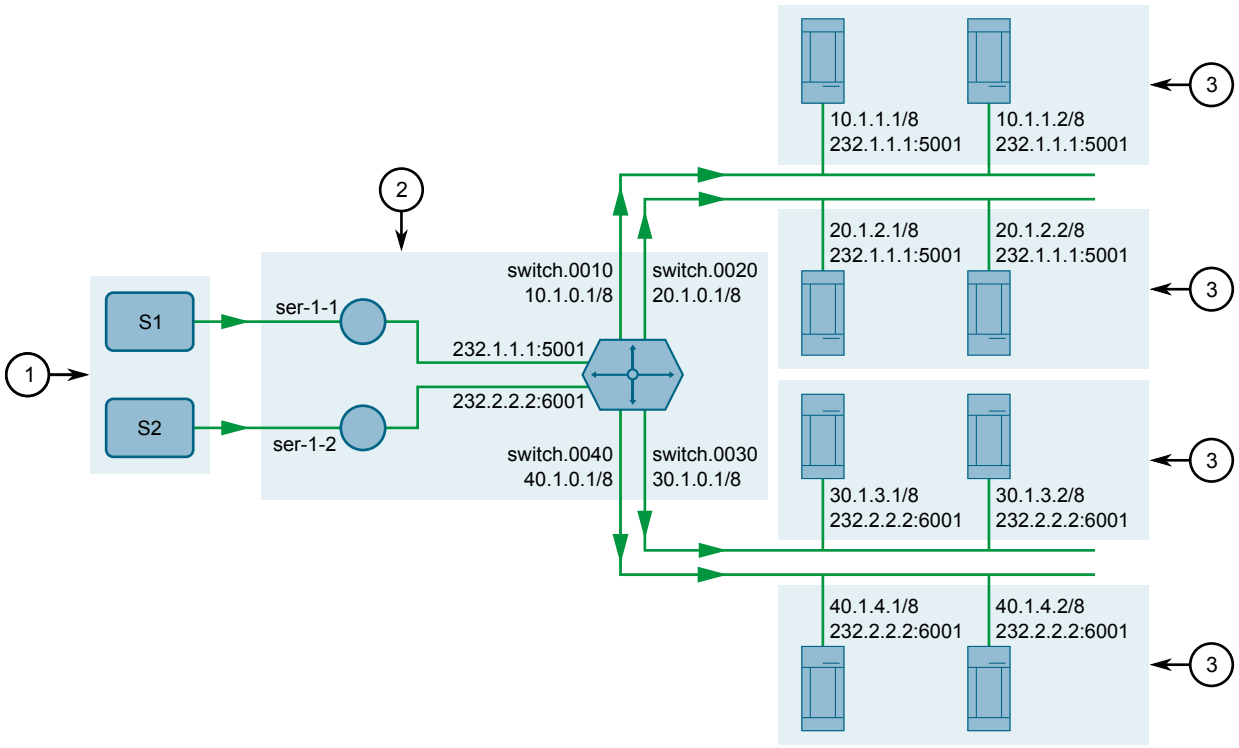


Figure 14: Topology - Serial Interfaces Configured as a Source for Multicast Streams

1. Serial Devices **2.** Source Device (RUGGEDCOM RX1400) **3.** Listeners

» 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 Section 7.1.3.2, "Adding an IPv4 Address".
2. Create a raw socket connection for ser-1-1:

```
interface serial serport 1 protocols rawsocket
```

For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".

3. Set the raw socket of the local port to 10001:

```
setrawsocket local-port 10001
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

4. Set the transport method to *UDP*:

```
setrawsocket transport udp
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

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 Section 9.5.2, "Adding a Remote Host".

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 Section 9.7.2, "Adding a Remote Host Interface"

7. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

» Step 2: Configure ser-1-2

1. Create a raw socket connection for ser-1-2:

```
interface serial serport 2 protocols rawsocket
```

For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".

2. Set the rawsocket of the local port to 10002:

```
setrawsocket local-port 10002
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

3. Set the transport method to *UDP*:

```
setrawsocket transport udp
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

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 Section 9.6.2, "Adding a Local Host".

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 Section 9.7.2, "Adding a Remote Host Interface"

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 serport 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 serport 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
```

Section 9.4.5

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.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

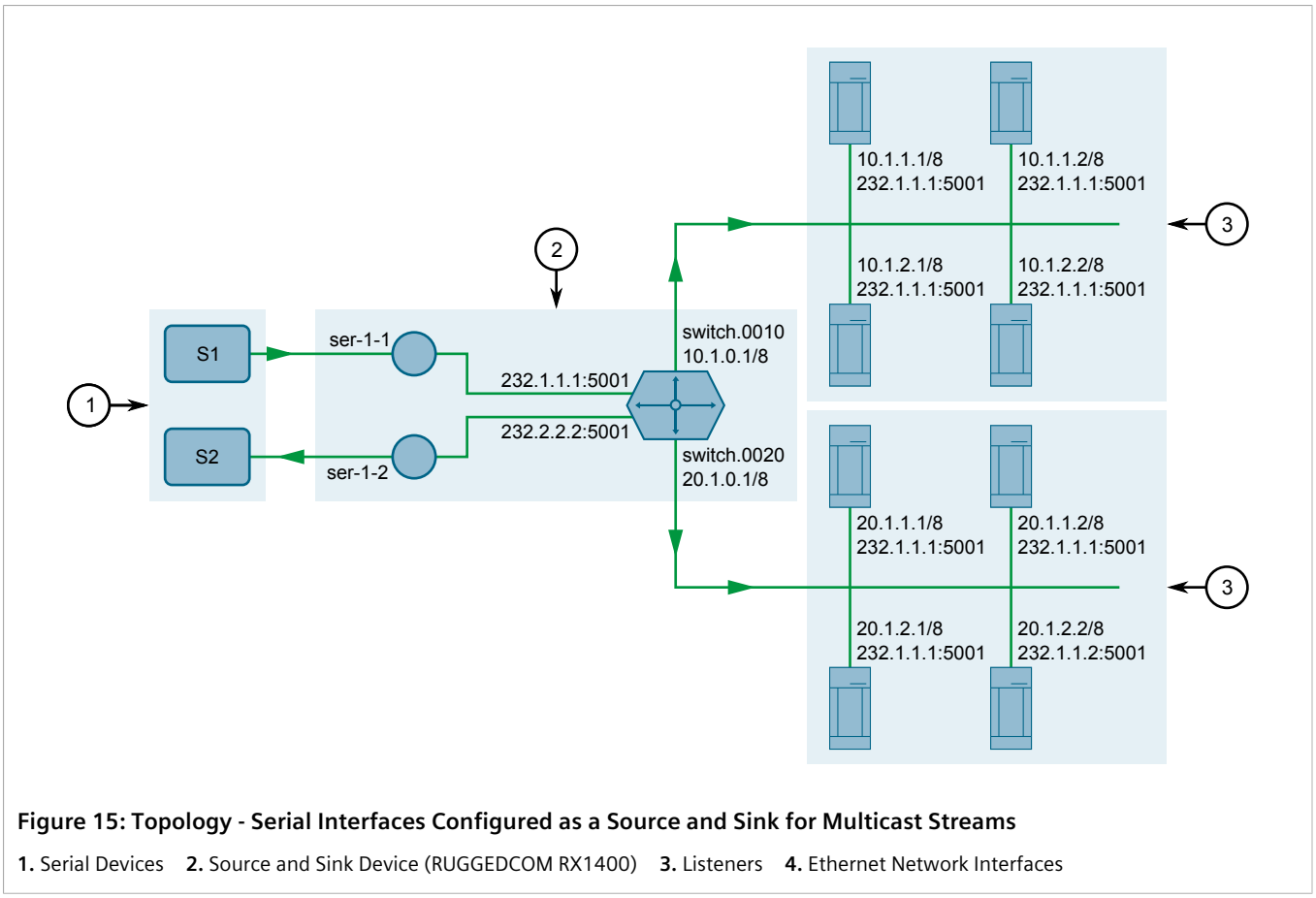


Figure 15: Topology - Serial Interfaces Configured as a Source and Sink for Multicast Streams

1. Serial Devices **2.** Source and Sink Device (RUGGEDCOM RX1400) **3.** Listeners **4.** Ethernet Network Interfaces

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 Section 7.1.3.2, "Adding an IPv4 Address".
2. Create a raw socket connection for ser-1-1:

   ```
   interface serial serport 1 protocols rawsocket
   ```

   For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".
3. Set the raw socket of the local port to 10001:

   ```
   setrawsocket local-port 10001
   ```

   For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".
4. Set the transport method to *UDP*:

   ```
   setrawsocket transport udp
   ```

   For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".
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 Section 9.5.2, "Adding a Remote Host".
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 Section 9.7.2, "Adding a Remote Host Interface"

7. Enable remote host loopback:

```
loopback true
```

For more information, refer to Section 9.6.2, "Adding a Local Host"

8. Create a raw socket connection for ser-1-2:

```
interface serial serport 2 protocols rawsocket
```

For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol"

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 Section 9.6.2, "Adding a Local Host"

10. Set the transport method to *UDP*:

```
setrawsocket transport udp
```

For more information, refer to Section 9.2.6, "Configuring the Raw Socket Protocol".

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 Section 9.6.2, "Adding a Local Host"

12. Enable local host loopback:

```
loopback true
```

For more information, refer to Section 9.6.2, "Adding a Local Host"

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 serport 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 serport 2
  no alias
  protocols rawsocket
   setrawsocket local-port 5001
   setrawsocket transport udp
   setrawsocket local-host 232.1.1.1
    loopback true
```

Section 9.5
Managing Remote Hosts

Remote hosts are required when the UDP transport connection protocol is selected for the raw socket protocol.

CONTENTS

- Section 9.5.1, "Viewing a List of Remote Hosts"
- Section 9.5.2, "Adding a Remote Host"
- Section 9.5.3, "Deleting a Remote Host"

Section 9.5.1
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 setrawsocket 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 serport 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 Section 9.5.2, "Adding a Remote Host".

Section 9.5.2
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 serport port protocols rawsocket setrawsocket remote-host address remote-port
   ```

   Where:

   - *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	**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 Section 9.7.2, "Adding a Remote Host Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 9.5.3
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 serport port protocols rawsocket setrawsocket remote-host address remote-port
   ```

   Where:

   - *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, or type **revert** and press **Enter** to abort.

Section 9.6
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.

CONTENTS

- Section 9.6.1, "Viewing a List of Local Hosts"
- Section 9.6.2, "Adding a Local Host"
- Section 9.6.3, "Deleting a Local Host"

Section 9.6.1
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 setrawsocket 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 serport 1
  protocols rawsocket
   setrawsocket local-host 172.30.151.11 62011
   !
   setrawsocket local-host 172.30.151.22 63000
   !
  !
 !
!
```

If no local hosts have been configured, add hosts as needed. For more information, refer to Section 9.6.2, "Adding a Local Host".

Section 9.6.2
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 serport port protocols rawsocket setrawsocket local-host address
   ```

   Where:

   - *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. 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 Section 9.8.2, "Adding a Local Host Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 9.6.3
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 serport port protocols rawsocket setrawsocket local-host address local-port
   ```

   Where:

   - *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, or type **revert** and press **Enter** to abort.

Section 9.7
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.

CONTENTS

- Section 9.7.1, "Viewing a List of Remote Host Interfaces"
- Section 9.7.2, "Adding a Remote Host Interface"
- Section 9.7.3, "Deleting a Remote Host Interface"

Section 9.7.1
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 serport port protocols rawsocket setrawsocket remote-host remote-host interface
```

Where:

- *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 serport 1 protocols rawsocket setrawsocket remote-host
 224.1.2.1 interface
interface
 serial serport 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 Section 9.7.2, “Adding a Remote Host Interface”.

Section 9.7.2
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 serport port protocols rawsocket setrawsocket remote-host remote-host interface
   ```

   Where:

   - *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 }	**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, or type **revert** and press **Enter** to abort.

Section 9.7.3
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 serport port protocols rawsocket setrawsocket remote-host interface interface name
   ```

   Where:

   - *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, or type **revert** and press **Enter** to abort.

Section 9.8
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.

CONTENTS

- Section 9.8.1, "Viewing a List of Local Host Interfaces"
- Section 9.8.2, "Adding a Local Host Interface"
- Section 9.8.3, "Deleting a Local Host Interface"

Section 9.8.1
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 serport port protocols rawsocket setrawsocket local-host local-host interface
```

Where:

- *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 serport 1 protocols rawsocket setrawsocket local-host
 224.1.2.1 interface
```

```
interface
 serial serport 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 Section 9.8.2, "Adding a Local Host Interface".

Section 9.8.2
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 serport port protocols rawsocket setrawsocket local-host local-host interface
   ```

   Where:

   - *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 }	**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, or type **revert** and press **Enter** to abort.

Section 9.8.3
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 serport port protocols rawsocket setrawsocket local-host interface interface name
   ```

   Where:

- *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, or type **revert** and press **Enter** to abort.

10 Wireless

This chapter describes how to configure and manage the various wireless interfaces and utilities available in RUGGEDCOM ROX II.

NOTE
Some wireless features require the device to be equipped with a specific line module.

CONTENTS

- Section 10.1, "Managing the WLAN Interface"
- Section 10.2, "Managing Cellular Modem Interfaces"
- Section 10.3, "Running AT Commands"
- Section 10.4, "Connecting as a PPP Client"
- Section 10.5, "Managing Cellular Modem Profiles"
- Section 10.6, "Managing the LTE Modem"

Section 10.1

Managing the WLAN Interface

This section describes how to configure an interface to a Wireless Local Area Network (WLAN). The device can be configured as an access point or client.

CONTENTS

- Section 10.1.1, "Enabling and Configuring the WLAN Interface"
- Section 10.1.2, "Managing Wireless Access Points"
- Section 10.1.3, "Managing WLAN Clients"
- Section 10.1.4, "Example: Configuring a WLAN with a Firewall"

Section 10.1.1

Enabling and Configuring the WLAN Interface

To enable and configure the interface to a WLAN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable the WLAN interface by typing:

```
interface wlan wlanport 1 enabled
```

3. Configure the following parameter(s) as required:

IMPORTANT!
The `country` parameter defines the channel (or radio frequency) that can be used by the access point. Some countries restrict the use of certain channels. Make sure the channel selection complies with regional requirements.

NOTE
The `country` parameter is not configurable on devices certified for use only in the United States.

Parameter	Description
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 1 to 64 characters long The SNMP alias name of the interface
name { name }	**Synopsis:** A string 1 to 15 characters long The specific name of the interface
country { country }	**Synopsis:** { Afghanistan, Åland Islands, Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin, Bermuda, Bhutan, Bolivia, Bonaire, Bosnia and Herzegovina, Botswana, Bouvet Island, Brazil, British Indian Ocean Territory, Brunei Darussalam, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Canada, Cape Verde, Cayman Islands, Central African Republic, Chad, Chile, China, Christmas Island, Cocos (Keeling) Islands, Colombia, Comoros, Congo, Cook Islands, Costa Rica, Côte d'Ivoire, Croatia, Cuba, Curaçao, Cyprus, Czech Republic, Denmark, Djibouti, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Falkland Islands (Malvinas), Faroe Islands, Fiji, Finland, France, French Guiana, French Polynesia, French Southern Territories, Gabon, Gambia, Georgia, Germany, Ghana, Gibraltar, Greece, Greenland, Grenada, Guadeloupe, Guam, Guatemala, Guernsey, Guinea, Guinea-Bissau, Guyana, Haiti, Heard Island and McDonald Islands, Holy See (Vatican City State), Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Iran, Iraq, Ireland, Isle of Man, Israel, Italy, Jamaica, Japan, Jersey, Jordan, Kazakhstan, Kenya, Kiribati, Korea, Kuwait, Kyrgyzstan, Lao People's Democratic Republic, Latvia, Lebanon, Lesotho, Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Macao, Macedonia, Madagascar, Malawi, Malaysia, Maldives, Mali, Malta, Marshall Islands, Martinique, Mauritania, Mauritius, Mayotte, Mexico, Micronesia, Moldova, Monaco, Mongolia, Montenegro, Montserrat, Morocco, Mozambique, Myanmar, Namibia, Nauru, Nepal, Netherlands, New Caledonia, New Zealand, Nicaragua, Niger, Nigeria, Niue, Norfolk Island, Northern Mariana Islands, Norway, Oman, Pakistan, Palau, Palestine, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Pitcairn, Poland, Portugal, Puerto Rico, Qatar, Réunion, Romania, Russian Federation, Rwanda, Saint Barthélemy, Saint Helena, Saint Kitts and Nevis, Saint Lucia, Saint Martin (French part), Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Samoa, San Marino, Sao Tome and Principe, Saudi Arabia, Senegal, Serbia, Seychelles, Sierra Leone, Singapore, Sint Maarten (Dutch part), Slovakia, Slovenia, Solomon Islands, Somalia, South Africa, South Georgia and the South Sandwich Islands, South Sudan, Spain, Sri Lanka, Sudan, Suriname, Svalbard and Jan Mayen, Swaziland, Sweden, Switzerland, Syrian Arab Republic, Taiwan, Tajikistan, Tanzania, Thailand, Timor-Leste, Togo, Tokelau, Tonga, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Turks and Caicos Islands, Tuvalu, Uganda, Ukraine, United Arab Emirates, United Kingdom, United States, United States Minor Outlying Islands, Uruguay, Uzbekistan, Vanuatu,

Parameter	Description
	Venezuela, Viet Nam, Virgin Islands, Wallis and Futuna, Western Sahara, Yemen, Zambia, Zimbabwe } **Default:** United States The country the access point and client are operating within.

4. If the device will act as an access point, add one or more Service Set Identifiers or SSIDs. For more information, refer to Section 10.1.2.4, "Adding a Wireless Access Point".
5. If the device will act as a client, add one or more aliases. For more information, refer to Section 10.1.3.3, "Adding a WLAN Client".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.2
Managing Wireless Access Points

This section describes how to configure the device to act as a Wireless Access Point (WAP) in a WLAN.

IMPORTANT!
When the device is to be enabled as a WAP, make sure the WLAN client is disabled.

IMPORTANT!
No more than two WAPs can be enabled at the same time.

CONTENTS

- Section 10.1.2.1, "Viewing a List of Wireless Access Points"
- Section 10.1.2.2, "Viewing the Status of Wireless Access Points"
- Section 10.1.2.3, "Viewing the Status of WLAN Client Associations"
- Section 10.1.2.4, "Adding a Wireless Access Point"
- Section 10.1.2.5, "Configuring WPA-EAP"
- Section 10.1.2.6, "Deleting a Wireless Access Point"

Section 10.1.2.1
Viewing a List of Wireless Access Points

To view a list of Wireless Access Points (WAPs) for a WLAN interface, type:

```
show running-config interface wlan wlanport 1 access-point
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface wlan wlanport 1 access-point ssids | tab
                                          CHANNEL  HT                          WEP
SSID        ENABLED  INTERFACE  BAND    MODE   WIDTH    MODE  CHANNEL  SECURITY   KEY  PASSPHRASE
-------------------------------------------------------------------------------------------------------------
RX1400-Air  X        wlan-ap1   2.4GHz  mixed  -        MIMO  6        wpa2_ccmp  -
 $4$05sxb9ZekzsdprcI0d4IDw==
```

```
RX1400AP    -        -          2.4GHz  mixed  -        MIMO  auto     wpa2_ccmp  -
 $4$05sxb9ZekzsdhYYI0d4IDw==

 !
!
```

If no WAPs have been configured, add WAPs as needed. For more information, refer to Section 10.1.2.4, "Adding a Wireless Access Point".

Section 10.1.2.2
Viewing the Status of Wireless Access Points

To view the status of all Wireless Access Point (WAP), type:

```
show interfaces wlan status access_point
```

If WAPs have been configured, a list similar to the following example appears:

```
ruggedcom# show interfaces wlan status access_point
interfaces wlan status access_point RX1400-Air
 interface     wlan-ap1
 mac           7c:ec:79:c0:8a:81
 mimo          2x2
 state         Enabled
 mode          mixed
 band          "2.4 GHz"
 channel       6
 channel width "20 MHz"
 security      "WPA2 CCMP"
 connected-client
BSSID              RX     TX          SIGNAL
------------------------------------------------
7c:ec:79:c0:93:7c       9643    957975218       -25 dBm
```

The list provides the following information:

Parameter	Description
ssid	**Synopsis:** A string SSID of this WLAN.
interface	**Synopsis:** A string Interface used by this WLAN.
mac	**Synopsis:** A string MAC address of the interface.
mimo	**Synopsis:** A string MIMO configuration of the access point.
state	**Synopsis:** A string State of this access point.
mode	**Synopsis:** A string Mode of this WLAN.
band	**Synopsis:** A string Frequency band of this access point.
channel	**Synopsis:** A string

Parameter	Description
	Channel of this access point.
channel-width	**Synopsis:** A string Width of the channel.
security	**Synopsis:** A string Security mode of this WLAN.

If no WAPs have been configured, configure WAPs as needed. For more information, refer to Section 10.1.2.4, "Adding a Wireless Access Point".

Section 10.1.2.3
Viewing the Status of WLAN Client Associations

To view the status of WLAN clients connected to a specific Wireless Access Point (WAP), type:

```
show interfaces wlan status access_point access-point connected-client
```

Where *access-point* is the desired WAP.

If a client is connected to the WAP, a list similar to the following example appears:

```
ruggedcom# show interfaces wlan status access_point RX1400-Air connected-client
BSSID              RX           TX           SIGNAL
------------------------------------------------------
7c:ec:79:c0:93:7c       1889951798      1216926171      -64 dBm
```

The list provides the following information:

Parameter	Description
bssid	**Synopsis:** A string The BSSID of associated station.
RX	**Synopsis:** A string The number of bytes received from the client.
TX	**Synopsis:** A string The number of bytes transmitted to the client.
signal	**Synopsis:** A string Average signal strength.

Section 10.1.2.4
Adding a Wireless Access Point

To add a Wireless Access Point (WAP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the access point by typing:

   ```
   interface wlan wlanport 1 access-point ssids ssid
   ```

   Where *ssid* is the Service Set Identifier (SSID) for the access point.

IMPORTANT!
No more than two WAPs can be enabled at the same time.

3. Configure the following common parameters by typing:

Parameter	Description
enabled	When selected (checked), enables the the access point.
band { band }	**Synopsis:** { 2.4GHz, 5GHz } **Default:** 2.4GHz The frequency band.
channel { channel }	**Synopsis:** A string 1 to 10 characters long **Default:** auto The channel.
security { security }	**Synopsis:** { wpa_eap, wpa2_ccmp, wpa2_ccmp_wpa_tkip, wpa_ccmp, wpa_tkip_ccmp, wpa_tkip, wep, open } **Default:** wpa2_ccmp_wpa_tkip The security protocol supported by the WLAN.
passphrase { passphrase }	**Synopsis:** A string 1 to 128 characters long The password for the WLAN. The password must be between 8 and 63 characters. It can contain numbers, uppercase and lowercase characters, and special characters (e.g. !@#$%^&*()_+-={}). For improved security, use a password that is at least 12 characters long and contains at least one uppercase character, lowercase character, number, and special character. This parameter is mandatory.

NOTE
The 5.0 GHz frequency band only supports SISO, which can support a channel width of 20 or 40 MHz. The 2.4 GHz frequency band supports both SISO (20 MHz) and MIMO (40 MHz).

4. Depending on the selected frequency band, configure the following additional parameters:

- **For 2.4 GHz**

Parameter	Description
mode { mode }	**Synopsis:** { mixed, b-g-only, b-only, g-only } **Default:** mixed The mode that best matches the clients that will connect to the WLAN.
ht-mode { ht-mode }	**Synopsis:** { SISO, MIMO } **Default:** MIMO The MIMO mode.

- **For 5.0 GHz**

Parameter	Description
channel-width { channel-width }	**Synopsis:** { 20MHz, 40MHz } **Default:** 20MHz The channel width.

5. If *WPA-EAP* is selected as a security protocol, configure WPA-EAP. For more information, refer to Section 10.1.2.5, "Configuring WPA-EAP".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.2.5
Configuring WPA-EAP

RUGGEDCOM ROX II supports IEEE 802.1x authentication. For more information about the Extensible Authentication Protocol (EAP), refer to Section 6.5.1.2, "IEEE 802.1x Authentication".

To configure WPA-EAP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wlan » wlanport/1 » access-point » ssids » {name}***, where *name* is the desired service set identifier.
3. Configure the following parameters:

Parameter	Description
version { version }	**Synopsis:** { wpa, wpa2, wpa_wpa2 } **Default:** wpa2 The version of WPA.
cipher { cipher }	**Synopsis:** { TKIP, CCMP, TKIP_CCMP } **Default:** CCMP The cipher used with WPA.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.2.6
Deleting a Wireless Access Point

To delete a Wireless Access Point (WAP), do the following:

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

```
no interface wlan wlanport 1 access-point ssids ssid
```

   Where *`ssid`* is the Service Set Identifier (SSID) for the access point.
3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.3
Managing WLAN Clients

This section describes how to configure the device to act as a client in the WLAN. This is done by configuring aliases, which are connected to specific access points.

CONTENTS

- Section 10.1.3.1, "Viewing a List of WLAN Clients"
- Section 10.1.3.2, "Viewing the Status of the WLAN Clients"
- Section 10.1.3.3, "Adding a WLAN Client"
- Section 10.1.3.4, "Configuring WPA-EAP Authentication"
- Section 10.1.3.5, "Adding a CA Certificate for WPA-EAP Authentication"

- Section 10.1.3.6, “Deleting a WLAN Client”
- Section 10.1.3.7, “Scanning for WLAN Clients”

Section 10.1.3.1
Viewing a List of WLAN Clients

To view a list of WLAN clients, type:

```
show running-config interface wlan wlanport 1 client wireless-lans
```

```
ruggedcom# show running-config interface wlan wlanport 1 client wireless-lans | tab
                                                                          IP
                                                                          ADDRESS
WLAN ALIAS    ENABLED  SSID SECURITY       PASSWORD                       SRC
-------------------------------------------------------------------------------
WLAN-Client1  X        RX1400AP-Air--WPA2  $4$05sxb9ZekzsdhYYI0d4IDw==  static

 !
!
```

If no WLAN clients have been configured, add clients as needed. For more information, refer to Section 10.1.3.3, “Adding a WLAN Client”.

Section 10.1.3.2
Viewing the Status of the WLAN Clients

To view the status of the WLAN clients, type:

```
show interfaces wlan status link
```

A list similar to the following example appears:

```
ruggedcom# show interfaces wlan status link
interfaces wlan status link
 interface wlan-cl1
 mac       7c:ec:79:c0:93:7c
 state     Enabled
 ssid      RX1400-Air
 frequency 2437
 signal    "-39 dBm"
```

The list provides the following information:

Parameter	Description
interface	**Synopsis:** A string Network interface for this link.
mac	**Synopsis:** A string MAC address of the interface.
state	**Synopsis:** A string State of this link.
ssid	**Synopsis:** A string WLAN this client is connected to.

Parameter	Description
frequency	**Synopsis:** A string Frequency used to communicate with the access point.
signal	**Synopsis:** A string Signal strength.

Section 10.1.3.3
Adding a WLAN Client

To add a WLAN client, do the following:

1. Scan the network for all available WLAN clients. Each client discovered will be made selectable when adding the client. For more information, refer to Section 10.1.3.7, "Scanning for WLAN Clients".
2. Make sure the CLI is in Configuration mode.
3. Add the client by typing:

   ```
   interface wlan wlanport 1 client wireless-lans name
   ```

   Where *name* is the client name.
4. Configure the following parameter(s) as required:

Parameter	Description
enabled	When selected (checked), enables the WLAN alias.
ssid-security { ssid-security }	**Synopsis:** A string The WLAN to connect with. Either select a WLAN from the list or select manual-setup to manually specify a WLAN.
password { password }	**Synopsis:** A string 1 to 32 characters long The password for the WLAN. This parameter is mandatory.
ip-address-src { ip-address-src }	**Synopsis:** { static, dynamic } **Default:** dynamic Determines whether the IP address is static or dynamically assigned via DHCP or BOOTP.
ipv6-address-src { ipv6-address-src }	**Synopsis:** { static, dynamic } **Default:** dynamic Determines whether the IP address is static or dynamically assigned via DHCPv6.

5. If *SSID Security* is set to `manual-setup`, configure the following additional parameter(s) as required:

   IMPORTANT!
   *The WLAN password can contain numbers, uppercase and lowercase characters, and special characters (e.g. *()_+-={}[];:',<.>/?\|`~). For improved security, use a password that is at least 12 characters long and contains at least one uppercase character, lowercase character, number, and special character.*

Parameter	Description
ssid { ssid }	**Synopsis:** A string The SSID for the WLAN.

Parameter	Description
	This parameter is mandatory.
security { security }	**Synopsis:** { wpa_eap, wpa/wpa2, wep, open } **Default:** wpa/wpa2 The security protocol supported by the WLAN.
password { password }	**Synopsis:** A string 1 to 32 characters long The password for the WLAN. This parameter is mandatory.

6. If *WPA-EAP* is selected as a security protocol, configure WPA-EAP authentication. For more information, refer to Section 10.1.3.4, "Configuring WPA-EAP Authentication".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.3.4
Configuring WPA-EAP Authentication

RUGGEDCOM ROX II supports IEEE 802.1x authentication. For more information about the Extensible Authentication Protocol (EAP), refer to Section 6.5.1.2, "IEEE 802.1x Authentication".

To configure WPA-EAP authentication, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wlan » wlanport/1 » client » wireless-lans » {name} » wpa-eap***, where *{name}* is the desired wireless lan.
3. Configure the following parameter(s) as required:

Parameter	Description
version { version }	**Synopsis:** { wpa, wpa2, wpa_wpa2 } WPA version to be used - options are WPA, WPA2 or WPA_WPA2 This parameter is mandatory.
ciphers { ciphers }	**Synopsis:** { TKIP, CCMP, TKIP_CCMP } WPA ciphers to be used - options are TKIP, CCMP or TKIP_CCMP This parameter is mandatory.
authentication-method { authentication-method }	**Synopsis:** { TLS } **Default:** TLS Authentication method for EAP
certificate { certificate }	**Synopsis:** A string Local certificate sent to server for authentication
identity { identity }	**Synopsis:** A string 1 to 64 characters long Identity string sent to server This parameter is mandatory.
server-subject-name { server-subject-name }	**Synopsis:** A string Expected subject name (sub-string match) of the server certificate
server-domain-name-suffix { server-domain-name-suffix }	**Synopsis:** A string

Parameter	Description
	Expected domain name suffix (suffix match) in DNS entries of alternative subject name or common name fields

4. Add a CA certificate for WPA-EAP authentication. For more information, refer to Section 10.1.3.5, "Adding a CA Certificate for WPA-EAP Authentication".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.3.5
Adding a CA Certificate for WPA-EAP Authentication

To add a CA Certificate for WPA-EAP authentication, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wlan » wlanport/1 » client » {wireless-lan} » wpa-eap » Add-ca-cert-list***, where *{wireless-lan)* is the desired wireless lan.

NOTE
If no certificates have been configured, add certificates as needed. Refer to Section 6.7.4.3, "Adding a CA Certificate and CRL".

NOTE
The client CA certificate must match the local certificate. For more information, refer to Section 10.1.3.4, "Configuring WPA-EAP Authentication".

3. Configure the following parameter(s) as required:

Parameter	Description
{ ca-cert }	**Synopsis:** A string The CA Certificate

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.3.6
Deleting a WLAN Client

To delete a WLAN client, do the following:

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

```
no interface wlan wlanport 1 client wireless-lans name
```

Where *`name`* is the client name.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.1.3.7
Scanning for WLAN Clients

Before configuring a WLAN client for a device, use the scan utility to find available WLAN clients in the area. WLAN clients found are selectable when configuring an alias for the client and can also be viewed in the scan results.

To scan for available WLAN clients, do the following:

1. Make sure the WLAN interface is enabled. For more information, refer to Section 10.1.1, "Enabling and Configuring the WLAN Interface".
2. Make sure all existing WLAN clients are disabled. For more information, refer to Section 10.1.3.3, "Adding a WLAN Client".
3. Run the scan utility by typing:

```
interface wlan wlanport 1 scan
```

4. [Optional] Display the scan results by typing:

```
show running-config interface wlan wlanport 1 scan-results
```

For example:

```
show running-config interface wlan wlanport 1 scan-results | tab
WLAN
--------------------
RX1400AP-Air--WPA2
RuggedCom--OPEN
manual-setup

 !
!
```

Section 10.1.4
Example: Configuring a WLAN with a Firewall

This example demonstrates how to link WAN and LAN networks wirelessly while controlling traffic with a firewall.

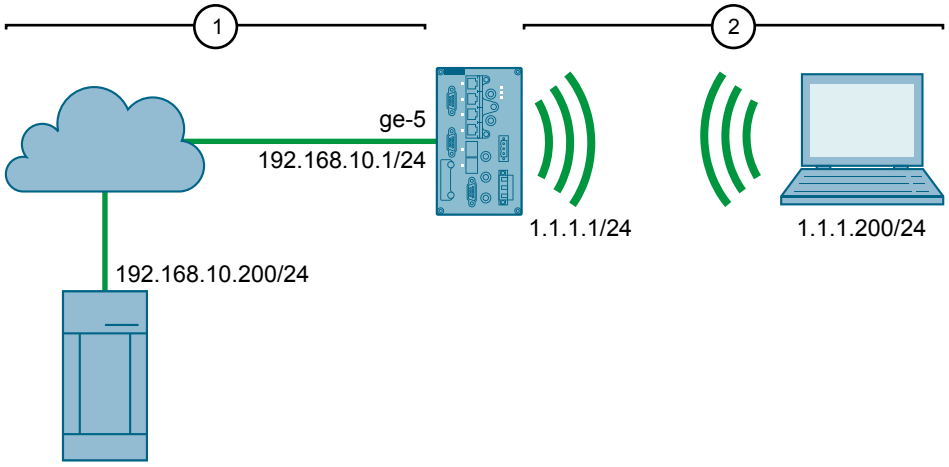


Figure 16: WLAN with Firewall Topology

1. WAN **2.** LAN

Step 1: Connect the WAN and LAN Networks

1. Make sure the WLAN interface is enabled. For more information, refer to Section 10.1.1, "Enabling and Configuring the WLAN Interface".
2. Configure a wireless access point. For more information, refer to Section 10.1.2.4, "Adding a Wireless Access Point".
3. Assign an IPv4 or IPv6 address to the interface associated with the new wireless access point. For more information, refer to either Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
4. Connect the WAN network to an available switched Ethernet port on the device.
5. Configure the port as follows:

Parameter	Value
Switchport	{ disabled }
IP Address Source	static

For more information about configuring a port, refer to Section 8.1.2, "Configuring a Switched Ethernet Port".

NOTE
*When a switched Ethernet port is in direct routing mode (versus switch mode), an interface in the form of **ge-{port}** is added automatically to the **ip** menu. For example, if direct routing mode is configured for port 5, the interface **ge-5** is created.*

6. Assign an IPv4 or IPv6 address to the switched Ethernet port connected to the WAN side of the network. For more information, refer to either Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
7. For each PC on the WAN side of the network, do the following:
   a. Configure an IP address that is on the same subnet as the IP address configured for the switched Ethernet port. For example:

Router IP Address	192.168.10.1/24
PC IP Address	192.168.10.200/24

This step is operating system specific. For more information, refer to the user documentation for the OS.

b. Add a static route. For example, on Linux® PCs:

```
# route add 1.1.1.1 mask 255.255.255.0 192.168.10.0
```

For information about how to add static routes for other operating systems, refer to the user documentation for the OS.

8. For each PC on the LAN side of the network, do the following:

a. Configure an IP address and default gateway that are on the same subnet as the IP address configured for the access point. For example:

Router IP Address	1.1.1.1/24
PC IP Address	1.1.1.200/24
PC Default Gateway	1.1.1.1

This step is operating system specific. For more information, refer to the user documentation for the OS.

b. Add a static route. For example, on Linux® PCs:

```
# route add 192.168.10.0 mask 255.255.255.0 1.1.1.1
```

For information about how to add static routes for other operating systems, refer to the user documentation for the OS.

c. Connect the PC to the access point and assign the PC's wireless interface an IP address on the same subnet (e.g. 1.1.1.200/24).

9. Click **Commit**.

10. Verify the WAN and LAN networks are connected via the router by sending pings between PCs.

For example, `1.1.1.200/24` should be able to ping `192.168.10.200/24`, and `192.168.10.200/24` should be able to ping `1.1.1.200/24`.

Step 2: Configure the Firewall

1. Add a new firewall (e.g. WLAN-Firewall). For more information, refer to Section 6.8.3, "Adding a Firewall".

2. Configure a zone for each side of the network, as well as a zone for the firewall itself. For example:

Zone Name	IP Type	Type
WAN	ipv4	ipv4
LAN	ipv4	ipv4
FW	ipv4	firewall

For information about how to add zones, refer to Section 6.8.9.2, "Adding a Zone".

3. Add interfaces for the switched Ethernet port, access point, and the device itself. Make sure the switched Ethernet port is associated with the WAN zone and that other interfaces are associated with the LAN zone. For example:

Interface	Predefined Zone
ge-5	WAN
wlan-ap1	LAN
switch.0001	LAN

For information about adding an interface and associating it with a predefined zone, refer to Section 6.8.10.2, "Adding an Interface" and Section 6.8.10.3, "Associating an Interface with a Zone".

4. Add policies to control the flow of traffic between networks. For example:

Name	Source Zone	Destination Zone	Policy
Policy1	WAN	LAN	reject
Policy2	WAN	FW	accept
Policy3	LAN	WAN	accept
Policy4	LAN	FW	accept
Policy5	FW	LAN	accept
Policy6	FW	WAN	accept

For more information about adding policies, refer to Section 6.8.12.2, "Adding a Policy".

5. Validate the firewall configuration. For more information, refer to Section 6.8.16, "Validating a Firewall Configuration".
6. Enable the firewall. For more information, refer to Section 6.8.17, "Enabling/Disabling a Firewall".
7. Select the new firewall as the working configuration. For more information, refer to Section 6.8.5, "Working with Multiple Firewall Configurations".
8. Click **Commit**.
9. Verify the WAN and LAN networks are connected via the router by sending pings between PCs.

   For example, `1.1.1.200/24` should be able to ping `192.168.10.200/24`, but `192.168.10.200/24` should not be able to ping `1.1.1.200/24`.

Section 10.2

Managing Cellular Modem Interfaces

This section describes how to configure an interface to a 4G LTE cellular network, as well as how to enable the device's GPS capabilities.

CONTENTS

- Section 10.2.1, "Enabling/Disabling Cellular Modem Interfaces"
- Section 10.2.2, "Configuring a Cellular Modem Interface"
- Section 10.2.3, "Activating Dual SIM Cards"
- Section 10.2.4, "Viewing a List of Cellular Modem Interfaces"
- Section 10.2.5, "Viewing the Status of a Cellular Modem Interface"

- Section 10.2.6, "Viewing PPP Interface Statistics"

Section 10.2.1
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 » cellmodem » {interface}***, where *{interface}* is the cellular modem interface.
3. Enable or disable the desired cellular modem interface by typing:

   Enable

   ```
   interface wan interface enabled
   ```

   Where *interface* is the cellular modem interface.

   Disable

   ```
   no interface wan 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 Section 10.2.2, "Configuring a Cellular Modem Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 10.2.2
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 » cellmodem » {interface}***, where *{interface}* is the cellular modem interface.
3. Configure the following parameter(s) as required:

Parameter	Description
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 1 to 64 characters long The SNMP alias name of the interface

4. [Optional] Enable the interface. For more information, refer to Section 10.2.1, "Enabling/Disabling Cellular Modem Interfaces".
5. Enable and configure LTE on the interface. For more information, refer to Section 10.6, "Managing the LTE Modem".
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 10.2.3
Activating Dual SIM Cards

The RUGGEDCOM RX1400 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 *RUGGEDCOM RX1400 Installation Guide*.
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 Section 10.5.2, "Adding a GSM Profile".
3. Configure the cellular modem interface to connect to the cellular network via the primary profile. For more information, refer to Section 10.4, "Connecting as a PPP Client".

Section 10.2.4
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 celport 1
  enabled
  no alias
  lte ppp-client connect-to profile1
 !
!
```

Section 10.2.5
Viewing the Status of a Cellular Modem Interface

To view the status of a cellular modem interface, type:

```
show interfaces cellmodem port lte
```

Where:

- *port* is the port number for the module

A table or list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem cel-1 cdma
                NETWORK                RSSI        NETWORK   NETWORK   NETWORK   PHONE
IFNAME    TYPE  SUPPORTED  ESN  ECIO   INDICATOR   OPERATOR  IN USE    STATUS    NUMBER
-------------------------------------------------------------------------------------
cel-1     cdma                  0      0                              Unknown
```

This table or list provides the following information:

Parameter	Description
state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's link status. This parameter is mandatory.
media	**Synopsis:** A string 1 to 31 characters long The wireless data communication technology that modem is compatible with{ GSM/HSPA, CDMA/EVDO, LTE }. This parameter is mandatory.
admin-state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status. This parameter is mandatory.

Section 10.2.6
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:

```
interfaces cellmodem cel-1 lte
 ppp-connections
  connection status Disconnected
  local ip          25.77.204.53
  remote ip         25.70.48.89
  apn               SP.TELUS.COM
  username          N/A
  tx bytes          0
  rx bytes          0
  mtu               1500
```

This table or list provides the following information:

Parameter	Description
connection-status	**Synopsis:** A string 1 to 128 characters long PPP connection status This parameter is mandatory.
local-ip	**Synopsis:** A string 1 to 32 characters long The IP address assigned to the modem by the remote server This parameter is mandatory.
remote-ip	**Synopsis:** A string 1 to 32 characters long The IP address of the remote server This parameter is mandatory.
apn	**Synopsis:** A string The name of the wireless network access point.
username	**Synopsis:** A string **Default:** N/A

Parameter	Description
	The user ID to connect to the remote server.
tx-bytes	**Synopsis:** A 32-bit unsigned integer The bytes transmitted over the modem This parameter is mandatory.
rx-bytes	**Synopsis:** A 32-bit unsigned integer The bytes received by the modem This parameter is mandatory.
mtu	**Synopsis:** A 32-bit unsigned integer MTU (Maximum Transmission Unit) value on the ppp interface This parameter is mandatory.

Section 10.3
Running AT Commands

To issue AT (Hayes) commands to the cellular modem, type:

```
interfaces cellmodem cel-1 lte at command command
```

Where *command* is the AT command.

Section 10.4
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 Section 10.2.2, "Configuring a Cellular Modem Interface".
3. Make sure an appropriate cellular modem profile has been configured. For more information, refer to Section 10.5, "Managing Cellular Modem Profiles".
4. Make sure an account has been activated with a service provider for the modem type.
5. Make sure antennas are properly connected to the device before initiating the connection. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
6. Insert a SIM card into the cellular modem module.
7. Select the cellular modem profile to use when connecting to the wireless network by typing:

   ```
   interface cellmodem celport 1 lte ppp-client connect-to profile
   ```

   Where:

   - *profile* is the cellular modem profile.
8. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 10.5

Managing Cellular Modem Profiles

GSM (Global System for Mobile Communications) profiles must be configured before HSPA data is available.

CONTENTS

- Section 10.5.1, "Viewing a List of GSM Profiles"
- Section 10.5.2, "Adding a GSM Profile"
- Section 10.5.3, "Deleting a GSM Profile"

Section 10.5.1

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     DEMAND
   MTU   AUTHENTICATION
-----------------------------------------------------------------------------------------------------
gsm1  apn.gsm2.net  ipv4  *99***1#  1    -        -     N/A       N/A       -       0           -
   1500  none
gsm2  apn.gsm2.net  ipv4  *99***1#  2    gsm1     -     N/A       N/A       -       0           -
   1500  none

!
```

If no GSM profiles have been configured, add profiles as needed. For more information, refer to Section 10.5.2, "Adding a GSM Profile".

Section 10.5.2

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:

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:** A 32-bit signed integer between 1 and 2 **Default:** 1 Specify SIM index to be used by this profile
peer { peer }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 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 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 **Default:** N/A The password to be authenticated by the remote server.
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:** A 32-bit signed 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:** A 32-bit signed integer between 128 and 1500 **Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP interface.
authentication { authentication }	**Synopsis:** { none, chap, pap } **Default:** none

Parameter	Description
	The authentication protocol used to establish a cellular data link

6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 10.5.3
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, or type **revert** and press **Enter** to abort.

Section 10.6
Managing the LTE Modem

This section describes how to manage the LTE modem.

CONTENTS

- Section 10.6.1, "Viewing LTE Cellular Modem Information"
- Section 10.6.2, "Configuring the LTE Modem"
- Section 10.6.3, "Enabling/Disabling the LTE Modem"
- Section 10.6.4, "Resetting the Cellular Modem"
- Section 10.6.5, "Enabling/Disabling GPS"
- Section 10.6.6, "Viewing the Configured GPS Mode"
- Section 10.6.7, "Enabling and Configuring GPS NMEA Data Streams"
- Section 10.6.8, "Changing the Active SIM Card"
- Section 10.6.9, "Managing Firmware Updates"

Section 10.6.1
Viewing LTE Cellular Modem Information

To view information about the LTE cellular modem, type the following:

```
show interfaces cellmodem cel-1 lte
```

A list similar to the following appears:

```
interfaces cellmodem cel-1 lte
 lte
  network supported "umts,lte"
  imei              35437509018059
  radio             on
  rssi indicator    -73
  network operator  "TELUS"
  network in use    "lte"
  network status    "Registered to Home network"
  sim               8912230100043535630(Sim1)
  active profile    telus1
  ber               2
  imsi              302220023252658
  msisdn            "16472960957"
  mcc               "302"
  mnc               "220"
  gps
   mode standalone
```

This table or list provides the following information:

Parameter	Description
network-supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.
imei	**Synopsis:** A string 1 to 128 characters long International Mobile Equipment Indentity This parameter is mandatory.
radio	**Synopsis:** A string 1 to 128 characters long The current RF status of cellmodem This parameter is mandatory.
rssi-indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
network-operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
network-in-use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.
network-status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
sim	**Synopsis:** A string 1 to 128 characters long The Subscriber Indentity Module number This parameter is mandatory.
active-profile	**Synopsis:** A string 1 to 128 characters long The active profile of cellular connection This parameter is mandatory.

Parameter	Description
ber	**Synopsis:** A string 1 to 128 characters long The percentage at which errors occur in the transmission of digital data.
imsi	**Synopsis:** A string 1 to 128 characters long The unique identifier of a cellular network user.
msisdn	**Synopsis:** A string 1 to 128 characters long The identity of a mobile phone number, internationally.
mcc	**Synopsis:** A string 1 to 128 characters long The country to which a mobile subscriber belongs.
mnc	**Synopsis:** A string 1 to 128 characters long A two or three digit number used to uniquely identify a given network from within a specified country.

Section 10.6.2
Configuring the LTE Modem

To configure the LTE modem, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable the LTE modem. For more information, refer to Section 10.6.3, "Enabling/Disabling the LTE Modem".
3. Navigate to ***interface » cellmodem » celport/1 » lte***.
4. Configure the following parameter(s) as required:

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:** A 32-bit signed integer between 0 and 65535 **Default:** 0 Specify the maximum number of SIM card failover retries. 0 means re-try forever
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:** A 32-bit signed integer between 1 and 10 **Default:** 2 The time in minutes before initiating SIM card failover.
ipv4-address { ipv4-address }	**Synopsis:** A string 7 to 15 characters long The IPv4 address used for sending pings to test connectivity.
ip-polling-interval { ip-polling-interval }	**Synopsis:** A 32-bit signed integer between 5 and 65535

Parameter	Description
	Default: 60 The time in seconds between each ping message sent to the remote host.
ip-polling-resp-timeout { ip-polling-resp-timeout }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed 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, or type **`revert`** and press **Enter** to abort.
6. [Optional] Enable GPS. For more information, refer to Section 10.6.5, "Enabling/Disabling GPS".

Section 10.6.3
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 Section 10.2.1, "Enabling/Disabling Cellular Modem Interfaces".

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the LTE modem by typing:

   Enable

   ```
   interface cellmodem celport 1 lte
   ```

   Disable

   ```
   no interface cellmodem celport 1 lte
   ```

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 10.6.4
Resetting the Cellular Modem

To reset a cellular modem, type:

```
interfaces cellmodem cel-1 lte reset
```

Where:

Section 10.6.5
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 1 lte gps enabled
   ```

   Disabling GPS

   ```
   no interface cellmodem celport 1 lte gps enabled
   ```
3. [Optional] Enable or disable NMEA GPS data streams. For more information, refer to Section 10.6.7, "Enabling and Configuring GPS NMEA Data Streams".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 10.6.6
Viewing the Configured GPS Mode

To view the configured GPS mode for the interface, type the following:

```
show interfaces cellmodem cel-1 lte gps
```

A list similar to the following appears:

```
IFNAME  TYPE  MODE
-------------------------
cel-1   lte   standalone
```

This table or list provides the following information:

Parameter	Description
mode	**Synopsis:** A string 1 to 64 characters long Shows configured GPS mode

Section 10.6.7
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 celport 1 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:** A 16-bit unsigned 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:** A 32-bit signed 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, or type **revert** and press **Enter** to abort.

Section 10.6.8

Changing the Active SIM Card

When dual SIM cards are installed, the SIM card in Slot 1 is the primary (or active) card by default. The card in Slot 2 is considered the backup should the primary card lose connectivity with the network.

To manually switch which card is the active SIM card, do the following:

1. Switch the SIM cards by typing:

```
interfaces cellmodem cel-1 lte force-switch-profile
```

2. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

To verify the SIM cards were successfully switched, type:

```
show interfaces cellmodem cel-1 lte
```

A list similar to the following appears:

```
ruggedcom# show interfaces cellmodem cel-1 lte
interfaces cellmodem cel-1 lte
 lte
  network supported GSM,GPRS,EDGE,UMTS,HSDPA/HSUPA,HSPA+,LTE
  imei              359225052306750
  radio             on
  rssi indicator    -73
  network operator  TELUS
  network in use    LTE
  network status    "Registered to Home network"
  sim               8912230100043535630(Sim1)
```

```
  active profile    Profile2
  gps
   mode standalone
```

The currently active SIM card is listed under **active profile**.

Section 10.6.9
Managing Firmware Updates

Firmware for the LTE modem can be upgraded either directly via microSD/microSDHC flash drive or wirelessly via a remote HTTP/HTTPS server.

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 microSD/microSDHC 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

CONTENTS

- Section 10.6.9.1, “Viewing the Firmware Update Status”
- Section 10.6.9.2, “Configuring the Firmware Update Mode and Source”
- Section 10.6.9.3, “Launching a Firmware Update”

Section 10.6.9.1
Viewing the Firmware Update Status

To view the status of the firmware update, type:

```
show interfaces cellmodem cel-1 firmware-update
```

Where:

- *interface* is the cellular modem interface.

This table displays the following information:

Parameter	Description
current-version	**Synopsis:** A string 1 to 64 characters long The current firmware revision This parameter is mandatory.
status-message	**Synopsis:** A string 1 to 128 characters long Additional details on the status of the update.
last-update-attempt	**Synopsis:** A string 1 to 64 characters long

Parameter	Description
	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

Section 10.6.9.2
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 microSD/microSDHC flash drive.

To upgrade the firmware update mode and source, do the following:

1. Make sure the upgrade server is configured and the latest firmware version has been added. For more information, refer to Section 4.15.2, "Setting Up an Upgrade Server".
2. Make sure a cellular modem interface is enabled. For more information, refer to Section 10.2.2, "Configuring a Cellular Modem Interface".
3. Make sure the CLI is in Configuration mode.
4. Navigate to ***interface » cellmodem » {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 1 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 1 to 64 characters long The user name required to connect with the upgrade server.
password { password }	**Synopsis:** A string 1 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:** A 16-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 10.6.9.3
Launching a Firmware Update

To manually launch a firmware update, do the following:

NOTE
If the upgrade fails, refer to Section 19.5, "Firmware Updates".

1. Make sure the firmware update mode has been configured. For more information, refer to Section 10.6.9.2, "Configuring the Firmware Update Mode and Source".
2. If updating the device via USB/Mico SD, insert the storage media in the device.
3. Launch the firmware update by typing:

   ```
   interfaces cellmodem interface firmware-update
   ```

   Where:

   - *interface* is the cellular modem interface.

11 Tunneling and VPNs

This chapter describes how to configure various tunnels and Virtual Private Networks (VPNs).

CONTENTS

- Section 11.1, “Managing Virtual Switches”
- Section 11.2, “Managing the Layer2 Tunnel Daemon”
- Section 11.3, “Managing L2TP Tunnels”
- Section 11.4, “Managing L2TPv3 Tunnels”
- Section 11.5, “Managing GOOSE Tunnels”
- Section 11.6, “Managing Generic Tunnels”
- Section 11.7, “Managing Generic Routing Encapsulation Tunnels”
- Section 11.8, “Managing IPsec Tunnels”
- Section 11.9, “Managing 6in4 and 4in6 Tunnels”
- Section 11.10, “Managing DMVPN”

Section 11.1

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. 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.

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. cel1 or switch.0001), 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 switch.0001 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 Section 6.8.10, "Managing Interfaces".

CONTENTS

- Section 11.1.1, "Viewing a List of Virtual Switches"
- Section 11.1.2, "Adding a Virtual Switch"
- Section 11.1.3, "Deleting a Virtual Switch"
- Section 11.1.4, "Managing Virtual Switch Interfaces"
- Section 11.1.5, "Filtering Virtual Switch Traffic"
- Section 11.1.6, "Managing Filtering Rules"
- Section 11.1.7, "Managing In/Out Interfaces"
- Section 11.1.8, "Managing VLANs for Virtual Switches"

Section 11.1.1

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 Section 11.1.2, "Adding a Virtual Switch".

Section 11.1.2
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	**Synopsis:** { true, false } **Default:** true Enables this interface.
retain-ip	**Synopsis:** { true, false } **Default:** false Retain IP on bridge device.
forward-delay { forward-delay }	**Synopsis:** An 8-bit unsigned integer **Default:** 15 Delay (in seconds) of the listening and learning state before goes to forwarding state.
alias { alias }	**Synopsis:** A string 1 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 Section 11.1.4.2, "Adding a Virtual Switch Interface".
5. If *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 Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
6. [Optional] Assign one or more VLANs to the virtual switch. For more information, refer to Section 11.1.8.2, "Adding a Virtual Switch VLAN".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.1.3
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, or type **revert** and press **Enter** to abort.

Section 11.1.4
Managing Virtual Switch Interfaces

This section describes how to configure and manage interfaces for virtual switches.

CONTENTS

- Section 11.1.4.1, "Viewing a List of Virtual Switch Interfaces"
- Section 11.1.4.2, "Adding a Virtual Switch Interface"
- Section 11.1.4.3, "Deleting a Virtual Switch Interface"

Section 11.1.4.1
Viewing a List of Virtual Switch Interfaces

To view a list of virtual switch interfaces, type:

```
show running-config interface virtualswitch name interface
```

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


 !
!
```

If no virtual switch interfaces have been configured, add interfaces as needed. For more information, refer to Section 11.1.4.2, "Adding a Virtual Switch Interface".

Section 11.1.4.2
Adding a Virtual Switch Interface

To add a virtual switch interface, do the following:

IMPORTANT!
At least two interfaces are required for a virtual switch bridge.

CAUTION!
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 Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
4. If necessary, add one or more VLANs to the virtual switch interface. For more information, refer to Section 11.1.8.2, "Adding a Virtual Switch VLAN".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.1.4.3
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 interface
   ```

   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, or type **revert** and press **Enter** to abort.

Section 11.1.5
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.

CONTENTS

- Section 11.1.5.1, "Enabling/Disabling Virtual Switch Filtering"
- Section 11.1.5.2, "Viewing a List of Virtual Switch Filters"
- Section 11.1.5.3, "Adding a Virtual Switch Filter"
- Section 11.1.5.4, "Deleting a Virtual Switch Filter"

Section 11.1.5.1
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 Section 11.1.2, "Adding a Virtual Switch".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.1.5.2
Viewing a List of Virtual Switch Filters

To view a list of virtual switch filters, type:

```
show running-config security virtualswitch-filter virtualswitch
```

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 Section 11.1.5.3, "Adding a Virtual Switch Filter".

Section 11.1.5.3
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 Section 11.1.2, "Adding a Virtual Switch".
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 Section 11.1.6.3, "Adding a Rule".
5. Add the desired rules to the virtual switch filter. For more information, refer to Section 11.1.6.4, "Adding a Rule to a Virtual Switch Filter".
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.1.5.4
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, or type **revert** and press **Enter** to abort.

Section 11.1.6
Managing Filtering Rules

A virtual switch filter can apply one or more rules to traffic traversing a virtual switch.

CONTENTS

- Section 11.1.6.1, "Viewing a List of Rules"
- Section 11.1.6.2, "Viewing a List of Rules Assigned to a Virtual Switch Filter"
- Section 11.1.6.3, "Adding a Rule"
- Section 11.1.6.4, "Adding a Rule to a Virtual Switch Filter"
- Section 11.1.6.5, "Deleting a Rule"
- Section 11.1.6.6, "Deleting a Rule from a Virtual Switch Filter"

Section 11.1.6.1
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 Section 11.1.6.3, "Adding a Rule".

Section 11.1.6.2
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 virtualswitch 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 Section 11.1.6.4, "Adding a Rule to a Virtual Switch Filter".

Section 11.1.6.3

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 Section 11.1.2, "Adding a Virtual Switch".
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 17 characters long The required source MAC address for incoming frames.
dstmac { dstmac }	**Synopsis:** A string 17 characters long The required destination MAC address for incoming frames.
proto { proto }	**Synopsis:** { iso, arp, ipv4, ipv6 } or a string The pre-defined protocol or hex-string (i.e. 0x88A2) used to create the frames.

Parameter	Description
	This parameter is mandatory.

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.
6. Add the rule to a virtual switch filter. For more information, refer to Section 11.1.6.4, "Adding a Rule to a Virtual Switch Filter".

Section 11.1.6.4
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 Section 11.1.7.2, "Adding an In/Out Interface".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.1.6.5
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, or type **revert** and press **Enter** to abort.

Section 11.1.6.6
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, or type **revert** and press **Enter** to abort.

Section 11.1.7
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.

CONTENTS

- Section 11.1.7.1, "Viewing a List of In/Out Interfaces"
- Section 11.1.7.2, "Adding an In/Out Interface"
- Section 11.1.7.3, "Deleting an In/Out Interface"

Section 11.1.7.1
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 virtualswitch name rule rule [ in-interface | out-interface ]
```

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 Section 11.1.7.2, "Adding an In/Out Interface".

Section 11.1.7.2
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, or type **revert** and press **Enter** to abort.

Section 11.1.7.3
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 ]
   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, or type **revert** and press **Enter** to abort.

Section 11.1.8
Managing VLANs for Virtual Switches

This section describes how to configure and manage VLANs for virtual switches.

CONTENTS

- Section 11.1.8.1, “Viewing a List of Virtual Switch VLANs”
- Section 11.1.8.2, “Adding a Virtual Switch VLAN”
- Section 11.1.8.3, “Deleting a Virtual Switch VLAN”

Section 11.1.8.1
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 Section 11.1.8.2, "Adding a Virtual Switch VLAN".

Section 11.1.8.2
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 Section 15.2.7.2, "Adding a QoS Map".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.1.8.3
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, or type **revert** and press **Enter** to abort.

Section 11.2
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.

CONTENTS

- Section 11.2.1, "Viewing Round Trip Time Statistics"
- Section 11.2.2, "Configuring the Layer 2 Tunnel Daemon"

Section 11.2.1
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 Section 11.6.5, "Managing Remote Daemon IP Addresses for Generic Tunnels".

```
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
remote-ip	**Synopsis:** A string 7 to 15 characters long The IP address of remote daemon. This parameter is mandatory.
transmitted	**Synopsis:** A 32-bit unsigned integer The number of beacon frames transmitted through the tunnel. This parameter is mandatory.
received	**Synopsis:** A 32-bit unsigned integer The number of beacon frames received through the tunnel. This parameter is mandatory.
minimum-rtt	**Synopsis:** A string 1 to 32 characters long The Minimum Beacon Round-Trip-Time. This parameter is mandatory.
average-rtt	**Synopsis:** A string 1 to 32 characters long The Average Beacon Round-Trip-Time. This parameter is mandatory.
maximum-rtt	**Synopsis:** A string 1 to 32 characters long The Maximum Beacon Round-Trip-Time. This parameter is mandatory.
deviation	**Synopsis:** A string 1 to 32 characters long The standard deviation. This parameter is mandatory.

Section 11.2.2
Configuring the Layer 2 Tunnel Daemon

To configure the Layer 2 tunnel daemon, do the following:

IMPORTANT!
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:** A 32-bit signed integer between 1 and 65535 **Default:** 1311 The UDP port to communicate with the other daemon.

Parameter	Description
beacon-interval { beacon-interval }	**Synopsis:** { off } or a 32-bit signed integer between 10 and 3600 **Default:** 60 The Round Trip Time (RTT) of the sent message

3. Add GOOSE or generic tunnels as required. For more information, refer to Section 11.5.3, "Adding a GOOSE Tunnel" or Section 11.6.3, "Adding a Generic Tunnel".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.3
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.

IMPORTANT!
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.

CONTENTS

- Section 11.3.1, "Configuring L2TP Tunnels"
- Section 11.3.2, "Configuring DNS Servers"
- Section 11.3.3, "Configuring PPP Options"
- Section 11.3.4, "Configuring WINS Servers"

Section 11.3.1
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 7 to 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 7 to 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.

Parameter	Description
max-connection { max-connection }	**Synopsis:** A 32-bit unsigned integer between 1 and 10 The maximum number of connections.
closing-wait-timeout { closing-wait-timeout }	**Synopsis:** A 32-bit unsigned 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 Section 11.3.2, "Configuring DNS Servers" or Section 11.3.4, "Configuring WINS Servers".
4. Configure L2TP tunnels to carry Point-to-Point Protocol (PPP) sessions. For more information, refer to Section 11.3.3, "Configuring PPP Options".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.3.2
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, or type **`revert`** and press **Enter** to abort.

Section 11.3.3
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 Section 6.6.3.2, "Configuring RADIUS Authentication for PPP Services".*

Parameter	Description
auth-local	Authorizes locally instead of using radius server.
mtu { mtu }	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1410

Parameter	Description
	The Maximum Transmit Unit (MTU) or maximum packet size transmitted.
mru { mru }	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1410 The Maximum Receive Unit (MRU) or maximum packet size passed when received.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.3.4
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, or type **revert** and press **Enter** to abort.

Section 11.4
Managing L2TPv3 Tunnels

L2TPv3 (Layer 2 Tunneling Protocol Version 3) provides a pseudo-wire service that encapsulates multi-protocol Layer 2 traffic over IP networks. There are no restrictions on the Layer 2 data formats that can be transmitted or received, unlike L2TP.

L2TPv3 is a simplified alternative to MPLS (Multiprotocol Label Switching) that offers improved performance (e.g. high data packet rate and low CPU consumption) over L2TP and IP networks.

Two types of L2TPv3 tunnels are available:

- **Static**
  A static L2TPv3 tunnel is a fixed connection between two Provider Edge devices (PE), where the session IDs and cookies are defined on both devices. This allows the devices to route Layer 2 traffic as soon as the session connects with the attachment circuit.
- **Dynamic**
  A dynamic 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.

IMPORTANT!
RUGGEDCOM ROX II supports a maximum of 128 tunnel sessions, which in turn support a maximum of 128 VLANs each.

CONTENTS

- Section 11.4.1, "L2TPv3 Tunnel Scenarios"
- Section 11.4.2, "Creating an L2TPv3 Tunnel"
- Section 11.4.3, "Managing Static L2TPv3 Tunnels"
- Section 11.4.4, "Managing Dynamic L2TPv3 Tunnels"
- Section 11.4.5, "Managing Sessions for L2TPv3 Tunnels"
- Section 11.4.6, "Managing VLANs for L2TPv3 Tunnels"

Section 11.4.1

L2TPv3 Tunnel Scenarios

The following illustrates some of the ways in which L2TPv3 tunnels can be implemented.

Basic L2TPv3 Tunnel

In the following topology, an L2TPv3 tunnel is established between routers R1 and R2 over a WAN interface. The tunnel interface is assigned an IPv4 address on both devices. Traffic routed from R1 is encapsulated in an L2TPv3 header and decapsulated by R2. The reverse is true when traffic is routed from R2.

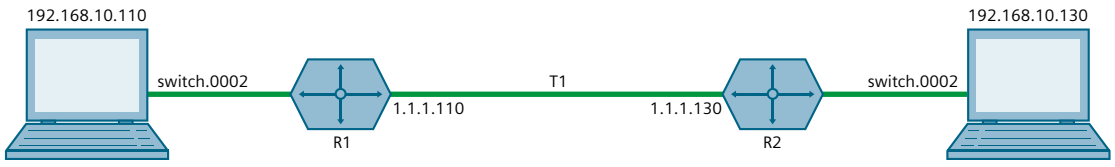


Figure 17: Basic L2TPv3 Tunnel

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.

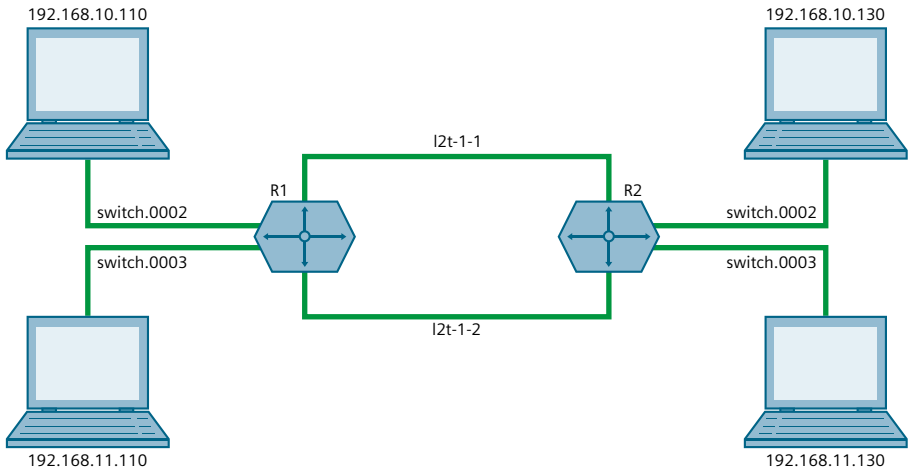


Figure 18: Multiple LAN Extensions Over a Single L2TPv3 Tunnel

» 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.

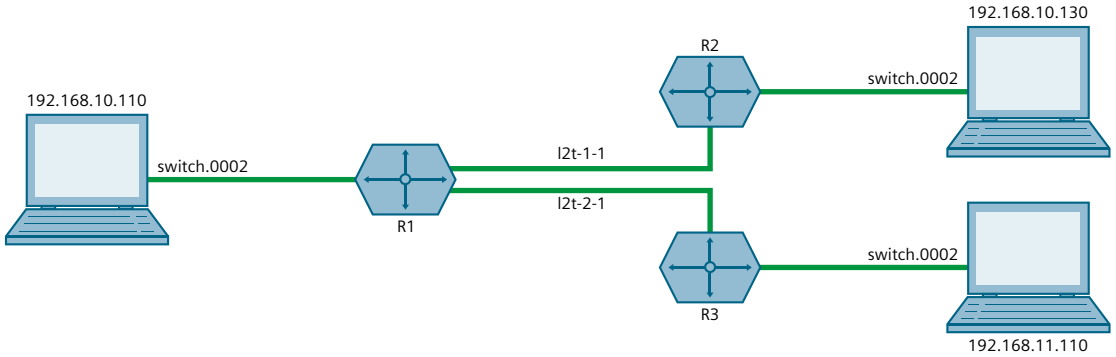


Figure 19: Multiple LAN Extensions Over Multiple L2TPv3 Tunnels

Section 11.4.2

Creating an L2TPv3 Tunnel

To create an L2TPv3 tunnel with another Provider Edge (PE) device, do the following:

1. **Create the L2TPv3 Tunnel Interface**

   An L2TPv3 tunnel interface is created automatically by RUGGEDCOM ROX II whenever a session is defined. The interface is listed under **ip** in the menu and adheres to the following naming convention:

```
l2t-{tunnel-name}-{session-name}
```

For example:

```
l2t-1-2
```

If the session is assigned a VLAN ID, an additional interface is generated in the form of:

```
l2t-{tunnel-name}-{session-name}.{vlan-id}
```

For example:

```
l2t-1-2.0004
```

To create the tunnel interface, start by adding a static or dynamic L2TPv3 tunnel. For more information, refer to either Section 11.4.3.3, "Adding a Static L2TPv3 Tunnel" or Section 11.4.4.3, "Adding a Dynamic L2TPv3 Tunnel".

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 Section 11.1.4.2, "Adding a Virtual Switch Interface".

   For information about assigning an IP address to the L2TPv3 tunnel interface, refer to either Section 7.1.3, "Managing IPv4 Addresses" or Section 7.1.4, "Managing IPv6 Addresses".

Section 11.4.3

Managing Static L2TPv3 Tunnels

Configure static L2TPv3 tunnels to manually control tunnel and sessions parameters at both ends of the bridge. These fixed tunnels are referred to as *unmanaged*.

CONTENTS

- Section 11.4.3.1, "Enabling/Disabling Static L2TPv3 Tunnels"
- Section 11.4.3.2, "Viewing a List of Static L2TPv3 Tunnels"
- Section 11.4.3.3, "Adding a Static L2TPv3 Tunnel"
- Section 11.4.3.4, "Deleting a Static L2TPv3 Tunnel"

Section 11.4.3.1

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, or type **revert** and press **Enter** to abort.

Section 11.4.3.2
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 Section 11.4.3.3, "Adding a Static L2TPv3 Tunnel".

Section 11.4.3.3
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	**Synopsis:** { true, false } **Default:** false Enables the static L2TPv3 tunnel.

Parameter	Description
tunnel-id	**Synopsis:** A 32-bit signed integer Tunnel local id This parameter is mandatory.
remote-tunnel-id	**Synopsis:** A 32-bit signed integer The remote tunnel-id This parameter is mandatory.
transport-encap	**Synopsis:** A string The transport encapsulation (UDP or IP). This parameter is mandatory.
local-ip	**Synopsis:** A string The interface upon which the tunnel is created This parameter is mandatory.
local-port	**Synopsis:** A 32-bit signed integer Local transport port for l2tpv3 service This parameter is mandatory.
remote-ip	**Synopsis:** A string 6 to 40 characters long Ip address of remote tunnel end This parameter is mandatory.
remote-port	**Synopsis:** A 32-bit signed integer Transport port of remote tunnel end This parameter is mandatory.
status	**Synopsis:** A string Current status of tunnel This parameter is mandatory.

4. Add one or more sessions to the tunnel configuration. For more information, refer to Section 11.4.5.2, "Adding a Session".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.4.3.4

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, or type **revert** and press **Enter** to abort.

Section 11.4.4
Managing Dynamic L2TPv3 Tunnels

Configure dynamic L2TPv3 tunnels to carry Point-to-Point Protocol (PPP) traffic, as with L2TPv2, or when static L2TPv3 tunnels are not supported by the peer device. Dynamic L2TPv3 tunnels have the ability to automatically negotiate connections, and reestablish connections in the case of a network failure.

CONTENTS

- Section 11.4.4.1, "Enabling and Configuring Dynamic L2TPv3 Tunnels"
- Section 11.4.4.2, "Viewing a List of Dynamic L2TPv3 Tunnels"
- Section 11.4.4.3, "Adding a Dynamic L2TPv3 Tunnel"
- Section 11.4.4.4, "Deleting a Dynamic L2TPv3 Tunnel"

Section 11.4.4.1
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, or type **revert** and press **Enter** to abort.

Section 11.4.4.2
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 Section 11.4.4.3, "Adding a Dynamic L2TPv3 Tunnel".

Section 11.4.4.3
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) as required:

   NOTE
   Transport encapsulation is only configurable when Dynamic L2TPv3 is in `lac` *mode.*

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** true Enables/Disables the tunnel
remote-ip { remote-ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long Ip address of remote tunnel endpoint
hostname { hostname }	**Synopsis:** A string 1 to 63 characters long Hostname used in AVP This parameter is mandatory.
local-ip { local-ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long

Parameter	Description
	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 { authentication }	**Synopsis:** { none, challenge } **Default:** none The authentication of tunnel
secret { secret }	**Synopsis:** A string 1 to 63 characters long The password of tunnel negotiation
digest { digest }	**Synopsis:** { md5, sha1 } **Default:** md5 Message digest AVP encryption
interop { interop }	**Synopsis:** A 32-bit signed 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-timeout }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed integer between 5 and 1000 **Default:** 60 timeout used for periodic L2TP Hello messages (in seconds)
hidden	**Synopsis:** { true, false } **Default:** false Enables/Disabled AVP hidden
receive-windows { receive-windows }	**Synopsis:** A 32-bit signed integer between 5 and 512 **Default:** 10 Received windows size
established-timeout { established-timeout }	**Synopsis:** A 32-bit signed 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	**Synopsis:** { true, false } **Default:** false Enables/Disables logging tunnel control messages

4. Add one or more sessions to the tunnel configuration. For more information, refer to Section 11.4.5.2, "Adding a Session".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.4.4.4
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, or type **revert** and press **Enter** to abort.

Section 11.4.5
Managing Sessions for L2TPv3 Tunnels

This section describes how to create and manage sessions for L2TPv3 tunnels. A single L2TPv3 can support up to 128 active sessions.

CONTENTS

- Section 11.4.5.1, "Viewing a List of Sessions"
- Section 11.4.5.2, "Adding a Session"
- Section 11.4.5.3, "Deleting a Session"

Section 11.4.5.1
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 Section 11.4.5.2, "Adding a Session".

Section 11.4.5.2
Adding a Session

To add a session to a static or dynamic L2TPv3 tunnel, 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
```

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:

NOTE
The Log parameter is only applicable to dynamic L2TPv3 tunnel sessions.

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** true Enables/Disables the session
remote-end-id { remote-end-id }	**Synopsis:** A 32-bit signed integer between 1 and 65535 Remote endpoint ID to identify session with remote system This parameter is mandatory.
l2tp-specific-sublayer { l2tp-specific-sublayer }	**Synopsis:** { default, none } **Default:** default L2TP specific sublayer processing type
mtu { mtu }	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1460 MTU of network interface
log	**Synopsis:** { true, false } **Default:** false Enables/Disables logging session control messages

IMPORTANT!
Configuration of the local cookie should match the configuration of the remote cookie on the device at the other end of the L2TPv3 tunnel.

4. 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:** A 32-bit unsigned integer

Parameter	Description
	Lower value of cookie. This value must match with low-value of other endpoint's remote cookie
high-value { high-value }	**Synopsis:** A 32-bit unsigned integer Higher value of cookie if the cookie size is 8. This value must match with high-value of other endpoint's remote cookie

IMPORTANT!
Configuration of the remote cookie should match the configuration of the local cookie on the device at the other end of the L2TPv3 tunnel.

5. 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:** A 32-bit unsigned integer Lower value of cookie. This value must match with low-value of other endpoint's local cookie
high-value { high-value }	**Synopsis:** A 32-bit unsigned integer Higher value of cookie if its size is 8. This value must match with high-value of other endpoint's local cookie

6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.4.5.3
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 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 **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.4.6

Managing VLANs for L2TPv3 Tunnels

This section describes how to manage VLANs for L2TPv3 tunnel sessions. Each session supports up to 128 VLAN memberships.

CONTENTS

- Section 11.4.6.1, "Viewing a List of VLANs"
- Section 11.4.6.2, "Adding a VLAN"
- Section 11.4.6.3, "Deleting a VLAN"

Section 11.4.6.1

Viewing a List of VLANs

To view a list of the VLANs configured for a static or dynamic L2TPv3 tunnel session, 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 Section 11.4.6.2, "Adding a VLAN".

Section 11.4.6.2

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, or type **revert** and press **Enter** to abort.

Section 11.4.6.3
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 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
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.5
Managing GOOSE Tunnels

The GOOSE tunnel feature provides the capability to bridge GOOSE frames over a Wide Area Network (WAN).

GOOSE tunnels provide the following features:

- GOOSE traffic is bridged over the WAN via UDP/IP.
- One GOOSE traffic source can be mapped to multiple remote router Ethernet interfaces in mesh fashion.
- To reduce bandwidth consumption, GOOSE daemons may be located at each of the *legs* and at the center of a star network. The centrally located daemon will accept GOOSE packets and re-distribute them.
- Statistics report availability of remote GOOSE daemons, packet counts and Round Trip Time (RTT) for each remote daemon.
- When the Virtual Router Redundancy Protocol (VRRP) is employed, GOOSE transport is improved by sending redundant GOOSE packets from each VRRP gateway.
- You can enable GOOSE forwarding by configuring a generic Layer 2 tunnel. When configured, the device listens for GOOSE packets on one VLAN and forwards them to another VLAN.

The GOOSE protocol is supported by the Layer 2 Tunnel Daemon. The daemon listens to configured Ethernet interfaces and to the network itself (i.e. for tunnel connections from other daemon instances) on a configurable UDP port.

The Media Access Control (MAC) destination address of frames received from Ethernet is inspected in order to determine which GOOSE group they are in. The frames are then encapsulated in network headers and forwarded (with MAC source and destination addresses intact) to the network as GOOSE packets.

IEC61850 recommends that the MAC destination address should be in the range 01:0c:cd:01:00:00 to 01:0c:cd:01:01:ff.

GOOSE packets received from the network are stripped of their network headers and forwarded to Ethernet ports configured for the same multicast address. The forwarded frames contain the MAC source address or the originating device, and not that of the transmitting interface. The VLAN used will be that programmed locally for

the interface and may differ from the original VLAN. The frame will be transmitted with the highest 802.1p priority level (p4).

Packets received from the network will also be forwarded to any other remote daemons included in the group.

To enable forwarding for GOOSE packets, configure a generic Layer 2 tunnel to listen for GOOSE packets on one VLAN and forward them to a second VLAN. To configure the generic Layer 2 tunnel for this operation, set the following for the tunnel:

- Ethernet Interface: select the VLAN on which the GOOSE packets originate
- Ethernet Type: set as 0x88b8
- Remote Daemon: select the VLAN to which to forward the GOOSE packets

CONTENTS

- Section 11.5.1, "Viewing the GOOSE Tunnel Statistics"
- Section 11.5.2, "Viewing a List of GOOSE Tunnels"
- Section 11.5.3, "Adding a GOOSE Tunnel"
- Section 11.5.4, "Deleting a GOOSE Tunnel"
- Section 11.5.5, "Managing Remote Daemons for GOOSE Tunnels"

Section 11.5.1

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
tunnel-name	**Synopsis:** A string 1 to 32 characters long The GOOSE tunnel name. This parameter is mandatory.
ifname	**Synopsis:** A string 1 to 15 characters long The name of the VLAN interface. This parameter is mandatory.

Parameter	Description
mac	**Synopsis:** A string 17 characters long The Multicast Destination MAC Address of the Goose message. This parameter is mandatory.
rx-frames	**Synopsis:** A 32-bit unsigned integer The number of frames received through the tunnel. This parameter is mandatory.
tx-frames	**Synopsis:** A 32-bit unsigned integer The number of frames transmitted through the tunnel. This parameter is mandatory.
rx-chars	**Synopsis:** A 32-bit unsigned integer The number of bytes received through the tunnel. This parameter is mandatory.
tx-chars	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted through the tunnel. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of errors through the tunnel. This parameter is mandatory.

Section 11.5.2
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 Section 11.5.3, "Adding a GOOSE Tunnel".

Section 11.5.3
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 17 characters long The multicast MAC address to listen for. This parameter is mandatory.

4. If necessary, configure one or more remote daemons for the tunnel. For more information, refer to Section 11.5.5.2, "Adding a Remote Daemon".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.5.4

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, or type **revert** and press **Enter** to abort.

Section 11.5.5

Managing Remote Daemons for GOOSE Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

CONTENTS

- Section 11.5.5.1, "Viewing a List of Remote Daemons"
- Section 11.5.5.2, "Adding a Remote Daemon"
- Section 11.5.5.3, "Deleting a Remote Daemon"

Section 11.5.5.1
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 Section 11.5.5.2, "Adding a Remote Daemon".

Section 11.5.5.2
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, or type **revert** and press **Enter** to abort.

Section 11.5.5.3
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, or type **revert** and press **Enter** to abort.

Section 11.6

Managing Generic Tunnels

The Layer 2 Tunnel Daemon supports a generic mode of operation based on the Ethernet type of Layer 2 data traffic seen by the router. Multiple tunnels may be configured, each one with:

- an Ethernet type
- a tunnel ingress (Ethernet interface)
- a tunnel egress (either another locally connected Ethernet interface, or the remote IP address of another Layer 2 Tunnel daemon instance running on another Router)

CONTENTS

- Section 11.6.1, "Viewing the Generic Tunnel Statistics"
- Section 11.6.2, "Viewing a List of Generic Tunnels"
- Section 11.6.3, "Adding a Generic Tunnel"
- Section 11.6.4, "Deleting a Generic Tunnel"
- Section 11.6.5, "Managing Remote Daemon IP Addresses for Generic Tunnels"
- Section 11.6.6, "Managing Remote Daemon Egress Interfaces for Generic Tunnels"
- Section 11.6.7, "Managing Ethernet Types for Generic Tunnels"

Section 11.6.1

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 1 to 32 characters long The generic tunnel name. This parameter is mandatory.
ifname	**Synopsis:** A string 1 to 15 characters long The name of the ingress interface. This parameter is mandatory.
rx-frames	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The number of frames received through the tunnel. This parameter is mandatory.
tx-frames	**Synopsis:** A 32-bit unsigned integer The number of frames transmitted through the tunnel. This parameter is mandatory.
rx-chars	**Synopsis:** A 32-bit unsigned integer The number of bytes received through the tunnel. This parameter is mandatory.
tx-chars	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted through the tunnel. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of errors received through the tunnel. This parameter is mandatory.

Section 11.6.2
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 Section 11.6.3, “Adding a Generic Tunnel”.

Section 11.6.3
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 Section 11.6.5.2, "Adding an IP Address".
5. If necessary, define one or more Ethernet types to be forwarded. For more information, refer to Section 11.6.7.2, "Adding an Ethernet Type".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.6.4
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, or type **`revert`** and press **Enter** to abort.

Section 11.6.5
Managing Remote Daemon IP Addresses for Generic Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

NOTE
When a remote daemon IP address is configured, the interface on the receiver side, where traffic leaves, should be configured on the ingress interface (instead of egress interface).

CONTENTS

- Section 11.6.5.1, "Viewing a List of IP Addresses"
- Section 11.6.5.2, "Adding an IP Address"
- Section 11.6.5.3, "Deleting an IP Address"

Section 11.6.5.1
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 remote-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 Section 11.6.3, "Adding a Generic Tunnel".

Section 11.6.5.2
Adding an IP Address

To add the IP address of a remote Layer 2 protocols server to a generic tunnel configuration, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 11.6.5.3
Deleting an IP Address

To delete the IP address of a remote Layer 2 protocols server from a generic tunnel configuration, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 11.6.6

Managing Remote Daemon Egress Interfaces for Generic Tunnels

This section describes how to create and manage remote daemon egress interfaces for generic tunnels.

CONTENTS

- Section 11.6.6.1, "Viewing a List of Egress Interfaces"
- Section 11.6.6.2, "Adding an Egress Interface"
- Section 11.6.6.3, "Deleting an Egress Interface"

Section 11.6.6.1

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 remote-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 Section 11.6.6.2, "Adding an Egress Interface".

Section 11.6.6.2

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, or type **revert** and press **Enter** to abort.

Section 11.6.6.3
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, or type **revert** and press **Enter** to abort.

Section 11.6.7
Managing Ethernet Types for Generic Tunnels

This section describes how to define the types of Ethernet protocols that can be forwarded by generic tunnels.

CONTENTS

- Section 11.6.7.1, "Viewing a List of Ethernet Types"
- Section 11.6.7.2, "Adding an Ethernet Type"
- Section 11.6.7.3, "Deleting an Ethernet Type"

Section 11.6.7.1
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 ethernet-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 Section 11.6.7.2, "Adding an Ethernet Type".

Section 11.6.7.2
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, or type **revert** and press **Enter** to abort.

Section 11.6.7.3
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, or type **revert** and press **Enter** to abort.

Section 11.7
Managing Generic Routing Encapsulation Tunnels

RUGGEDCOM ROX II can employ the Generic Routing Encapsulation (GRE) protocol to encapsulate multicast traffic and IPv6 packets together and transport them through an IPv4 network tunnel. As such, GRE tunnels can transport traffic through any number of intermediate networks.

The key parameters for GRE tunnels is the tunnel name, local router address, remote router address and remote subnet.

The following illustrates a typical GRE tunnel configuration:

Figure 20: 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. 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.

CONTENTS

- Section 11.7.1, “Viewing Statistics for GRE Tunnels”
- Section 11.7.2, “Viewing a List of GRE Tunnels”
- Section 11.7.3, “Adding a GRE Tunnel”
- Section 11.7.4, “Configuring a DSCP Marking for GRE Tunnel Traffic”
- Section 11.7.5, “Enabling/Disabling Keepalive Messages”
- Section 11.7.6, “Deleting a GRE Tunnel”
- Section 11.7.7, “Example: Configuring a GRE Tunnel with IPsec”

Section 11.7.1

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 1 to 10 characters long The name of the GRE tunnel.
status	**Synopsis:** A string 1 to 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 This parameter is mandatory.
tunnel-status	**Synopsis:** A string

Parameter	Description
	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 This parameter is mandatory.
rx-packets	**Synopsis:** A 64-bit unsigned integer The number of packets received through the tunnel. This parameter is mandatory.
rx-errors	**Synopsis:** A 64-bit unsigned integer The error packets received through the tunnel. This parameter is mandatory.
rx-drops	**Synopsis:** A 64-bit unsigned integer The number of packets dropped by the tunnel. This parameter is mandatory.
tx-packets	**Synopsis:** A 64-bit unsigned integer The number of packets transmitted through the tunnel. This parameter is mandatory.
tx-errors	**Synopsis:** A 64-bit unsigned integer The number of error packets transmitted through the tunnel. This parameter is mandatory.
tx-drops	**Synopsis:** A 64-bit unsigned integer The number of packets dropped by the tunnel. This parameter is mandatory.

Section 11.7.2
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 Section 11.7.3, “Adding a GRE Tunnel”.

Section 11.7.3
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 7 to 15 characters long or a string 6 to 40 characters long The IP address of the local end of the tunnel. This parameter is mandatory.
remote-ip { remote-ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the remote end of the tunnel. This parameter is mandatory.
remote-net { remote-net }	**Synopsis:** A string 9 to 18 characters long or a string 4 to 43 characters long The target network of remote end of the tunnel.
mtu { mtu }	**Synopsis:** A 32-bit signed integer **Default:** 1476 The MTU of the GRE interface.
multicast	Enables multicast traffic on the tunnel interface.
cost { cost }	**Synopsis:** A 32-bit signed 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:** A 32-bit unsigned 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	**Synopsis:** { true, false } **Default:** false

Parameter	Description
	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 Section 11.7.5, "Enabling/Disabling Keepalive Messages".
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 Section 11.7.4, "Configuring a DSCP Marking for GRE Tunnel Traffic".

> **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 Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.7.4
Configuring a DSCP Marking for GRE Tunnel Traffic

Each packet traversing a GRE tunnel can be assigned a Differentiated Services Code Point (DSCP) mark either defined by the device or inherited by the original IP header.

To 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, or type **`revert`** and press **Enter** to abort.

Section 11.7.5
Enabling/Disabling Keepalive Messages

Keepalive messages enable endpoints of a GRE tunnel to determine one another's current operational status.

Traditionally, GRE tunnels are stateless, meaning that remote endpoints retain no information about one another. As a result, an endpoint will not know when the other endpoint becomes unreachable and continue sending frames, even though the other end is unable to receive them.

With keepalive messages enabled, RUGGEDCOM ROX II will send keepalive messages to the other endpoint and wait for a response. If a response is not received before the next message is scheduled to be sent, it begins to count the number of consecutive messages sent that did not receive a reply. After so many failures to reply, the other endpoint is considered unreachable and a *Link Down* alarm is raised. This is the cue to the network administrator to bring down the GRE tunnel and investigate.

By default, keepalive messages are sent every 10 seconds and the remote endpoint has three opportunities to reply. These thresholds are user configurable.

To enable or disable keepalive messages for a GRE tunnel, do the following:

1. 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:** A 16-bit unsigned 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 8-bit unsigned integer between 1 and 255 **Default:** 3 The number of keepalive message the remote endpoint can ignore before it is considered unreachable.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.7.6
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, or type **revert** and press **Enter** to abort.

Section 11.7.7

Example: Configuring a GRE Tunnel with IPsec

This example describes one method to configure a GRE tunnel with IPsec on RUGGEDCOM ROX II devices.

For more information about IPsec tunnels, refer to Section 11.8, "Managing IPsec Tunnels".

IMPORTANT!
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.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

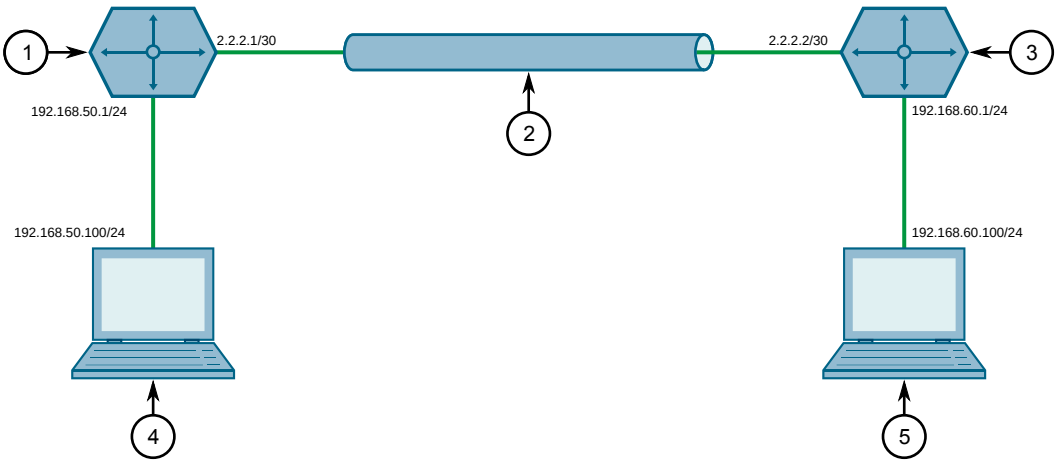


Figure 21: Topology – Site-to-Site Encrypted VPN Tunnel with a Pre-Shared Key

1. Device A **2.** GRE/IPsec Tunnel **3.** Device B **4.** Client 1 **5.** Client 2

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 Section 5.2, "Configuring the Host Name".
   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 Section 11.7.3, "Adding a GRE Tunnel".

c. Enable Keepalive messages for GRE tunnel. For more information, refer to Section 11.7.5, "Enabling/Disabling Keepalive Messages".

d. Assign IP address *172.16.1.1/24* to the gre tunnel interface. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

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 Section 11.8.5.2, "Adding a Pre-Shared Key".

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 Section 11.8.6.2, "Adding a Connection".

g. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to Section 11.8.7.2, "Adding an IKE Algorithm".

h. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to Section 11.8.8.3, "Adding an ESP Algorithm".

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 Section 11.8.9, "Configuring the Connection Ends".

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 Section 11.8.9, "Configuring the Connection Ends".

k. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

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 Section 11.8.9, "Configuring the Connection Ends".

m. Configure the right connection end for the IPsec tunnel with the following nexthop address parameters:

Parameter	Value
Type	address
Value	172.16.1.1

For more information about configuring connection ends, refer to Section 11.8.9, "Configuring the Connection Ends".

n. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

2. Configure Device B:

a. Configure a host name for the device. For more information, refer to Section 5.2, "Configuring the Host Name".

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 Section 11.7.3, "Adding a GRE Tunnel".

c. Enable Keepalive messages for GRE tunnel. For more information, refer to Section 11.7.5, "Enabling/Disabling Keepalive Messages".

d. Assign IP address *172.16.1.2/24* to the gre tunnel interface. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

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 Section 11.8.5.2, "Adding a Pre-Shared Key".

f. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret

Parameter	Value
Connection Type	tunnel

For more information about IPsec connections, refer to Section 11.8.6.2, "Adding a Connection".

g. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to Section 11.8.7.2, "Adding an IKE Algorithm".

h. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to Section 11.8.8.3, "Adding an ESP Algorithm".

i. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to Section 11.8.9, "Configuring the Connection Ends".

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 Section 11.8.9, "Configuring the Connection Ends".

k. Add subnet *192.168.50.0/24* for the right connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

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 Section 11.8.9, "Configuring the Connection Ends".

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 Section 11.8.9, "Configuring the Connection Ends".

n. Add subnet *192.168.60.0/24* for the left connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

3. Enable the IPsec tunnel. For more information, refer to Section 11.8.2, "Configuring IPsec Tunnels".
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 Section 11.8.4, "Viewing the IPsec Tunnel Status".

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
  !
!
```

Section 11.8

Managing IPsec Tunnels

IPsec (Internet Protocol SECurity) uses strong cryptography to provide authentication and encryption services. Authentication ensures that packets are from the right sender and have not been altered in transit. Encryption prevents unauthorized reading of packet contents.

These services allow secure tunnels to be built through untrusted networks. Everything passing through the untrusted network is encrypted by the IPsec gateway and decrypted by the gateway at the other end. The result is a Virtual Private Network (VPN), a network which is effectively private even though it includes machines at several different sites connected by the insecure Internet.

For more information about IPsec tunnels, refer to Section 11.8.1, "IPsec Tunneling Concepts".

IMPORTANT!
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 Section 16.8, "Managing NTP Servers".

CONTENTS

- Section 11.8.1, "IPsec Tunneling Concepts"
- Section 11.8.2, "Configuring IPsec Tunnels"
- Section 11.8.3, "Configuring Certificates and Keys"
- Section 11.8.4, "Viewing the IPsec Tunnel Status"
- Section 11.8.5, "Managing Pre-Shared Keys"
- Section 11.8.6, "Managing Connections"
- Section 11.8.7, "Managing the Internet Key Exchange (IKE) Protocol"
- Section 11.8.8, "Managing the Encapsulated Security Payload (ESP) Protocol"
- Section 11.8.9, "Configuring the Connection Ends"
- Section 11.8.10, "Managing Private Subnets"
- Section 11.8.11, "Example: Configuring an Encrypted VPN Tunnel"

Section 11.8.1

IPsec Tunneling Concepts

The IPsec suite of protocols were developed by the Internet Engineering Task Force (IETF) and are required as part of IP version 6. Libreswan is the open source implementation of IPsec used by RUGGEDCOM ROX II.

The protocols used by IPsec are the Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) protocols. ESP provides encryption and authentication (ensuring that a message originated from the expected sender and has not been altered on route). IKE negotiates connection parameters, including keys, for ESP. IKE is

based on the Diffie-Hellman key exchange protocol, which allows two parties without any initial shared secret to create one in a manner immune to eavesdropping.

CONTENTS

- Section 11.8.1.1, "IPsec Modes"
- Section 11.8.1.2, "Supported Encryption Protocols"
- Section 11.8.1.3, "Public and Secret Key Cryptography"
- Section 11.8.1.4, "X509 Certificates"
- Section 11.8.1.5, "NAT Traversal"
- Section 11.8.1.6, "Remote IPsec Client Support"
- Section 11.8.1.7, "IPsec and Router Interfaces"

Section 11.8.1.1
IPsec Modes

IPsec has two basic modes of operation. 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.

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.

Section 11.8.1.2
Supported Encryption Protocols

Libreswan supports the following standard encryption protocols:

- **3DES (Triple DES)**

  Uses three Data Encryption Standard (DES) encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. 3DES is the most CPU intensive cipher.

- **AES**

  The Advanced Encryption Standard (AES) protocol cipher uses a 128-bit block and 128, 192 or 256-bit keys. This is the most secure protocol in use today, and is much preferred to 3DES due to its efficiency.

Section 11.8.1.3
Public and Secret Key Cryptography

In *public key* cryptography, keys are created in matched pairs (called public and private keys). The public key is made public while the private key is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Only the owner of the private key can decrypt the message.

When this form of encryption is used, each router configures its VPN connection to use the RSA algorithm and includes the public signature of its peer.

In *secret key* cryptography, a single key known to both parties is used for both encryption and decryption.

When this form of encryption is used, each router configures its VPN connection to use a secret pre-shared key. For information about how to configure pre-shared keys, refer to Section 11.8.5, "Managing Pre-Shared Keys".

Section 11.8.1.4
X509 Certificates

In addition to pre-shared keys, IPsec also uses certificates to authenticate connections with hosts and routers. Certificates are digital signatures that are produced by a trusted source, namely a Certificate Authority (CA). For each host, the CA creates a certificate that contains CA and host information. The certificate is "signed" by creating a digest of all the fields in the certificate and then encrypting the hash value with its private key. The host's certificate and the CA public key are installed on all gateways that the host connects to.

When the gateway receives a connection request, it uses the CA public key to decrypt the signature back into the digest. It then recomputes its own digest from the plain text in the certificate and compares the two. If both digests match, the integrity of the certificate is verified (it was not tampered with), and the public key in the certificate is assumed to be the valid public key of the connecting host.

Section 11.8.1.5
NAT Traversal

Historically, IPsec has presented problems when connections must traverse a firewall providing Network Address Translation (NAT). The Internet Key Exchange (IKE) used in IPsec is not NAT-translatable. When IPsec connections must traverse a firewall, IKE messages and IPsec-protected packets must be encapsulated as User Datagram Protocol (UDP) messages. The encapsulation allows the original untranslated packet to be examined by IPsec.

Encapsulation is enabled during the IPsec configuration process. For more information, refer to Section 11.8.2, "Configuring IPsec Tunnels".

Section 11.8.1.6
Remote IPsec Client Support

If the router is to support a remote IPsec client and the client will be assigned an address in a subnet of a local interface, a proxy ARP must be activated for that interface. This will cause the router to respond to ARP requests on behalf of the client and direct traffic to it over its connection.

IPsec relies upon the following protocols and ports:

- protocol 51, IPSEC-AH Authentication Header (RFC2402)
- protocol 50, IPSEC-ESP Encapsulating Security Payload (RFC2046)
- UDP port 500

The firewall must be configured to accept connections on these ports and protocols. For more information, refer to Section 6.8.6, "Configuring the Firewall for a VPN".

Section 11.8.1.7
IPsec and Router Interfaces

If IPsec works on an interface which could disappear, such as a PPP connection, or if the IP address could change, the **Monitor Interface** option must be set for the IPsec connection. When this option is set, IPsec will restart when the interface disappears and reappears, or the IP address is changed.

The **Monitor Interface** option is set on the **Connection** form available for each connection. For more information about connections, refer to Section 11.8.6, "Managing Connections".

Section 11.8.2
Configuring IPsec Tunnels

To configure IPsec tunnels, do the following:

NOTE
RUGGEDCOM ROX II supports the creation of policy-based VPNs, which can be characterized as follows:

- *No IPsec network interfaces have been created.*
- *The routing table is not involved in directing packets to IPsec.*
- *Only data traffic matching the tunnel's local and remote subnets is forwarded to the tunnel. Normal traffic is routed by one set of firewall rules and VPN traffic is routed based on separate rules.*
- *The firewall is configured with a VPN zone of type **ipsec**.*
- *As IPsec packets are received, they are decoded, flagged as IPsec-encoded, and presented as having arrived directly from the same network interface on which they were originally received.*
- *Firewall rules are written to allow traffic to and from VPN tunnels. These are based on the normal form of source/destination IP addresses, and IP protocol and port numbers. These rules, by virtue of the zones they match, use the policy flags inserted by the netkey to route matching data traffic to the proper interface.*

For more information about configuring a policy-based VPN, refer to Section 6.8, "Managing Firewalls".

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:** A 32-bit unsigned 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 Section 11.8.5.2, "Adding a Pre-Shared Key".
4. Configure one or more encrypted connections. For more information, refer to Section 11.8.6.2, "Adding a Connection".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.8.3
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 Section 6.7.4.3, "Adding a CA Certificate and CRL".
3. Add a private key. For more information, refer to Section 6.7.5.2, "Adding a Private Key".
4. Add a certificate. For more information, refer to Section 6.7.7.3, "Adding a Certificate".
5. Add a public key. For more information, refer to Section 6.7.6.2, "Adding a Public Key".
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, or type **revert** and press **Enter** to abort.

Section 11.8.4
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 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, keysizemax=64
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=8, keysizemin=192, keysizemax=192
000 algorithm ESP encrypt: id=11, name=ESP_NULL, ivlen=0, keysizemin=0, keysizemax=0
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=8, keysizemin=128, keysizemax=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, keysizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=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, keydeflen=128
000 algorithm IKE encrypt: id=65289, name=OAKLEY_TWOFISH_CBC_SSH, blocksize=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@example.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@example.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 initiate
000 #2: "ipsec-12":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 19349s;
 newest IPSEC; eroute owner; isakmp#1; idle; import:admin 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
```

Section 11.8.5

Managing Pre-Shared Keys

Pre-shared keys are used in *secret key* cryptography. For more information about *secret key* cryptography and pre-shared keys, refer to Section 11.8.1.3, “Public and Secret Key Cryptography”.

CONTENTS

- Section 11.8.5.1, “Viewing a List of Pre-Shared Keys”
- Section 11.8.5.2, “Adding a Pre-Shared Key”

- Section 11.8.5.3, "Deleting a Pre-Shared Key"

Section 11.8.5.1
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 $4$9YslfOBfkyYV8c1tqN4IDw==
  !
 !
!
```

If no pre-shared keys have been configured, add pre-shared keys as needed. For more information, refer to Section 11.8.5.2, "Adding a Pre-Shared Key".

Section 11.8.5.2
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 | local-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 1 to 8192 characters long The pre-shared key. This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.8.5.3
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 | local-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, or type **revert** and press **Enter** to abort.

Section 11.8.6

Managing Connections

An IPsec connection is an encrypted connection between two devices who share the same pre-authorized authentication key.

CONTENTS

- Section 11.8.6.1, "Viewing a List of Connections"
- Section 11.8.6.2, "Adding a Connection"
- Section 11.8.6.3, "Configuring Dead Peer Detection"
- Section 11.8.6.4, "Deleting a Connection"
- Section 11.8.6.5, "Viewing the Status of a Connection"

Section 11.8.6.1

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 Section 11.8.6.2, "Adding a Connection".

Section 11.8.6.2
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 'default' 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.
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 a 32-bit unsigned integer between 1081 and 28800 **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

Parameter	Description
	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 a 32-bit unsigned 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.
l2tp	Enables/disables L2TP for this connection.
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.

4. If required, enable and configure dead peer detection. For more information, refer to Section 11.8.6.3, "Configuring Dead Peer Detection".
5. If required, configure the Internet Key Exchange (IKE) protocol by adding one or more algorithms. For more information, refer to Section 11.8.7.2, "Adding an IKE Algorithm".
6. If required, configure Encapsulated Security Payload (ESP) encryption for the connection. For more information, refer to Section 11.8.8, "Managing the Encapsulated Security Payload (ESP) Protocol".
7. If required, configure the left (local router) and right (remote router) ends of the connection. For more information, refer to Section 11.8.9, "Configuring the Connection Ends".
8. If required, configure L2TP tunnels. For more information, refer to Section 11.3.1, "Configuring L2TP Tunnels".
9. If certificates and keys are required, make sure they are configured on the device. For more information, refer to Section 11.8.3, "Configuring Certificates and Keys".
10. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.8.6.3

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:** A 32-bit unsigned 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:** A 32-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 11.8.6.4
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, or type **revert** and press **Enter** to abort.

Section 11.8.6.5
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.

Section 11.8.7

Managing the Internet Key Exchange (IKE) Protocol

The Internet Key Exchange (IKE) protocol negotiates connection parameters, including keys, for the Encapsulated Security Payload (ESP) protocol employed by IPsec. IKE is based on the Diffie-Hellman key exchange protocol, which allows two parties without any initially shared secret to create one in a manner immune to eavesdropping.

CONTENTS

- Section 11.8.7.1, "Viewing a List of IKE Algorithms"
- Section 11.8.7.2, "Adding an IKE Algorithm"
- Section 11.8.7.3, "Deleting an IKE Algorithm"

Section 11.8.7.1

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 Section 11.8.7.2, "Adding an IKE Algorithm".

Section 11.8.7.2
Adding an IKE Algorithm

To add a new algorithm for the Internet Key Exchange (IKE) protocol, do the following:

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

   ```
   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`. 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.
   - *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, or type **`revert`** and press **Enter** to abort.

Section 11.8.7.3
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`. 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.
   - *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, or type **`revert`** and press **Enter** to abort.

Section 11.8.8

Managing the Encapsulated Security Payload (ESP) Protocol

The Encapsulated Security Payload (ESP) employed by IPsec provides encryption and authentication, making sure that messages originated from the expected sender have not been altered in transit.

CONTENTS

- Section 11.8.8.1, "Configuring ESP Encryption"
- Section 11.8.8.2, "Viewing a List of ESP Algorithms"
- Section 11.8.8.3, "Adding an ESP Algorithm"
- Section 11.8.8.4, "Deleting an ESP Algorithm"

Section 11.8.8.1

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 Section 11.8.8.3, "Adding an ESP Algorithm".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.8.8.2

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 Section 11.8.8.3, "Adding an ESP Algorithm".

Section 11.8.8.3
Adding an ESP Algorithm

To add a new algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

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

   ```
   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, or type **revert** and press **Enter** to abort.

Section 11.8.8.4
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, or type **revert** and press **Enter** to abort.

Section 11.8.9
Configuring the 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.

To configure a connection end for an IPsec tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***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.
3. Configure the public IP address by configuring the following parameters:

   IMPORTANT!
   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 1 to 4095 characters long The public hostname or IP address.

4. Configure the system public key by configuring the following parameters:

Parameter	Description
type { type }	**Synopsis:** { none, rsasig, certificate-any, certificate } **Default:** none Key type.
rsa-sig { rsa-sig }	**Synopsis:** A string The RSA signature key name.
rsa-sig-ipsec	**Synopsis:** A string 1 to 8192 characters long The RSA signature in IPsec format.
certificate { certificate }	**Synopsis:** A string The selected certificate.

5. 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 1 to 1024 characters long The hostname, IP address or the Distinguished Name in the certificate.

6. Configure the next hop to the other system by configuring 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 7 to 15 characters long The IP address of the next hop that can be used to reach the destination network.

7. Configure the Network Address Translation (NAT) traversal negotiation method by configuring the following parameters:

> **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.*

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-t-ike-02 will solve this problem. The default value is 'rfc-3947' unless overwritten by the default connection setting.

8. If required, configure a subnet for the connection end. For more information, refer to Section 11.8.10.3, “Adding an Address for a Private Subnet”.
9. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.8.10
Managing Private Subnets

If the device is connected to an internal, private subnet, access to the subnet can be granted to the device at the other end of the IPsec tunnel. Only the IP address and mask of the private subnet is required.

CONTENTS

- Section 11.8.10.1, “Configuring Private Subnets for Connection Ends”
- Section 11.8.10.2, “Viewing a List of Addresses for Private Subnets”
- Section 11.8.10.3, “Adding an Address for a Private Subnet”
- Section 11.8.10.4, “Deleting an Address for a Private Subnet”

Section 11.8.10.1
Configuring Private Subnets for Connection Ends

To configure a private subnet for either the left (local router) or right (remote router) connection ends in a VPN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection/{end} » subnet***, where *{end}* is the either the left (local router) or right (remote router) connection end.
3. Configure the following parameter(s) as required:

Parameter	Description
{ network }	**Synopsis:** A string 9 to 18 characters long The IP address/prefix.

4. Add one or more subnet addresses. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 11.8.10.2
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 Section 11.8.10.3, "Adding an Address for a Private Subnet".

Section 11.8.10.3
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, or type **revert** and press **Enter** to abort.

Section 11.8.10.4
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 ] 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, or type **revert** and press **Enter** to abort.

Section 11.8.11
Example: Configuring an Encrypted VPN Tunnel

This example describes how to configure an encrypted VPN tunnel over a public network using Layer 3 RUGGEDCOM ROX II devices.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

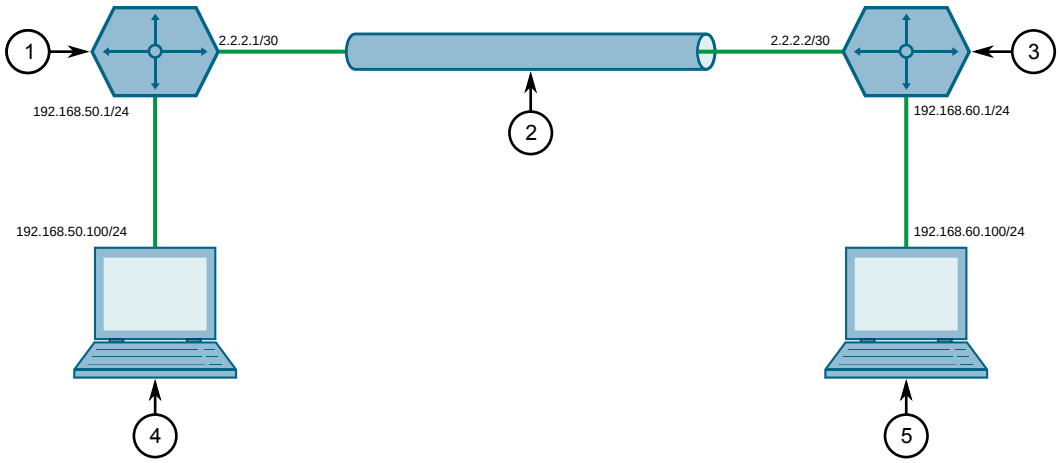


Figure 22: Topology – Site-to-Site Encrypted VPN Tunnel with a Pre-Shared Key

1. Device A **2.** IPsec Encrypted VPN Tunnel **3.** Device B **4.** Client 1 **5.** Client 2

To configure a VPN tunnel, do the following:

1. Configure a connection name for the VPN. For more information, refer to Section 11.8.6.2, "Adding a Connection".
2. Configure Device A:
   a. Configure a host name for the device. For more information, refer to Section 5.2, "Configuring the Host Name".
   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 Section 11.8.5.2, "Adding a Pre-Shared Key".
   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 Section 11.8.6.2, "Adding a Connection".
   d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to Section 11.8.7.2, "Adding an IKE Algorithm".
   e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to Section 11.8.8.3, "Adding an ESP Algorithm".
   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 Section 11.8.9, "Configuring the Connection Ends".

g. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

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 Section 11.8.9, "Configuring the Connection Ends".

i. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

3. Configure Device B:

a. Configure a host name for the device. For more information, refer to Section 5.2, "Configuring the Host Name".

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 Section 11.8.5.2, "Adding a Pre-Shared Key".

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 Section 11.8.6.2, "Adding a Connection".

d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to Section 11.8.7.2, "Adding an IKE Algorithm".

e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to Section 11.8.8.3, "Adding an ESP Algorithm".

f. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address

Parameter	Value
Value	2.2.2.2

For more information about configuring connection ends, refer to Section 11.8.9, "Configuring the Connection Ends".

g. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

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 Section 11.8.9, "Configuring the Connection Ends".

i. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to Section 11.8.10.3, "Adding an Address for a Private Subnet".

4. Enable the IPsec tunnel. For more information, refer to Section 11.8.2, "Configuring IPsec Tunnels".
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@example.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
```

This indicates the IPsec tunnel is active.

For more information, refer to Section 11.8.4, "Viewing the IPsec Tunnel Status".

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 Section 2.4.9, "Capturing Packets from a Network Interface".

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
```

Section 11.9

Managing 6in4 and 4in6 Tunnels

In networks where IPv4 and IPv6 operate simultaneously, 6in4 and 4in6 tunnels can be used to enable IPv6/IPv4 hosts to reach services using the opposite protocol. IPv6/IPv4 hosts and networks isolated from one another can also use these tunnels to access one another.

In a 6in4 tunnel, IPv6 traffic is encapsulated over configured IPv4 links, and vice versa for 4in6 tunnels.

NOTE
For information about how to monitor traffic through the tunnel, refer to Section 7.1.2, "Viewing Statistics for Routable Interfaces".

CONTENTS

- Section 11.9.1, "Enabling/Disabling 6in4 or 4in6 Tunnels"

- Section 11.9.2, "Viewing a List of 6in4 or 4in6 Tunnels"
- Section 11.9.3, "Viewing the Status of 6in4/4in6 Tunnels"
- Section 11.9.4, "Adding a 6in4 or 4in6 Tunnel"
- Section 11.9.5, "Deleting a 6in4 or 4in6 Tunnel"

Section 11.9.1
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, or type **`revert`** and press **Enter** to abort.

Section 11.9.2
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

!
```

Section 11.9.3
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
```

Section 11.9.4
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
local-ip	**Synopsis:** A string 7 to 15 characters long The interface upon which the tunnel is created This parameter is mandatory.
remote-ip	**Synopsis:** A string 7 to 15 characters long Ip address of remote tunnel end This parameter is mandatory.
status	**Synopsis:** A string Current status of tunnel This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 11.9.5
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, or type **revert** and press **Enter** to abort.

Section 11.10

Managing DMVPN

This section describes how to configure the device as a spoke in a Dynamic Multipoint Virtual Private Network (DMVPN) hub-and-spoke network.

CONTENTS

- Section 11.10.1, "Understanding DMVPN"
- Section 11.10.2, "Configuring DMVPN"
- Section 11.10.3, "Managing DMVPN Interfaces"
- Section 11.10.4, "Viewing the Status of DMVPN"

Section 11.10.1

Understanding DMVPN

Dynamic Multipoint Virtual Private Network (DMVPN) is a routing solution for building scalable and secure VPN networks. It allows network designers to rapidly deploy routers for medium to large enterprises without having to configure static connections between all devices.

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.

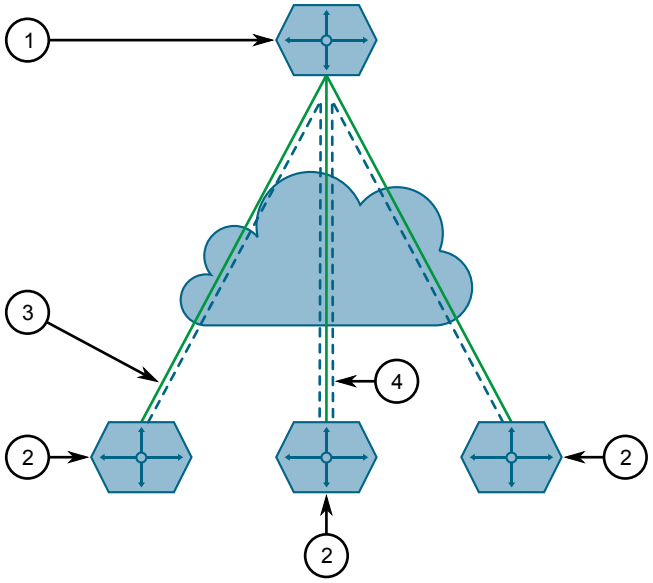


Figure 23: Hub-and-Spoke Topology – Single Hub

1. Hub (Static IP Address) **2.** Spoke (Static IP Address) **3.** Hub-to-Spoke GRE/IPsec Tunnel

Spokes can also be connected to a secondary hub when redundancy is required.

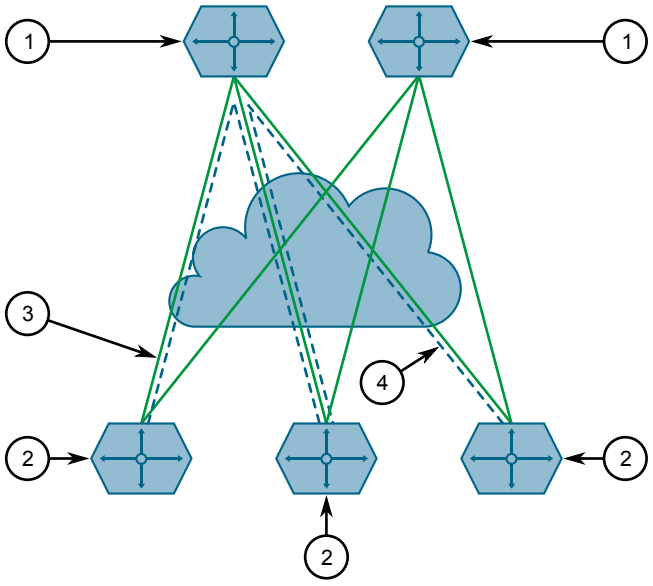


Figure 24: Hub-and-Spoke Topology – Dual Hub

1. Hub (Static IP Address) **2.** Spoke (Static IP Address) **3.** Hub-to-Spoke GRE/IPsec Tunnel

Section 11.10.2
Configuring DMVPN

To configure the device to act as a spoke in a hub-and-spoke network, do the following:

NOTE
RUGGEDCOM ROX II supports connections with up to two hubs.

1. Determine the static IP address of the hub router.
2. Configure a GRE tunnel to the hub. For more information, refer to Section 11.7.3, "Adding a GRE Tunnel".
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 Section 11.8.2, "Configuring IPsec Tunnels".
4. Configure a BGP route for the GRE tunnel. For more information, refer to Section 12.8.1, "Configuring BGP".
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 Section 11.10.3.2, "Adding a DMVPN Interface".
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 Section 11.10.4, "Viewing the Status of DMVPN".

Section 11.10.3
Managing DMVPN Interfaces

Configure a DMVPN interface to connect with a host. Up to two interfaces can be configured, allowing the device to connect with two hubs.

CONTENTS

- Section 11.10.3.1, "Viewing a List of DMVPN Interfaces"
- Section 11.10.3.2, "Adding a DMVPN Interface"
- Section 11.10.3.3, "Deleting a DMVPN Interface"

Section 11.10.3.1
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 Section 11.10.3.2, "Adding a DMVPN Interface".

Section 11.10.3.2
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:

   CAUTION!
   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 9 to 18 characters long IPv4 address of remote GRE interface to be used for this NHRP session.
holdtime { holdtime }	**Synopsis:** A 32-bit unsigned 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 { authentication }	**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, or type **`revert`** and press **Enter** to abort.

Section 11.10.3.3
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, or type **revert** and press **Enter** to abort.

Section 11.10.4
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 • `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	Type: local
Protocol-Address	The interface's IP address.	Protocol-Address: 172.30.168.2/32
Flags	The flag(s) assigned to the last NHRP registration request packet. Possible values: • `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

12 Unicast and Multicast Routing

This chapter describes how to configure, monitor and manage static and dynamic routes unicast and multicast traffic.

CONTENTS

- Section 12.1, “Viewing the Status of IPv4 Routes”
- Section 12.2, “Viewing the Status of IPv6 Routes”
- Section 12.3, “Viewing the Memory Statistics”
- Section 12.4, “Configuring ICMP”
- Section 12.5, “Managing Event Trackers”
- Section 12.6, “Managing IS-IS”
- Section 12.7, “Managing RIP”
- Section 12.8, “Managing BGP”
- Section 12.9, “Managing OSPF”
- Section 12.10, “Managing MPLS”
- Section 12.11, “Managing Virtual Routing and Forwarding (VRF)”
- Section 12.12, “Managing Static Routing”
- Section 12.13, “Managing Static Multicast Routing”
- Section 12.14, “Managing Dynamic Multicast Routing”

Section 12.1

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
```

This table/list provides the following information:

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.
metric	**Synopsis:** A string The route metric value.

If no IPv4 routes have been configured, add routes as needed. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

Section 12.2
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
```

This table/list provides the following information:

Parameter	Description
destination	**Synopsis:** A string The network/prefix.
gateway	**Synopsis:** A string

Parameter	Description
	The gateway address.
interface	**Synopsis:** A string The interface name.
type	**Synopsis:** A string The route type.
weight	**Synopsis:** A string The route weight.
metric	**Synopsis:** A string The metric value.

If no IPv6 routes have been configured, add routes as needed. For more information, refer to Section 12.12.3, "Adding an IPv6 Static Route".

Section 12.3
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
```

This list provides the following information:

Parameter	Description
total	**Synopsis:** A 32-bit unsigned integer The total heap allocated (in bytes). This parameter is mandatory.
used	**Synopsis:** A 32-bit unsigned integer The number of used ordinary blocks (in bytes). This parameter is mandatory.
free	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The number of free ordinary blocks (in bytes). This parameter is mandatory.

Section 12.4
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	**Synopsis:** { true, false } **Default:** false Ignores all ICMP echo requests sent to it.
ignore-icmp-broadcast	**Synopsis:** { true, false } **Default:** true Ignores all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast.
send-icmp-redirect	**Synopsis:** { true, false } **Default:** true Sends the ICMP redirect.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.5
Managing Event Trackers

Trackers monitor the availability of hosts or devices by periodically transmitting ICMP messages (or pings). Based on the ICMP results, the tracker updates operational data with the status of the host or device as it changes (i.e. between "up " and "down" states). Other parts of the system can then subscribe to the operational data to be notified when changes take place.

Where available, a tracker can allow a user greater flexibility when configuring a feature. For example, advertised or received routes can be filtered or blocked entirely, based on the status of the tracker.

NOTE
Trackers only use ICMP messages to ping an IP target. Therefore, it can only provide availability for an IP device, and only up to the IP layer.

CONTENTS

- Section 12.5.1, "Viewing a List of Event Trackers"
- Section 12.5.2, "Viewing Event Tracker Statistics"
- Section 12.5.3, "Adding an Event Tracker"
- Section 12.5.4, "Deleting an Event Tracker"

Section 12.5.1
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 Section 12.5.3, "Adding an Event Tracker".

Section 12.5.2
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:** A 32-bit unsigned integer The number of echo attempts.
echo-replies	**Synopsis:** A 32-bit unsigned 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).

Section 12.5.3
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 1 to 253 characters long Configures the ping target as an IPv4 address or hostname.domain. This parameter is mandatory.
source-ip { source-ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 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:** A 32-bit unsigned integer Determines how many milliseconds to wait for the ICMP response. This parameter is mandatory.
interval { interval }	**Synopsis:** A 32-bit unsigned integer equaling 100 or higher Determines how many milliseconds to wait before sending another ICMP request. This parameter is mandatory.
fall { fall }	**Synopsis:** A 32-bit unsigned integer equaling 1 or higher

Parameter	Description
	The number of times a failure occurs before changing the tracking state from up to down. This parameter is mandatory.
rise { rise }	**Synopsis:** A 32-bit unsigned integer equaling 1 or higher 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, or type **`revert`** and press **Enter** to abort.

Section 12.5.4
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, or type **`revert`** and press **Enter** to abort.

Section 12.6
Managing IS-IS

Intermediate System - Intermediate System (IS-IS) is one of a suite of routing protocols tasked with sharing routing information between routers. The job of the router is to enable the efficient movement of data over sometimes complex networks. Routing protocols are designed to share routing information across these networks and use sophisticated algorithms to decide the shortest route for the information to travel from point A to point B. One of the first link-state routing protocols was IS-IS developed in 1986 and later published in 1987 by ISO as ISO/IEC 10589. It was later republished as an IETF standard (RFC 1142 [http://tools.ietf.org/html/rfc1142]).

CONTENTS

- Section 12.6.1, “IS-IS Concepts”
- Section 12.6.2, “Configuring IS-IS”
- Section 12.6.3, “Viewing the Status of Neighbors”
- Section 12.6.4, “Viewing the Status of the Link-State Database”
- Section 12.6.5, “Managing Area Tags”
- Section 12.6.6, “Managing Interfaces”
- Section 12.6.7, “Managing LSP Generation”
- Section 12.6.8, “Managing SPF Calculations”

- Section 12.6.9, “Managing the Lifetime of LSPs”
- Section 12.6.10, “Managing LSP Refresh Intervals”
- Section 12.6.11, “Managing Network Entity Titles (NETs)”
- Section 12.6.12, “Managing Redistribution Metrics”

Section 12.6.1

IS-IS Concepts

IS-IS is an Interior Gateway Protocol (IGP) meant to exchange information within Autonomous Systems (AS). It is designed to operate within an administrative domain or network using link-state information to decide optimal data packet routing, similar to OSPF. IS-IS floods the network with link-state information and builds a database of the network's topology. The protocol computes the best path through the network (using Dijkstra's algorithm) and then forwards packets to their destination along that path.

Although it was originally designed as an ISO Connectionless-mode Network Protocol (CLNP), it was later adapted for IP network use (Dual IS-IS) in RFC 1195 [http://tools.ietf.org/html/rfc1195]. 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.

CONTENTS

- Section 12.6.1.1, “IS-IS Routers”
- Section 12.6.1.2, “Network Entity Title (NET) Addresses”
- Section 12.6.1.3, “Advantages and Disadvantages of Using IS-IS”

Section 12.6.1.1

IS-IS Routers

IS-IS routers can be defined as Level-1, Level-2, or both. Level 1 routers form the area, while Level 2 routers form the backbone of the network. By default, RUGGEDCOM ROX II configures areas to be both (or Level-1-2). This allows the device to inter-operate between different areas with minimal configuration.

- **Level-1** routers are intra-area routers. They maintain a single Link-State Database (LSD) that only contains information about the Level-1 and Level-2 neighbors in its area. To communicate with routers in another area, Level-1 routers forward traffic through their closest Level-2 router.
- **Level-2** routers are inter-area routers, meaning they can communicate with routers in other areas. They also maintain a single LSD, but it only contains information about other Level-2 routers from the router's area or other areas. The router knows nothing about the Level-1 routers in its area.
- **Level-1-2** routers are both inter- and intra-area routers, meaning they can communicate with Level-1 and Level-2 routers in any area. They maintain separate LSDs for Level-1 and Level-2 routers in and outside the router's area.

Section 12.6.1.2
Network Entity Title (NET) Addresses

IS-IS routers are identified by their Network Entity Title (NET) address, which is in Network Service Access Point (NSAP) format (RFC 1237 [http://tools.ietf.org/html/rfc1237]). 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)
```

Section 12.6.1.3
Advantages and Disadvantages of Using IS-IS

The advantages and disadvantages of using IS-IS include the following:

Advantages

- runs natively on the OSI network layer
- can support both IPv4 and IPv6 networks due to 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

Section 12.6.2
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 Section 12.6.5, “Managing Area Tags”.

4. Configure one or more interfaces on which to perform IS-IS routing. For more information, refer to Section 12.6.6, "Managing Interfaces".
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.

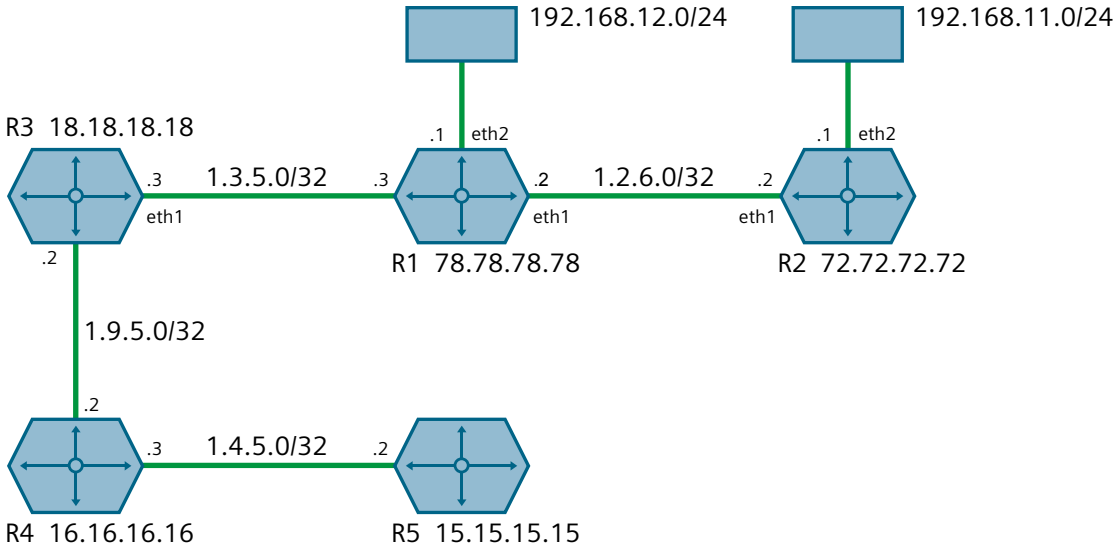


Figure 25: Multi-Level IS-IS Configuration

Section 12.6.3

Viewing the Status of Neighbors

To view the status of neighboring devices on an IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to Section 12.6.2, "Configuring IS-IS".
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.
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).

Section 12.6.4

Viewing the Status of the Link-State Database

To view the basic status of the link-state database for the IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to Section 12.6.2, "Configuring IS-IS".
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.

Section 12.6.5

Managing Area Tags

An IS-IS area is a grouping of inter-connected (or neighboring) IS-IS configured routers. As opposed to OSPF, where an Area Border Router (ABR) can exist in two areas at once, IS-IS routers reside only in one area. It is the link between routers in two different areas that forms the border. This is because an IS-IS router has only one Network Service Access Point (NSAP) address.

A single router can be configured to act as a Level-1, Level-2 or Level-1-2 router in one or more areas.

Routers are associated with areas by area tags, which define the routing type, metric, and authentication/ authorization rules.

CONTENTS

- Section 12.6.5.1, “Viewing a List of Area Tags”
- Section 12.6.5.2, “Adding an Area Tag”
- Section 12.6.5.3, “Deleting an Area Tag”

Section 12.6.5.1
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 Section 12.6.5.2, “Adding an Area Tag”.

Section 12.6.5.2
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-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 1 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 1 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 Section 12.6.11, "Managing Network Entity Titles (NETs)".
5. If necessary, configure intervals for the generation of Link-State Packets (LSPs). The default is 30 seconds. For more information, refer to Section 12.6.7, "Managing LSP Generation".
6. If necessary, configure refresh intervals for Link-State Packets (LSPs). The default is 900 seconds. For more information, refer to Section 12.6.10, "Managing LSP Refresh Intervals".
7. If necessary, configure the minimum interval between consecutive SPF calculations. The default is 1 second. For more information, refer to Section 12.6.8, "Managing SPF Calculations".
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 Section 12.6.9, "Managing the Lifetime of LSPs".
9. If necessary, define rules for redistributing static, RIP, BGP or OSPF routes. For more information, refer to Section 12.6.12, "Managing Redistribution Metrics".
10. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.6.5.3
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, or type **revert** and press **Enter** to abort.

Section 12.6.6
Managing Interfaces

IS-IS transmits hello packets and Link-State Packets (LSPs) through IS-IS enabled interfaces.

> **NOTE**
> *IS-IS is only supported on Ethernet interfaces.*

CONTENTS

- Section 12.6.6.1, “Viewing a List of Interfaces”
- Section 12.6.6.2, “Configuring an Interface”

Section 12.6.6.1
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  INTERVAL
 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 Section 8.5, “Managing VLANs”.

Section 12.6.6.2
Configuring an Interface

When IS-IS is enabled, the *switch.0001* interface is already configured.

To configure optional parameters for this 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 Section 8.5, "Managing VLANs".

3. Configure the following parameter(s) as required:

Parameter	Description
{ ifname }	**Synopsis:** A string Interface name.
ipv4-area-tag { ipv4-area-tag }	**Synopsis:** A string 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	**Synopsis:** { true, false } **Default:** false Enable or disable point-to-point network communication
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 1 to 254 characters long The value to be used as a transmit password in IIH PDUs transmitted by this Intermediate System.
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:** A 32-bit signed 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:** A 16-bit unsigned integer between 1 and 600 **Default:** 10 CSNP interval in seconds, ranging from 1 to 600. Default is 10.
hello-interval { hello-interval }	**Synopsis:** A 16-bit unsigned integer between 1 and 600 **Default:** 3

Parameter	Description
	Hello interval in seconds, ranging from 1 to 600. Default is 3.
hello-multiplier { hello-multiplier }	**Synopsis:** A 16-bit unsigned 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 8-bit unsigned 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, or type **`revert`** and press **Enter** to abort.

Section 12.6.7
Managing LSP Generation

IS-IS generates new Link-State Packets (LSPs) every 30 seconds by default. However, the interval can be configured anywhere between 1 and 120 seconds.

Since the introduction of a new LSP causes other routers in the area to recalculate routes, it is recommended to increase the interval to decrease flooding during periods of network instability, so as to reduce the load on other routers in the area.

CONTENTS

- Section 12.6.7.1, “Viewing a List of LSP Generation Intervals”
- Section 12.6.7.2, “Adding an LSP Generation Interval”
- Section 12.6.7.3, “Deleting an LSP Generation Interval”

Section 12.6.7.1
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 Section 12.6.7.2, “Adding an LSP Generation Interval”.

Section 12.6.7.2
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 [ 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, or type **revert** and press **Enter** to abort.

Section 12.6.7.3
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, or type **revert** and press **Enter** to abort.

Section 12.6.8
Managing SPF Calculations

IS-IS uses the Shortest Path First (SPF) algorithm to determine the best routes to every known destination in the network. When the network topology (not external links) changes, a partial recalculation is required.

IS-IS can be configured to perform the SPF calculation every 1 to 120 seconds. By default, IS-IS performs the SPF calculation every second. which could potentially be processor intensive, depending on the size of the area and how often the topology changes.

CONTENTS

- Section 12.6.8.1, “Viewing a List of SPF Calculation Intervals”
- Section 12.6.8.2, “Adding an SPF Calculation Interval”
- Section 12.6.8.3, “Deleting an SPF Calculation Interval”

Section 12.6.8.1
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 Section 12.6.8.2, "Adding an SPF Calculation Interval".

Section 12.6.8.2
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 [ 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, or type **revert** and press **Enter** to abort.

Section 12.6.8.3
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 [ 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, or type **revert** and press **Enter** to abort.

Section 12.6.9
Managing the Lifetime of LSPs

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, the maximum time limit is 1200 seconds. However, this interval can be customized for different routing types within the range of 350 to 65535 seconds if needed.

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 Section 12.6.10, "Managing LSP Refresh Intervals".

CONTENTS

- Section 12.6.9.1, "Viewing a List of LSP Lifetime Intervals"
- Section 12.6.9.2, "Adding an LSP Lifetime Interval"
- Section 12.6.9.3, "Deleting an LSP Lifetime Interval"

Section 12.6.9.1
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-lifetime
```

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 Section 12.6.9.2, "Adding an LSP Lifetime Interval".

Section 12.6.9.2
Adding an LSP Lifetime Interval

To add an LSP lifetime interval to an IS-IS area, do the following:

IMPORTANT!
The LSP lifetime interval must be 300 seconds higher than the LSP refresh interval. For more information about LSP refresh intervals, refer to Section 12.6.10, "Managing LSP Refresh Intervals".

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 [ 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, or type **revert** and press **Enter** to abort.

Section 12.6.9.3
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, or type **revert** and press **Enter** to abort.

Section 12.6.10
Managing LSP Refresh Intervals

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, LSPs are retained in the LSDB for 1200 seconds (this is referred to as the *lifetime* of the LSP) and are refreshed every 900 seconds.

The refresh interval is configurable for each area and routing type in the IS-IS network.

NOTE
For information about configuring the lifetime of an LSP, refer to Section 12.6.9, "Managing the Lifetime of LSPs".

CONTENTS

- Section 12.6.10.1, "Viewing a List of LSP Refresh Intervals"
- Section 12.6.10.2, "Adding an LSP Refresh Interval"
- Section 12.6.10.3, "Deleting an LSP Refresh Interval"

Section 12.6.10.1
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-refresh-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 Section 12.6.10.2, "Adding an LSP Refresh Interval".

Section 12.6.10.2
Adding an LSP Refresh Interval

To add an LSP refresh interval to an IS-IS area, do the following:

IMPORTANT!
The LSP refresh interval must be 300 seconds less than the LSP lifetime interval. For more information about LSP refresh intervals, refer to Section 12.6.9, "Managing the Lifetime of LSPs".

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, or type **revert** and press **Enter** to abort.

Section 12.6.10.3
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, or type **revert** and press **Enter** to abort.

Section 12.6.11
Managing Network Entity Titles (NETs)

Network Entity Titles (NETs) define the area address and system ID for the router. Traffic received from another router that shares the same area address and system ID will be forwarded to this router.

RUGGEDCOM ROX II supports IS-IS multi-homing, which allows for multiple NETs to be defined for a single router and increases the list of possible traffic sources.

Each NET has a hexadecimal value, which can be between 8 and 20 octets long, although 10 octets is most common. The value includes an Authority and Format Identifier (AFI), an area ID, a system identifier, and a selector. The following is an example of an NET address:

```
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.

IMPORTANT!
The system identifier must be unique to the network.

CONTENTS

- Section 12.6.11.1, "Viewing a List of NETs"
- Section 12.6.11.2, "Adding a NET"
- Section 12.6.11.3, "Deleting a NET"

Section 12.6.11.1
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 Section 12.6.11.2, "Adding a NET".

Section 12.6.11.2
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, or type **revert** and press **Enter** to abort.

Section 12.6.11.3
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, or type **revert** and press **Enter** to abort.

Section 12.6.12
Managing Redistribution Metrics

Redistribution in general is the advertisement of routes by one protocol that have been learned via another dynamic routing protocol, a static route, or a directly connected router. It is deployed to promote interoperability between networks running different routing protocols.

The redistribution of a route is achieved by defining a metric for the source routing protocol. As each routing protocol calculates routes differently, care must be taken to define a metric that is understood by the protocol.

There are two types of metrics: internal and external. Both types can be assigned a value between 0 and 63. However, to prevent external metrics from competing with internal metrics, 64 is automatically added to any external metric. This puts external metrics in the range of 64 to 128, even though the metric value defined is only in the range of 0 to 63.

There is no default metric for IS-IS. A metric should be defined for each routing protocol, otherwise a metric value of zero (0) is automatically applied.

CONTENTS

- Section 12.6.12.1, “Viewing a List of Redistribution Metrics”
- Section 12.6.12.2, “Adding a Redistribution Metric”
- Section 12.6.12.3, “Deleting a Redistribution Metric”

Section 12.6.12.1
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 Section 12.6.12.2, "Adding a Redistribution Metric".

Section 12.6.12.2
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:** A 32-bit unsigned integer between 0 and 16777214 The metric for redistributed routes.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.6.12.3
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, or type **revert** and press **Enter** to abort.

Section 12.7

Managing RIP

The Routing Information Protocol (RIP) determines the best path for routing IP traffic over a TCP/IP network based on the number of hops between any two routers. It uses the shortest route available to a given network as the route to use for sending packets to that network.

The RUGGEDCOM ROX II RIP daemon is an RFC 1058 [http://tools.ietf.org/rfc/rfc1058.txt] 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, 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 Section 12.9, “Managing OSPF”.

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.

CONTENTS

- Section 12.7.1, “Configuring RIP”
- Section 12.7.2, “Viewing the Status of Dynamic RIP Routes”
- Section 12.7.3, “Managing Prefix Lists and Entries”
- Section 12.7.4, “Managing Networks”
- Section 12.7.5, “Managing Network IP Addresses”
- Section 12.7.6, “Managing Network Interfaces”
- Section 12.7.7, “Managing Neighbors”
- Section 12.7.8, “Managing the Prefix List Distribution”
- Section 12.7.9, “Managing Key Chains and Keys”
- Section 12.7.10, “Managing Redistribution Metrics”
- Section 12.7.11, “Managing Routing Interfaces”

Section 12.7.1
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
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 8-bit signed 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:** A 32-bit unsigned integer between 1 and 255 Sets the default RIP distance.
version { version }	**Synopsis:** An 8-bit signed 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 Section 12.7.3.3, “Adding a Prefix List”.
4. Configure a network. For more information, refer to Section 12.7.4.1, “Configuring a Network”.
5. Configure the prefix list distribution. For more information, refer to Section 12.7.8.2, “Adding a Prefix List Distribution Path”.
6. Configure key chains. For more information, refer to Section 12.7.9.3, “Adding a Key Chain”.
7. Configure redistribution metrics. For more information, refer to Section 12.7.10.2, “Adding a Redistribution Metric”.
8. Configure interfaces. For more information, refer to Section 12.7.11.2, “Configuring a Routing Interface”.
9. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.7.2
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.

Parameter	Description
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 Section 12.7.1, "Configuring RIP".

Section 12.7.3

Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the RIPs daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

CONTENTS

- Section 12.7.3.1, "Viewing a List of Prefix Lists"
- Section 12.7.3.2, "Viewing a List of Prefix Entries"
- Section 12.7.3.3, "Adding a Prefix List"
- Section 12.7.3.4, "Adding a Prefix Entry"
- Section 12.7.3.5, "Deleting a Prefix List"
- Section 12.7.3.6, "Deleting a Prefix Entry"

Section 12.7.3.1

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 Section 12.7.3.3, "Adding a Prefix List".

Section 12.7.3.2
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 Section 12.7.3.4, "Adding a Prefix Entry".

Section 12.7.3.3
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 1 to 1024 characters long The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to Section 12.7.3.4, "Adding a Prefix Entry".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.3.4
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 9 to 18 characters long The IPv4 network address and prefix. This parameter is mandatory.
le { le }	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The maximum prefix length to be matched.
ge { ge }	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The minimum prefix length to be matched.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.3.5
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, or type **revert** and press **Enter** to abort.

Section 12.7.3.6
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 number
```

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, or type **revert** and press **Enter** to abort.

Section 12.7.4

Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

NOTE
For point to point links, specify neighbors instead of a network. For more information, refer to Section 12.7.7.2, "Adding a Neighbor".

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 Section 12.7.7, "Managing Neighbors".

CONTENTS

- Section 12.7.4.1, "Configuring a Network"
- Section 12.7.4.2, "Tracking Commands"

Section 12.7.4.1

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 Section 12.7.5.2, "Adding a Network IP Address".
3. Add one or more network interfaces. For more information, refer to Section 12.7.6.2, "Adding a Network Interface".
4. Add one or more neighbors. For more information, refer to Section 12.7.7.2, "Adding a Neighbor".

Section 12.7.4.2
Tracking Commands

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 12.5, "Managing Event Trackers".

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 Selects an event to track. The distribute-prefix-list is applied only when the tracked event is in the UP state. This parameter is mandatory.
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, or type **`revert`** and press **Enter** to abort.

Section 12.7.5
Managing Network IP Addresses

This section describes how to manage IP addresses for RIP networks.

CONTENTS

- Section 12.7.5.1, "Viewing a List of Network IP Addresses"
- Section 12.7.5.2, "Adding a Network IP Address"
- Section 12.7.5.3, "Deleting a Network IP Address"

Section 12.7.5.1
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 Section 12.7.5.2, "Adding a Network IP Address".

Section 12.7.5.2
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, or type **revert** and press **Enter** to abort.

Section 12.7.5.3
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, or type **revert** and press **Enter** to abort.

Section 12.7.6
Managing Network Interfaces

This section describes how to manage interfaces used by RIP networks.

CONTENTS

- Section 12.7.6.1, "Viewing a List of Network Interfaces"
- Section 12.7.6.2, "Adding a Network Interface"
- Section 12.7.6.3, "Deleting a Network Interface"

Section 12.7.6.1
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 neighbors as needed. For more information, refer to Section 12.7.7.2, "Adding a Neighbor".

Section 12.7.6.2
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, or type **revert** and press **Enter** to abort.

Section 12.7.6.3
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, or type **revert** and press **Enter** to abort.

Section 12.7.7
Managing Neighbors

Neighbors are other routers with which to exchange routes.

CONTENTS

- Section 12.7.7.1, "Viewing a List of Neighbors"
- Section 12.7.7.2, "Adding a Neighbor"
- Section 12.7.7.3, "Deleting a Neighbor"

Section 12.7.7.1
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 Section 12.7.7.2, "Adding a Neighbor".

Section 12.7.7.2
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, or type **revert** and press **Enter** to abort.

Section 12.7.7.3
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, or type **revert** and press **Enter** to abort.

Section 12.7.8

Managing the Prefix List Distribution

This section describes how to manage the distribution of prefix lists.

CONTENTS

- Section 12.7.8.1, "Viewing a List of Prefix List Distribution Paths"
- Section 12.7.8.2, "Adding a Prefix List Distribution Path"
- Section 12.7.8.3, "Deleting a Prefix List Distribution Path"

Section 12.7.8.1

Viewing a List of Prefix List Distribution Paths

To view a list of prefix list distribution paths for dynamic RIP routes, 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 Section 12.7.8.2, "Adding a Prefix List Distribution Path".

Section 12.7.8.2

Adding a Prefix List Distribution Path

To add a prefix list distribution path for dynamic RIP routes, do the following:

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

```
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. Configure the following parameter(s) as required:

Parameter	Description
prefix-list { prefix-list }	**Synopsis:** A string The name of the prefix list. This parameter is mandatory.

4. If necessary, configure an event tracker to track network commands. For more information, refer to Section 12.7.4.2, "Tracking Commands".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.8.3
Deleting a Prefix List Distribution Path

To delete a prefix list distribution path for dynamic RIP routes, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 12.7.9
Managing Key Chains and Keys

Key chains are collections of keys (or shared secrets), which are used to authenticate communications over a dynamic RIP network. Only routers with the same key are able to send and receive advertisements.

Multiple key chains can be configured for different groups of interfaces and the lifetime for each key within a chain can be separately configured.

CONTENTS

- Section 12.7.9.1, "Viewing a List of Key Chains"
- Section 12.7.9.2, "Viewing a List of Keys"
- Section 12.7.9.3, "Adding a Key Chain"
- Section 12.7.9.4, "Adding a Key"
- Section 12.7.9.5, "Deleting a Key Chain"
- Section 12.7.9.6, "Deleting a Key"

Section 12.7.9.1
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 Section 12.7.9.3, "Adding a Key Chain".

Section 12.7.9.2
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 Section 12.7.9.4, "Adding a Key".

Section 12.7.9.3
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 Section 12.7.9.4, "Adding a Key".
4. Configure a routing interface to use the key chain for authentication purposes. For more information, refer to Section 12.7.11.2, "Configuring a Routing Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.9.4

Adding a Key

Keys (or shared secrets) are used to authenticate communications over a RIP network. To maintain network stability, each key is assigned an accept and send lifetime.

The *accept* lifetime is the time period in which the key is accepted by the device.

The *send* lifetime is the time period in which 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:** { infinite } or a string 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:** { infinite } or a string The time at which the key expires.

6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.9.5
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, or type **revert** and press **Enter** to abort.

Section 12.7.9.6
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, or type **revert** and press **Enter** to abort.

Section 12.7.10

Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the RIP networks, can also be advertised.

CONTENTS

- Section 12.7.10.1, "Viewing a List of Redistribution Metrics"
- Section 12.7.10.2, "Adding a Redistribution Metric"
- Section 12.7.10.3, "Deleting a Redistribution Metric"

Section 12.7.10.1

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 Section 12.7.10.2, "Adding a Redistribution Metric".

Section 12.7.10.2

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 | connected | static | kernel ]
   ```

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.10.3

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 | connected | static | kernel ]
```

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.7.11
Managing Routing Interfaces

This section describes how to manage interfaces for RIP routes.

CONTENTS

- Section 12.7.11.1, "Viewing a List of Routing Interfaces"
- Section 12.7.11.2, "Configuring a Routing Interface"

Section 12.7.11.1
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
```

Section 12.7.11.2
Configuring a Routing Interface

To configure a routing interface for a RIP network, do the following:

NOTE
OSPF regards router interfaces as either passive or active, sending OSPF messages on active interfaces and ignoring passive interfaces.

1. 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

Parameter	Description
	The authentication key chain.
string { string }	**Synopsis:** A string 1 to 16 characters long The authentication string.

4. Configure the interface settings by typing the following commands:

Parameter	Description
{ ifname }	**Synopsis:** A string 1 to 32 characters long The name of the interface.
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.
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.
mode { mode }	**Synopsis:** { md5-rfc, md5-old-ripd, text, none } The authentication mode.
key-chain { key-chain }	**Synopsis:** A string The authentication key chain.
string { string }	**Synopsis:** A string 1 to 16 characters long The authentication string.

5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.8
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.

CONTENTS

- Section 12.8.1, "Configuring BGP"
- Section 12.8.2, "Managing Route Maps"
- Section 12.8.3, "Managing Prepended and Excluded Autonomous System Path Filters"
- Section 12.8.4, "Managing Prefix Lists and Entries"
- Section 12.8.5, "Managing Autonomous System Paths and Entries"
- Section 12.8.6, "Managing Neighbors"
- Section 12.8.7, "Managing Networks"
- Section 12.8.8, "Managing Aggregate Addresses"
- Section 12.8.9, "Managing Aggregate Address Options"
- Section 12.8.10, "Managing Redistribution Metrics"
- Section 12.8.11, "Managing Route Reflector Options"
- Section 12.8.12, "Viewing the Status of Dynamic BGP Routes"
- Section 12.8.13, "Resetting a BGP Session"

Section 12.8.1
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.
as-id { as-id }	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 Autonomous System ID.
always-compare-med	Always comparing MED from different neighbors.
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:** A 32-bit unsigned integer **Default:** 100 Default local preference value.
deterministic-med	Pick the best-MED path among paths advertised from neighboring AS.

Parameter	Description
router-id { router-id }	**Synopsis:** A string 7 to 15 characters long Router ID for BGP.

3. Configure autonomous system path filters. For more information, refer to Section 12.8.5.3, "Adding an Autonomous System Path Filter".
4. Configure prefix list filters. For more information, refer to Section 12.8.4.3, "Adding a Prefix List".
5. Configure route map filters. For more information, refer to Section 12.8.2.3, "Adding a Route Map Filter".
6. Configure a network. For more information, refer to Section 12.8.7.2, "Adding a Network".
7. Configure IP addresses for neighbors. For more information, refer to Section 12.8.6.2, "Adding a Neighbor".
8. Configure aggregate addresses. For more information, refer to Section 12.8.8.2, "Adding an Aggregate Address".
9. Configure redistribution metrics. For more information, refer to Section 12.8.10.2, "Adding a Redistribution Metric".
10. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

> **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 Section 12.8.13, "Resetting a BGP Session".

Section 12.8.2

Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

CONTENTS

- Section 12.8.2.1, "Viewing a List of Route Map Filters"
- Section 12.8.2.2, "Viewing a List of Route Map Filter Entries"
- Section 12.8.2.3, "Adding a Route Map Filter"
- Section 12.8.2.4, "Adding a Route Map Filter Entry"
- Section 12.8.2.5, "Deleting a Route Map Filter"
- Section 12.8.2.6, "Deleting a Route Map Filter Entry"
- Section 12.8.2.7, "Configuring Match Rules"
- Section 12.8.2.8, "Configuring a Set"

Section 12.8.2.1
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    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 Section 12.8.5.3, "Adding an Autonomous System Path Filter".

Section 12.8.2.2
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 entry
```

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
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
-------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -          -
      -      -     -       -           -

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 12.8.5.3, "Adding an Autonomous System Path Filter".

Section 12.8.2.3
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 Section 12.8.2.4, "Adding a Route Map Filter Entry".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.2.4
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 Jump to another route-map after match+set.
on-match-goto { on-match-goto }	**Synopsis:** A string Go to this entry on match.

4. Configure the match rules for the route map filter. For more information, refer to Section 12.8.2.7, "Configuring Match Rules".
5. Configure a set for the route map filter. For more information, refer to Section 12.8.2.8, "Configuring a Set".
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.2.5
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, or type **revert** and press **Enter** to abort.

Section 12.8.2.6
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, or type **revert** and press **Enter** to abort.

Section 12.8.2.7
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 as required:

Parameter	Description
as-path { as-path }	**Synopsis:** A string Match the BGP AS path filter.
metric { metric }	**Synopsis:** A 32-bit unsigned integer Match the route metric.
peer { peer }	**Synopsis:** A string 7 to 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. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.2.8
Configuring a Set

To configure matched 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} » set***, where *{tag}* is the tag for the route map filter and *{number}* is the sequence number for the entry.
3. Configure the following parameters as required:

Parameter	Description
local-preference { local-preference }	**Synopsis:** A 32-bit unsigned integer Local preference.
next-hop { next-hop }	**Synopsis:** { peer } or a string 7 to 15 characters long 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 7 to 15 characters long This parameter is not supported and any value is ignored by the system.
weight { weight }	**Synopsis:** A 32-bit unsigned integer Weight.

4. Add pre-pended and/or excluded autonomous system paths. For more information, refer to Section 12.8.3.3, "Adding a Prepended Autonomous System Path Filter" and/or Section 12.8.3.4, "Adding an Excluded Autonomous System Path filter".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.8.3
Managing Prepended and Excluded Autonomous System Path Filters

This section describes how to configure and manage prepended and excluded autonomous system path filters.

CONTENTS

- Section 12.8.3.1, "Viewing a List of Prepended Autonomous System Path Filters"
- Section 12.8.3.2, "Viewing a List of Excluded Autonomous System Paths"
- Section 12.8.3.3, "Adding a Prepended Autonomous System Path Filter"
- Section 12.8.3.4, "Adding an Excluded Autonomous System Path filter"
- Section 12.8.3.5, "Deleting a Prepended Autonomous System Path Filter"
- Section 12.8.3.6, "Deleting an Excluded Autonomous System Path Filter"

Section 12.8.3.1
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 entry number set as-path prepend
```

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 prepend
routing bgp
 filter route-map route
  entry 10
   set as-path prepend 120
   !
  !
 !
!
```

If no prepended autonomous system path filters have been configured, add filters as needed. For more information, refer to Section 12.8.3.3, "Adding a Prepended Autonomous System Path Filter".

Section 12.8.3.2
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 entry 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 Section 12.8.3.4, "Adding an Excluded Autonomous System Path filter".

Section 12.8.3.3
Adding a Prepended Autonomous System Path Filter

To add a prepended autonomous system path filter to a BGP route map entry, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 12.8.3.4
Adding an Excluded Autonomous System Path filter

To add an excluded autonomous system path filter to a BGP route map entry, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 12.8.3.5
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, or type **revert** and press **Enter** to abort.

Section 12.8.3.6
Deleting an Excluded Autonomous System Path Filter

To delete an excluded autonomous system path filter from a BGP route map entry, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 12.8.4
Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the BGP daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

CONTENTS

- Section 12.8.4.1, "Viewing a List of Prefix Lists"
- Section 12.8.4.2, "Viewing a List of Prefix Entries"
- Section 12.8.4.3, "Adding a Prefix List"
- Section 12.8.4.4, "Adding a Prefix Entry"
- Section 12.8.4.5, "Deleting a Prefix List"
- Section 12.8.4.6, "Deleting a Prefix Entry"

Section 12.8.4.1
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 Section 12.8.4.3, "Adding a Prefix List".

Section 12.8.4.2
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 Section 12.8.4.4, "Adding a Prefix Entry".

Section 12.8.4.3
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 1 to 1024 characters long The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to Section 12.8.4.4, "Adding a Prefix Entry".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.4.4
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 9 to 18 characters long Network (xxx.xxx.xxx.xxx/xx). This parameter is mandatory.
le { le }	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
ge { ge }	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.4.5
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, or type **revert** and press **Enter** to abort.

Section 12.8.4.6
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 number
   ```

   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, or type **revert** and press **Enter** to abort.

Section 12.8.5
Managing Autonomous System Paths and Entries

This section describes how to configure autonomous system paths and entries for dynamic BGP routes.

CONTENTS

- Section 12.8.5.1, "Viewing a List of Autonomous System Paths"
- Section 12.8.5.2, "Viewing a List of Autonomous System Path Entries"
- Section 12.8.5.3, "Adding an Autonomous System Path Filter"
- Section 12.8.5.4, "Adding an Autonomous System Path Filter Entry"
- Section 12.8.5.5, "Deleting an Autonomous System Path"
- Section 12.8.5.6, "Deleting an Autonomous System Path Filter Entry"

Section 12.8.5.1
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 Section 12.8.5.3, "Adding an Autonomous System Path Filter".

Section 12.8.5.2
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 Section 12.8.5.3, "Adding an Autonomous System Path Filter".

Section 12.8.5.3
Adding an Autonomous System Path Filter

To add an autonomous system path filter for dynamic BGP routes, do the following:

1. 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 Section 12.8.5.4, "Adding an Autonomous System Path Filter Entry".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.5.4
Adding an Autonomous System Path Filter Entry

Create an entry for an autonomous system path filter to match a string or integer value in AS path and then perform an action. The match criteria is defined using regular expressions.

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 Section 2.5.7, "Using Regular Expressions".

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.5.5
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, or type **revert** and press **Enter** to abort.

Section 12.8.5.6
Deleting an Autonomous System Path Filter Entry

To delete an entry for an autonomous system path filter, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 12.8.6
Managing Neighbors

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for BGP to operate.

NOTE
If neighbors are specified but no networks are specified, the router will receive BGP routing information from its neighbors but will not advertise any routes to them. For more information about networks, refer to Section 12.8.7, "Managing Networks".

CONTENTS

- Section 12.8.6.1, "Viewing a List of Neighbors"
- Section 12.8.6.2, "Adding a Neighbor"
- Section 12.8.6.3, "Configuring the Distribution of Prefix Lists"
- Section 12.8.6.4, "Tracking Commands for BGP Neighbors"
- Section 12.8.6.5, "Deleting a Neighbor"

Section 12.8.6.1
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 Section 12.8.6.2, "Adding a Neighbor".

Section 12.8.6.2
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 Apply route map to incoming routes.
out { out }	**Synopsis:** A string 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:** A 32-bit unsigned integer between 1 and 65535 A BGP neighbor. This parameter is mandatory.
ebgp-multihop { ebgp-multihop }	**Synopsis:** An 8-bit unsigned integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
maximum-prefix { maximum-prefix }	**Synopsis:** A 32-bit unsigned 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 1 to 1024 characters long Password.
update-source { update-source }	**Synopsis:** A string 7 to 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:** A 16-bit unsigned integer The default weight for routes from this neighbor.

6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.8.6.3
Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in a BGP network, do the following:

1. Make sure the 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 Section 12.8.6.4, "Tracking Commands for BGP Neighbors".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.6.4
Tracking Commands for BGP Neighbors

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 12.5, "Managing Event Trackers".

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 Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state. This parameter is mandatory.
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, or type **revert** and press **Enter** to abort.

Section 12.8.6.5
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, or type **revert** and press **Enter** to abort.

Section 12.8.7
Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

NOTE
For point-to-point links, specify neighbors instead of a network. For more information, refer to Section 12.8.6.2, "Adding a Neighbor".

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 Section 12.8.6, "Managing Neighbors".

CONTENTS

- Section 12.8.7.1, "Viewing a List of Networks"
- Section 12.8.7.2, "Adding a Network"
- Section 12.8.7.3, "Tracking Commands for a BGP Network"
- Section 12.8.7.4, "Deleting a Network"

Section 12.8.7.1
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 Section 12.8.7.2, "Adding a Network".

Section 12.8.7.2
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 Section 12.8.7.3, "Tracking Commands for a BGP Network".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.7.3
Tracking Commands for a BGP Network

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 12.5, "Managing Event Trackers".

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 Select an event. This parameter is mandatory.
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, or type **revert** and press **Enter** to abort.

Section 12.8.7.4
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, or type **revert** and press **Enter** to abort.

Section 12.8.8

Managing Aggregate Addresses

This section describes how to aggregate multiple addresses into a single dynamic BGP route.

CONTENTS

- Section 12.8.8.1, "Viewing a List of Aggregate Addresses"
- Section 12.8.8.2, "Adding an Aggregate Address"
- Section 12.8.8.3, "Deleting an Aggregate Address"

Section 12.8.8.1

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 Section 12.8.8.2, "Adding an Aggregate Address".

Section 12.8.8.2

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 Section 12.8.9.2, "Adding an Aggregate Address Option".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.8.3
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, or type **revert** and press **Enter** to abort.

Section 12.8.9
Managing Aggregate Address Options

This section describes how to set the `as-set` and `summary-only` options for BGP aggregate addresses.

CONTENTS

- Section 12.8.9.1, "Viewing a List of Aggregate Address Options"
- Section 12.8.9.2, "Adding an Aggregate Address Option"
- Section 12.8.9.3, "Deleting an Aggregate Address Option"

Section 12.8.9.1
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 Section 12.8.9.2, "Adding an Aggregate Address Option".

Section 12.8.9.2
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 [ 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, or type **revert** and press **Enter** to abort.

Section 12.8.9.3
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, or type **revert** and press **Enter** to abort.

Section 12.8.10
Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the BGP network, can also be advertised.

CONTENTS

- Section 12.8.10.1, “Viewing a List of Redistribution Metrics”
- Section 12.8.10.2, “Adding a Redistribution Metric”
- Section 12.8.10.3, “Deleting a Redistribution Metric”

Section 12.8.10.1
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 Section 12.8.10.2, "Adding a Redistribution Metric".

Section 12.8.10.2
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 | connected | static | kernel ] metric metric
   ```

   Where:

   - *metric* is the metric for redistributed routes
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.10.3
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 | connected | static | kernel ]
   ```
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.11
Managing Route Reflector Options

This section describes how to configure the device as a route reflector for BGP networks.

CONTENTS

- Section 12.8.11.1, "Understanding Route Reflectors"
- Section 12.8.11.2, "Configuring the Device as a Route Reflector"
- Section 12.8.11.3, "Configuring BGP Neighbors as Clients"
- Section 12.8.11.4, "Example: Basic Route Reflection"
- Section 12.8.11.5, "Example: Linking Clusters"

- Section 12.8.11.6, "Example: Clusters in Clusters"
- Section 12.8.11.7, "Example: Route Reflection in a VRF Instance"
- Section 12.8.11.8, "Example: Route Reflection with VPNv4 Clients"

Section 12.8.11.1
Understanding Route Reflectors

Route reflectors offer a method for simplifying BGP network topologies and improving scalability.

The Full-Mesh Requirement

Due to BGP route advertisement rules, BGP requires a logical full-mesh topology, wherein each router advertises and forwards its routes to each of its neighbors. This requirement is easily met by external BGP (eBGP) networks, where connections are established between Autonomous Systems (AS). Routers can easily avoid loops by dropping any routes that share the same AS numeric identifier. However, in internal BGP (iBGP), each router shares the same AS numeric identifier, so all routes received by a router would be dropped.

One method for solving this problem is to have each iBGP router establish neighborship with its peers, but that would result in a significant number of BGP sessions and unnecessary traffic on large networks. The formula for determining the number of BGP sessions for X number of routers is **X*(X-1)/2**. Therefore, 20 iBGP routers would generate 190 BGP sessions (20*[20-1]/2 = 190).

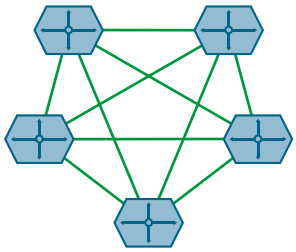


Figure 26: A Simple BGP Topology Without a Route Reflector

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.

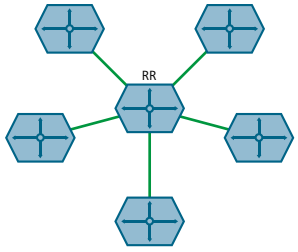


Figure 27: A Simple BGP Topology With a Route Reflector

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.

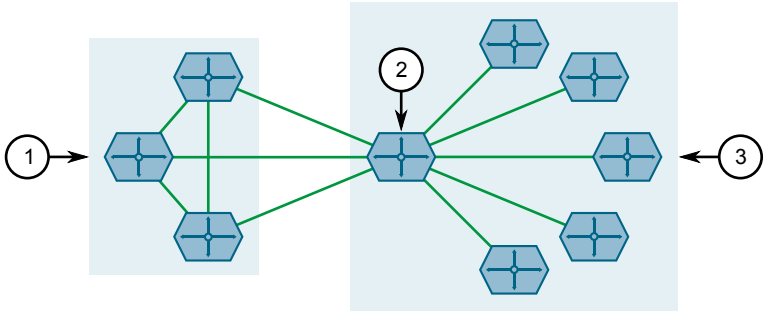


Figure 28: A Complex BGP Topology

1. Fully Meshed iBGP Peers (Non-Clients) **2.** Route Reflector **3.** Cluster (Clients)

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.

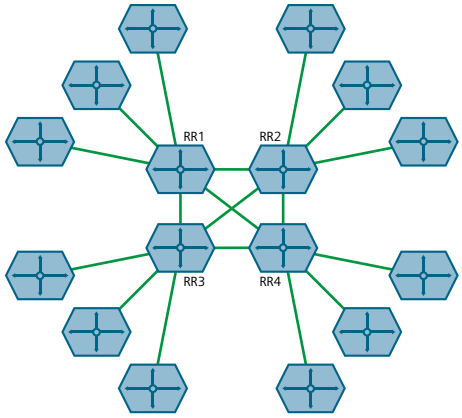


Figure 29: Multiple Clusters Fully-Meshed

Route reflectors can also be partially-meshed by combining them in a cluster of their own.

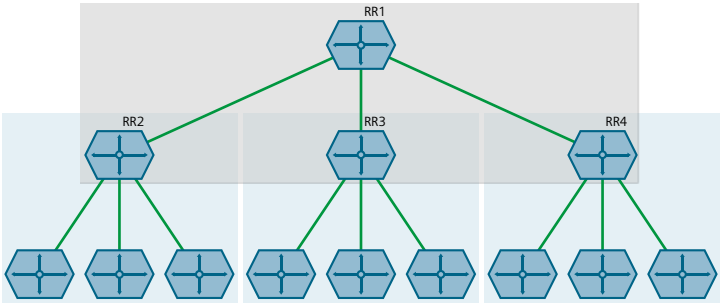


Figure 30: Multiple Clusters Partially-Meshed

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.

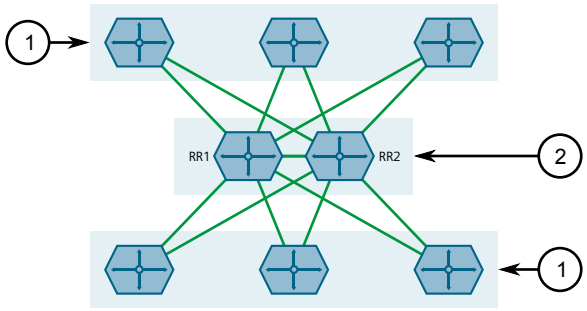


Figure 31: Redundant Route Reflector Topology

1. Cluster **2.** Route Reflector

Section 12.8.11.2
Configuring the Device as a Route Reflector

To configure the device to be a route reflector for a specific cluster, do the following:

1. 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 Section 12.8.11.3, "Configuring BGP Neighbors as Clients".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.11.3
Configuring BGP Neighbors as Clients

When the device is configured to be a route reflector, BGP neighbors can then be configured to be clients of the reflector.

BGP Neighbors

To configure a BGP neighbor to be a client of the device, do the following:

1. Make sure a BGP neighbor is defined. For more information, refer to Section 12.8.6.2, "Adding a Neighbor".
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, or type **revert** and press **Enter** to abort.

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 Section 12.11.10.2, "Adding an IPv4 Address Family".
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, or type **revert** and press **Enter** to abort.

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 Section 12.11.9.2, "Adding a Neighbor".
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-reflector-client enabled
   ```

   Where *address* is the IP address of the BGP neighbor.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.8.11.4

Example: Basic Route Reflection

This example demonstrates how to configure a partially-meshed Autonomous System (AS) where a route reflector advertises routes to clients and non-clients.

Overview

In the following topology, routes advertised by the external BGP (eBGP) router (labeled as R1) are forwarded to the route reflector (labeled as RR). The route reflector then in turn readvertises the routes to its BGP neighbors. Neighbors within the route reflector's cluster are the clients (labeled C1, C2 and C3). Neighbors outside of the cluster are non-clients (labeled NC1, NC2 and NC3).

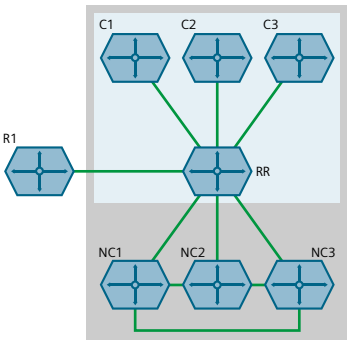


Figure 32: Basic Route Reflection Topology

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 Section 12.8.11.2, "Configuring the Device as a Route Reflector".
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 Section 12.8.6.2, "Adding a Neighbor".
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 Section 12.8.11.3, "Configuring BGP Neighbors as Clients".

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
 !
!
```

Section 12.8.11.5

Example: Linking Clusters

This example demonstrates how to link two multiple clusters together by connecting each route reflector in a full-mesh topology.

Overview

In the following topology, three route reflectors (RR1, RR2 and RR3) are internal peers of one another.

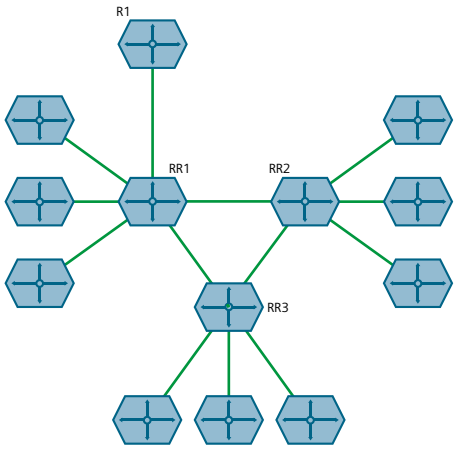


Figure 33: Linked Clusters

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 Section 12.8.11.2, "Configuring the Device as a Route Reflector".
2. For each route reflector, define the other route reflectors as BGP neighbors. For more information, refer to Section 12.8.6.2, "Adding a Neighbor".

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
 !
!
```

Section 12.8.11.6

Example: Clusters in Clusters

This example demonstrates how to group clusters into a hierarchical structure (clusters of clusters).

Overview

In the following topology, a route reflector (RR1) forms a cluster with two other route reflectors (RR2 and RR3). RR2 and RR3 are also part of their own individual clusters, each of which consists of three clients.

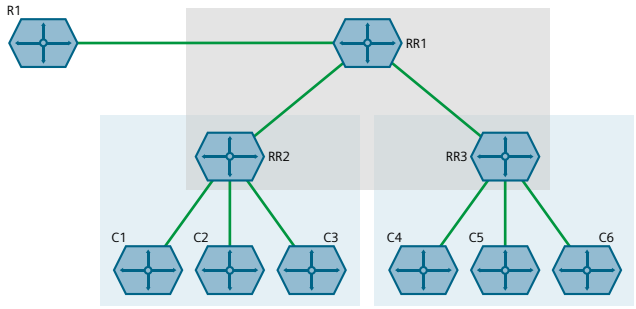


Figure 34: Hierarchical Clusters Topology

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 Section 12.8.11.2, "Configuring the Device as a Route Reflector".
2. Configure RR1 as a route reflector and define RR2 and RR3 as its clients. For more information, refer to Section 12.8.11.2, "Configuring the Device as a Route Reflector".

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
 !
!
```

Section 12.8.11.7

Example: Route Reflection in a VRF Instance

This example demonstrates how to configure BGP route reflection in a VRF instance.

Overview

In the following topology, router RR is a BGP route reflector configured with a VRF instance (VRF1). The VRF instance is configured with a single IPv4 address family consisting of routers R2 and R3. All three routers belong to the same autonomous system (AS1).

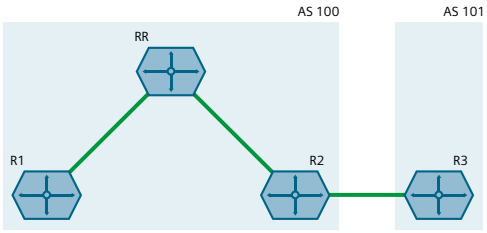


Figure 35: Route Reflection in a VRF Instance

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 Section 12.11.5.2, "Adding a VRF Definition".
   b. Define a route target for VRF1 of type `both` with the export community set to **100:1**. For more information, refer to Section 12.11.6.2, "Adding a Route Target".
   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 1.c to forward traffic to VRF1. For more information, refer to Section 12.11.4, "Configuring a VRF Interface".
   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 Section 12.8.11.2, "Configuring the Device as a Route Reflector".

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 Section 12.11.10.2, "Adding an IPv4 Address Family".

h. Define a redistribution metric for IPv4 family of type `connected`. For more information, refer to Section 12.11.11.2, "Adding a Redistribution".

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 Section 12.8.1, "Configuring BGP".

b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.1.2
Autonomous System ID	100

For more information, refer to Section 12.8.6.2, "Adding a Neighbor".

c. Define a redistribution metric for BGP of type `connected`. For more information, refer to Section 12.8.10.2, "Adding a Redistribution Metric".

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 Section 12.8.1, "Configuring BGP".

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 Section 12.8.6.2, "Adding a Neighbor".

c. Define a redistribution metric for BGP of type `connected`. For more information, refer to Section 12.8.10.2, "Adding a Redistribution Metric".

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 Section 12.8.1, "Configuring BGP".

b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.3.1
Autonomous System ID	101

For more information, refer to Section 12.8.6.2, "Adding a Neighbor".

c. Define a redistribution metric for BGP of type `connected`. For more information, refer to Section 12.8.10.2, "Adding a Redistribution Metric".

» 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
```

Section 12.8.11.8

Example: Route Reflection with VPNv4 Clients

BGP route reflection can be used to advertise VPNv4 routes between Provider Edge (PE) devices inside a provider network. This specific application is complicated by the fact that VPNv4 routes to the Customer Edge (CE) devices are within VRFs that are not known to the global VRF shared by each PE device.

For more information about configuring this type of topology, refer to the application description *Using BGP Route Reflection with VPNv4 Clients [https://support.industry.siemens.com/cs/ww/en/view/109757209]*.

Section 12.8.12

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.
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:** A 32-bit signed integer Metric value.
local-preference	**Synopsis:** A string Local preference.
weight	**Synopsis:** A 32-bit signed integer Weight.
as-path	**Synopsis:** A string Path.
origin	**Synopsis:** A string Origin.

To view the status of the dynamic BGP neighbor configured on the device, type:

```
show routing status bgp neighbor
```

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

```
ruggedcom# show routing status bgp neighbor | tab
                                                                    PREFIX
                              LOCAL               AS
ID          VERSION  AS    MSGRCVD  MSGSENT  UPTIME    STATE        RECEIVED  NETWORK        NEXT HOP
  SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
-------------------------------------------------------------------------------------------------------
13.13.13.2  4        2122  982      984      16:18:04  Established  2
                                                                              13.13.13.0/30  13.13.13.1
  true      false     0                   32768         IGP
                                                                              192.168.12.0   13.13.13.1
  true      false     2                   32768         Unspecified
```

The list provides the following information:

Parameter	Description
id	**Synopsis:** A string Neighbor address.

Parameter	Description
version	**Synopsis:** A 32-bit signed integer BGP version.
as	**Synopsis:** A string Remote AS number.
msgrcvd	**Synopsis:** A 32-bit signed integer Number of received BGP messages.
msgsent	**Synopsis:** A 32-bit signed integer Number of sent BGP messages.
uptime	**Synopsis:** A string Peer up time.
state	**Synopsis:** A string Connection state with this neighbor.
prefix-received	**Synopsis:** A string Number of prefixes (networks) received from this neighbor.

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:** A 32-bit signed integer Metric value.
local-preference	**Synopsis:** A string Local preference.
weight	**Synopsis:** A 32-bit signed integer Weight.
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 Section 12.8.1, “Configuring BGP”.

Section 12.8.13

Resetting a BGP Session

Whenever there is a change in the routing policy due to a configuration change, the BGP session must be reset for the new policy to take effect.

RUGGEDCOM ROX II allows users to perform either a hard or soft reset on both incoming and outbound sessions, as selected.

A BGP session can be reset for all routing tables, or for a specified neighbor.

Resetting All BGP Sessions

To reset all BGP sessions, do the following:

1. Navigate to:

```
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, or type **`revert`** and press **Enter** to abort.

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.

Parameter	Description
	• 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, or type **`revert`** and press **Enter** to abort.

Section 12.9
Managing OSPF

The Open Shortest Path First (OSPF) protocol determines the best path for routing IP traffic over a TCP/IP network based on link cost and quality. Unlike static routing, OSPF takes link failures and other network topology changes into account. OSPF also differs from RIP in that it provides less router to router update traffic.

The RUGGEDCOM ROX II OSPF daemon (ospfd) is an RFC 2178 [http://tools.ietf.org/html/rfc2178] 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 Section 12.11, "Managing Virtual Routing and Forwarding (VRF)".

CONTENTS

- Section 12.9.1, "OSPF Concepts"
- Section 12.9.2, "Configuring OSPF"
- Section 12.9.3, "Viewing the Status of Dynamic OSPF Routes"
- Section 12.9.4, "Managing Prefix Lists and Entries"
- Section 12.9.5, "Managing Areas"
- Section 12.9.6, "Managing Route Maps"
- Section 12.9.7, "Managing Incoming Route Filters"
- Section 12.9.8, "Managing Redistribution Metrics"

- Section 12.9.9, “Managing Routing Interfaces”
- Section 12.9.10, “Managing Message Digest Keys”
- Section 12.9.11, “Managing ABR Route Summarization”

Section 12.9.1
OSPF Concepts

When an OSPF configured router starts operating, it issues a *hello* packet. Routers having the same OSPF Area, hello-interval and dead-interval timers will communicate with each other and are said to be neighbors.

After discovering its neighbors, a router will exchange Link State Advertisements in order to determine the network topology.

Every 30 minutes (by default), the entire topology of the network must be sent to all routers in an area.

If the link speeds are too low, the links are too busy or there are too many routes, some routes may fail to get re-announced and will be aged out.

Splitting the network into smaller areas to reduce the number of routes within an area or reducing the number of routes to be advertised may help to avoid this problem.

In shared access networks (i.e. routers connected by switches or hubs) a designated router and a backup designated are elected to receive route changes from subnets in the area. Once a designated router is picked, all routing state changes are sent to the designated router, which then sends the resulting changes to all the routers.

The election is decided based on the priority assigned to the interface of each router. The highest priority wins. If the priority is tied, the highest router-id wins.

Section 12.9.2
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:** A 32-bit unsigned 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:** A 32-bit unsigned integer between 0 and 16777214 The default metric of redistribute routes.
distance { distance }	**Synopsis:** A 32-bit unsigned integer between 1 and 255

Parameter	Description
	The administrative distance.
opaque-lsa	Enables the Opaque-LSA capability (RFC2370).
passive-default	**Synopsis:** { true, false } **Default:** true Default passive value for new interface.
refresh-timer { refresh-timer }	**Synopsis:** A 16-bit unsigned integer between 10 and 1800 **Default:** 10 The refresh timer.
router-id { router-id }	**Synopsis:** A string 7 to 15 characters long The Router ID for OSPF.

3. Configure prefix list filters. For more information, refer to Section 12.9.4.3, "Adding a Prefix List".
4. Configure areas. For more information, refer to Section 12.9.5.2, "Adding an Area".
5. Configure route map filters. For more information, refer to Section 12.9.6.3, "Adding a Route Map Filter".
6. Configure redistribution metrics. For more information, refer to Section 12.9.8.2, "Adding a Redistribution Metric".
7. Configure interfaces. For more information, refer to Section 12.9.9.2, "Configuring a Routing Interface".
8. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.9.3
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

Parameter	Description
	Cost.
area	**Synopsis:** A string Area.

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.

Net

Parameter	Description
area	**Synopsis:** A string Area ID.

Summary

Parameter	Description
area	**Synopsis:** A string Area ID.

If no dynamic OSPF routes have been configured, configure OSPF and add routes as needed. For more information about configuring OSPF, refer to Section 12.9.2, "Configuring OSPF".

Section 12.9.4

Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the OSPF daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

CONTENTS

- Section 12.9.4.1, "Viewing a List of Prefix Lists"
- Section 12.9.4.2, "Viewing a List of Prefix Entries"
- Section 12.9.4.3, "Adding a Prefix List"
- Section 12.9.4.4, "Adding a Prefix Entry"
- Section 12.9.4.5, "Deleting a Prefix List"
- Section 12.9.4.6, "Deleting a Prefix Entry"

Section 12.9.4.1

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 Section 12.9.4.3, "Adding a Prefix List".

Section 12.9.4.2

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 Section 12.9.4.4, "Adding a Prefix Entry".

Section 12.9.4.3
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 1 to 1024 characters long The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to Section 12.9.4.4, "Adding a Prefix Entry".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.9.4.4
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.

Parameter	Description
subnet { subnet }	**Synopsis:** A string 9 to 18 characters long Network (xxx.xxx.xxx.xxx/xx). This parameter is mandatory.
le { le }	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
ge { ge }	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.9.4.5
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, or type **`revert`** and press **Enter** to abort.

Section 12.9.4.6
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, or type **revert** and press **Enter** to abort.

Section 12.9.5
Managing Areas

Network areas determine the regions within which routes are distributed to other routers. The subnets at a particular router can be added to its OSPF Area. The router will advertise these subnets to all routers in its area.

OSPF areas must be designed such that no single link failure will cause the network to be split into two disjointed networks.

A router can be part of multiple areas and function as a gateway between areas. When multiple areas are used on a network, area zero (0) is the backbone area. All areas must have a router connecting them to area zero (0).

CONTENTS

- Section 12.9.5.1, "Viewing a List of Areas"
- Section 12.9.5.2, "Adding an Area"
- Section 12.9.5.3, "Deleting an Area"

Section 12.9.5.1
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 Section 12.9.5.2, "Adding an Area".

Section 12.9.5.2
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, or type **revert** and press **Enter** to abort.

Section 12.9.5.3
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/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. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.9.6
Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed. In RUGGEDCOM ROX II, route maps are configured to filter routes based on their metric value, which defines the cost of the route. Once a match is found, the assigned action is taken.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

CONTENTS

- Section 12.9.6.1, "Viewing a List of Route Map Filters"
- Section 12.9.6.2, "Viewing a List of Route Map Filter Entries"
- Section 12.9.6.3, "Adding a Route Map Filter"
- Section 12.9.6.4, "Adding a Route Map Filter Entry"
- Section 12.9.6.5, "Deleting a Route Map Filter"
- Section 12.9.6.6, "Deleting a Route Map Filter Entry"
- Section 12.9.6.7, "Configuring Match Rules"

Section 12.9.6.1
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 Section 12.9.6.3, "Adding a Route Map Filter".

Section 12.9.6.2
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
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
-------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -           -
      -      -     -       -           -

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 12.9.6.4, "Adding a Route Map Filter Entry".

Section 12.9.6.3
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 Section 12.9.6.4, "Adding a Route Map Filter Entry".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.9.6.4
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 Jump to another route-map after match+set.
on-match-goto { on-match-goto }	**Synopsis:** A string Go to this entry on match.

Parameter	Description
metric { metric }	**Synopsis:** A 32-bit unsigned integer Metric value.
metric-type { metric-type }	**Synopsis:** An 8-bit signed integer between 1 and 2 External route type.

4. Configure the match rules for the route map filter. For more information, refer to Section 12.9.6.7, "Configuring Match Rules".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.9.6.5
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, or type **revert** and press **Enter** to abort.

Section 12.9.6.6
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 number
     ```
   - **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, or type **revert** and press **Enter** to abort.

Section 12.9.6.7
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 The prefix list name.

Parameter	Description
prefix-list { prefix-list }	**Synopsis:** A string The prefix list name.

Parameter	Description
ifname { ifname }	**Synopsis:** A string The interface name.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.9.7
Managing Incoming Route Filters

Incoming route advertisements can be filtered by assigning one or route map filters. This can be useful for excluding specific OSPF routes from the routing table.

NOTE
For more information about route map filters, refer to Section 12.9.6, "Managing Route Maps".

CONTENTS

- Section 12.9.7.1, "Viewing List of Incoming Route Filters"
- Section 12.9.7.2, "Adding an Incoming Route Filter"
- Section 12.9.7.3, "Deleting an Incoming Route Filter"

Section 12.9.7.1
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 Section 12.9.7.2, "Adding an Incoming Route Filter".

Section 12.9.7.2
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 Section 12.9.6, "Managing Route Maps".
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, or type **revert** and press **Enter** to abort.

Section 12.9.7.3
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, or type **revert** and press **Enter** to abort.

Section 12.9.8
Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the OSPF areas, can also be advertised.

CONTENTS

- Section 12.9.8.1, "Viewing a List of Redistribution Metrics"
- Section 12.9.8.2, "Adding a Redistribution Metric"
- Section 12.9.8.3, "Deleting a Redistribution Metric"

Section 12.9.8.1
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 Section 12.9.8.2, "Adding a Redistribution Metric".

Section 12.9.8.2
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 8-bit signed integer between 1 and 2 **Default:** 2 The OSPF exterior metric type for redistributed routes.
metric { metric }	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The metric for redistributed routes.
route-map { route-map }	**Synopsis:** A string The route map name.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.9.8.3
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, or type **revert** and press **Enter** to abort.

Section 12.9.9
Managing Routing Interfaces

This section describes how to manage interfaces for OSPF routes.

CONTENTS

- Section 12.9.9.1, “Viewing a List of Routing Interfaces”

- Section 12.9.9.2, “Configuring a Routing Interface”

Section 12.9.9.1

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    DELAY
     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
```

Section 12.9.9.2

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.

IMPORTANT!
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:** A 32-bit unsigned integer between 1 and 65535 **Default:** 40 The time before considering a router dead (in seconds).
minimal-hello-multiplier { minimal-hello-multiplier }	**Synopsis:** An 8-bit unsigned 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 Section 7.1.1, "Configuring Costing for Routable Interfaces".*

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
{ ifname }	**Synopsis:** A string 1 to 32 characters long Interface name.
authentication { authentication }	**Synopsis:** { message-digest, null } The authentication type on this interface.
cost { cost }	**Synopsis:** A 32-bit unsigned integer between 1 and 65535

Parameter	Description
	The link cost. If not set, the cost is based on calculation of reference bandwidth divide by interface bandwidth.
hello-interval { hello-interval }	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 10 The time (in seconds) between sending hello packets.
priority { priority }	**Synopsis:** An 8-bit unsigned integer between 0 and 255 **Default:** 1 Priority of interface.
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:** A 32-bit unsigned integer between 1 and 65535 **Default:** 5 Time (in seconds) between retransmitting lost link state advertisements.
transmit-delay { transmit-delay }	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 1 The link state transmit delay (in seconds).
dead-interval { dead-interval }	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 40 The time before considering a router dead (in seconds).
minimal-hello-multiplier { minimal-hello-multiplier }	**Synopsis:** An 8-bit unsigned integer between 1 and 10 The number of times a hello message can be sent within one second.

5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.9.10
Managing Message Digest Keys

Message digest keys use the MD5 algorithm to authenticate OSPF neighbors and prevent unauthorized routers from joining the OSPF network. By enabling authentication and configuring a shared key on all the routers, only routers which have the same authentication key will be able to send and receive advertisements within the OSPF network.

An ID for each key allows the router to use multiple passwords and prevent replay attacks where OSPF packets are captured, modified and transmitted to a router. To change passwords, simply create a new key and delete the old key.

IMPORTANT!
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.

CONTENTS

- Section 12.9.10.1, "Viewing a List of Message Digest Keys"
- Section 12.9.10.2, "Adding a Message Digest Key"
- Section 12.9.10.3, "Deleting a Message Digest Key"

Section 12.9.10.1
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 message-digest-key
```

- **For VRF Routes via OSPF**

```
show running-config routing ospf interface name message-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-digest-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 Section 12.9.10.2, "Adding a Message Digest Key".

Section 12.9.10.2
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-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, or type **revert** and press **Enter** to abort.

Section 12.9.10.3
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 message-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, or type **revert** and press **Enter** to abort.

Section 12.9.11
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.

CONTENTS

- Section 12.9.11.1, “Understanding ABR Route Summarization”
- Section 12.9.11.2, “Viewing a List of Summary Routes”
- Section 12.9.11.3, “Adding a Summary Route”
- Section 12.9.11.4, “Deleting a Summary Route”
- Section 12.9.11.5, “Example: Basic Route Summarization”

Section 12.9.11.1
Understanding ABR Route Summarization

ABR route summarization reduces the number of type-3 summary LSAs sent between OSPF areas. When ABR route summarization is enabled, type-3 summary LSAs within a specific subnet range(s) received by the ABR are summarized and forwarded to the next area as a single type-3 summary LSA. This significantly reduces traffic between areas and reduces CPU utilization.

ABR route summarization requires the configuration of one or more area ranges for an ABR. An area range defines a network prefix and area ID. An action type (advertise or not advertise) and cost can also be applied. Type-3 LSAs that fall within the specified range are collected by the ABR.

Choosing to not advertise LSAs within a specific area range helps filter LSAs, and prevents any route happening in one area from propagating from one area into others.

Section 12.9.11.2
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 Section 12.9.11.3, "Adding a Summary Route".

Section 12.9.11.3
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 action-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, or type **revert** and press **Enter** to abort.

Section 12.9.11.4
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, or type **revert** and press **Enter** to abort.

Section 12.9.11.5
Example: Basic Route Summarization

The following demonstrates how to define a series of summary routes for an ABR in a simple OSPF network. In the following topology:

- R1 resides in area 0.0.0.0, the backbone of the OSPF network
- R2 acts as the ABR for areas 0.0.0.0 and 0.0.0.1
- R3 resides in area 0.0.0.1 and is connected to four stub networks (192.168.*.0/24)

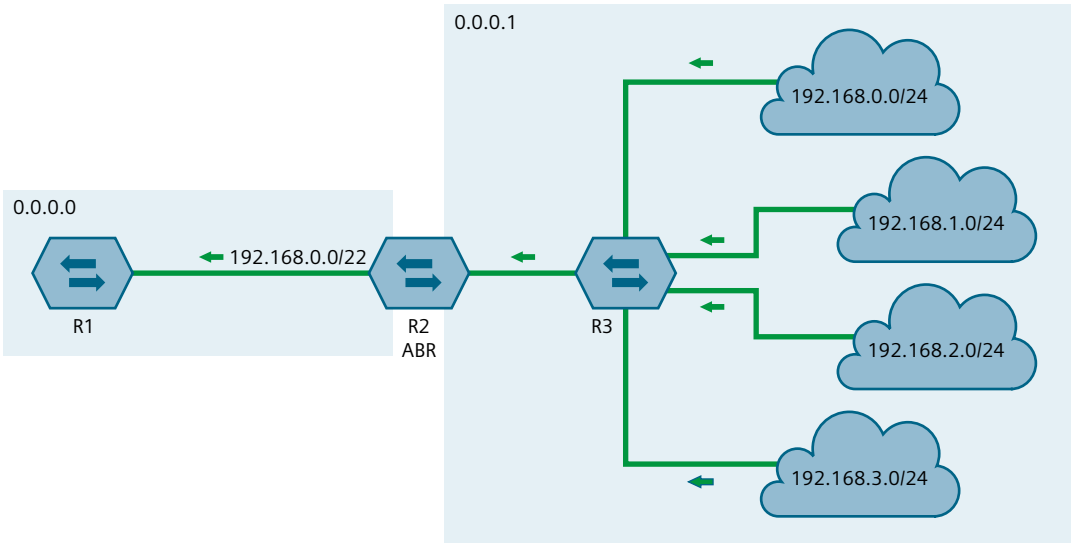


Figure 36: Basic ABR Router Summarization

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		

Section 12.10
Managing MPLS

MPLS (Multi-Protocol Label Switching) operates between Layer 2 and Layer 3 of the OSI (Open Systems Interconnection) model and provides a mechanism to carry traffic for any network layer protocol. MPLS makes forwarding decisions based on labels where the labels are mapped to destination IP networks. MPLS traffic flows are connection-oriented, as they operate on pre-configured LSPs (Label Switch Paths) built based on the dynamic Label Distribution Protocol (LDP), or through static label bindings.

CONTENTS

- Section 12.10.1, "Viewing the Status of IP Binding"
- Section 12.10.2, "Viewing the Status of the Forwarding Table"
- Section 12.10.3, "Enabling/Disabling MPLS"
- Section 12.10.4, "Managing the MPLS Interfaces"
- Section 12.10.5, "Managing Static Label Binding"
- Section 12.10.6, "Managing Static Cross-Connects"
- Section 12.10.7, "Managing LDP"

Section 12.10.1
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.
next-hop	**Synopsis:** A string The destination next hop router.
remote-label	**Synopsis:** A string The remote label

Section 12.10.2

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
```

This table or list provides the following information:

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.

Section 12.10.3
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, or type **`revert`** and press **Enter** to abort.

Section 12.10.4
Managing the MPLS Interfaces

This section describes how to manage the MPLS interfaces.

CONTENTS

- Section 12.10.4.1, "Viewing the Status of MPLS Interfaces"
- Section 12.10.4.2, "Viewing a List of MPLS Interfaces"
- Section 12.10.4.3, "Enabling/Disabling an MPLS Interface"

Section 12.10.4.1
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 Section 12.10.4.3, "Enabling/Disabling an MPLS Interface".

Section 12.10.4.2
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 Section 12.10.4.3, "Enabling/Disabling an MPLS Interface".

Section 12.10.4.3
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, or type **revert** and press **Enter** to abort.

Section 12.10.5
Managing Static Label Binding

This section describes how to bind (or reserve) labels for IPv4 or network prefixes.

CONTENTS

- Section 12.10.5.1, "Viewing the Status of Static Label Binding"
- Section 12.10.5.2, "Viewing a List of Static Labels"
- Section 12.10.5.3, "Adding a Static Label"
- Section 12.10.5.4, "Deleting a Static Label"

Section 12.10.5.1
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 Section 12.10.5.3, "Adding a Static Label".

Section 12.10.5.2
Viewing a List of Static Labels

To view a list of static labels, type:

```
show running-config mpls static-mpls binding [ ipv4 | ipv6 ]
```

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 Section 12.10.5.3, "Adding a Static Label".

Section 12.10.5.3
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 | ipv6 ] 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:** A 32-bit unsigned integer between 16 and 1048575 The incoming label: integer 16 -> 1048575.
next-hop { next-hop }	**Synopsis:** A string 7 to 15 characters long The IP address for the destination next-hop router.
out-label { out-label }	**Synopsis:** { explicit-null, implicit-null } or a 32-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 12.10.5.4
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 | ipv6 ] dest-address address
   ```

   Where:

   - *address* is the destination address and prefix.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.10.6
Managing Static Cross-Connects

Configure MPLS static cross-connects when the device is the core MPLS router. Cross-connects build Label Switch Paths (LSPs) when neighboring routers do not deploy the Label Distribution Protocol (LDP). The entry for static cross-connects is added to the Label Forwarding Information Base (LFIB). And, as such, label binding is not required in the Label Information Base (LIB).

CONTENTS

- Section 12.10.6.1, "Viewing the Status of Static Cross-Connects"
- Section 12.10.6.2, "Viewing a List of Static Cross-Connects"
- Section 12.10.6.3, "Adding a Static Cross-Connect"
- Section 12.10.6.4, "Deleting a Static Cross-Connect"

Section 12.10.6.1
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

Parameter	Description
	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 Section 12.10.6.3, "Adding a Static Cross-Connect".

Section 12.10.6.2
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 Section 12.10.6.3, "Adding a Static Cross-Connect".

Section 12.10.6.3
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. This parameter is mandatory.
next-hop { next-hop }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The destination next-hop router (IPv4 or IPv6 format).

Parameter	Description
	This parameter is mandatory.
out-label { out-label }	**Synopsis:** { explicit-null, implicit-null } or a 32-bit unsigned integer between 16 and 1048575 The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575. This parameter is mandatory.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.10.6.4
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, or type **`revert`** and press **Enter** to abort.

Section 12.10.7
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.

CONTENTS

- Section 12.10.7.1, “Viewing the Status of LDP Binding”
- Section 12.10.7.2, “Viewing the Status of the LDP Discovery Interfaces”
- Section 12.10.7.3, “Viewing the Status of the LDP Neighbor Local Node Information”
- Section 12.10.7.4, “Viewing the Status of the LDP Neighbor Connection Information”
- Section 12.10.7.5, “Viewing the Status of the LDP Neighbor Discovery Information”
- Section 12.10.7.6, “Configuring LDP”
- Section 12.10.7.7, “Configuring Neighbor Discovery”
- Section 12.10.7.8, “Viewing a List of LDP Interfaces”

- Section 12.10.7.9, "Enabling/Disabling an LDP Interface"

Section 12.10.7.1
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.

Section 12.10.7.2
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.
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 Section 12.10.7.9, "Enabling/Disabling an LDP Interface".

Section 12.10.7.3
Viewing the Status of the LDP Neighbor Local Node Information

To view the status of the local node(s) for the LDP neighbor on the device, 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
```

This table or list provides the following information:

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.

Section 12.10.7.4
Viewing the Status of the LDP Neighbor Connection Information

To view the status of the LDP neighbor connection on the device, 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
```

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.

This table provides the following information:

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.

Section 12.10.7.5

Viewing the Status of the LDP Neighbor Discovery Information

To view the status of the LDP neighbor discovery information on the device, 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
```

This table or list provides the following information:

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.
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.

Section 12.10.7.6
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	**Synopsis:** { true, false } **Default:** false A boolean flag to indicate that Label Distribution Protocol (LDP) is enabled.
holdtime { holdtime }	**Synopsis:** A 32-bit unsigned 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.

Section 12.10.7.7
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:** A 32-bit unsigned integer **Default:** 5 The time (in seconds) between the sending of consecutive Hello messages.
holdtime { holdtime }	**Synopsis:** A 32-bit unsigned integer **Default:** 15 The time (in seconds) that a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.

Section 12.10.7.8
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 Section 12.10.7.9, “Enabling/Disabling an LDP Interface”.

Section 12.10.7.9
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. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11

Managing Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) allows multiple routing instances to exist at the same time on a network router without conflicting with one another or the global routing table. This feature is used typically by service providers to route different types of traffic emanating from the same router.

Each routing instance is completely isolated and has its own set of interfaces. Any traffic sent on those interfaces is considered to be part of that VRF only.

An MPLS label can be applied as well to traffic traversing the tunnel to improve security. This is considered full VRF, as compared to VRF-Lite (first introduced by Cisco).

The RUGGEDCOM RX1400 can be configured to act as a CE, PE or P (provider core) router.

CONTENTS

- Section 12.11.1, "VRF Concepts"
- Section 12.11.2, "Viewing VRF Interface Statistics"
- Section 12.11.3, "Configuring VRF"
- Section 12.11.4, "Configuring a VRF Interface"
- Section 12.11.5, "Managing VRF Definitions"
- Section 12.11.6, "Managing Route Targets"
- Section 12.11.7, "Managing VRF Instances and OSPF"
- Section 12.11.8, "Managing IP/VPN Tunnels"
- Section 12.11.9, "Managing VPNv4 Neighbors"
- Section 12.11.10, "Managing IPv4 Address Families"
- Section 12.11.11, "Managing Redistribution for IPv4 Address Families"
- Section 12.11.12, "Managing Neighbors for IPv4 Address Families"
- Section 12.11.13, "Managing Static VRF Routes"
- Section 12.11.14, "Managing Gateways for Static VRF Routes"
- Section 12.11.15, "Managing Interfaces for Static VRF Routes"

Section 12.11.1

VRF Concepts

This section describes some of the concepts important to the implementation of Virtual Routing and Forwarding (VRF) in RUGGEDCOM ROX II.

CONTENTS

- Section 12.11.1.1, "VRF and VRF-Lite"
- Section 12.11.1.2, "Advantages and Disadvantages of Using VRF"

Section 12.11.1.1

VRF and VRF-Lite

Both full VRF and VRF-Lite employ the concept of VRFs to isolate interfaces, provide IP address reuse and manage routing tables. Both also provide a level of security for those interfaces forward to the VRFs. Under full VRF, MPLS is used in conjunction with IP/VPNs to provide a greater level of security than VRF-Lite.

RUGGEDCOM ROX II supports both VRF and VRF-Lite simultaneously. Use of full VRF interfaces and VRF-Lite interfaces can be mixed.

Section 12.11.1.2

Advantages and Disadvantages of Using VRF

The advantages and disadvantages of using VRF include the following:

Advantages

- Create multiple isolated network pipes for various data streams
- Provide individualized security for each VRF
- Manage each VRF separately for audit and billing purposes
- Create separate Intranets within one work environment
- 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

Section 12.11.2

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
```

This table or list provides the following information:

Parameter	Description
name	**Synopsis:** A string 1 to 15 characters long The name of the interface.
admin-state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status. This parameter is mandatory.
state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down. This parameter is mandatory.
pointopoint	**Synopsis:** { true, false } The point-to-point link. This parameter is mandatory.
bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes received. This parameter is mandatory.
packets	**Synopsis:** A 64-bit unsigned integer The number of packets received. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of error packets received. This parameter is mandatory.
dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the receiving device. This parameter is mandatory.

Parameter	Description
bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes transmitted. This parameter is mandatory.
packets	**Synopsis:** A 64-bit unsigned integer The number of packets transmitted. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of error packets transmitted. This parameter is mandatory.
dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the transmitting device. This parameter is mandatory.
collisions	**Synopsis:** A 32-bit unsigned integer The number of collisions detected on the port. This parameter is mandatory.

Section 12.11.3
Configuring VRF

To configure Virtual Routing and Forwarding (VRF), do the following:

IMPORTANT!
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 Section 12.8.1, "Configuring BGP".
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to Section 12.11.5.2, "Adding a VRF Definition".
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to Section 12.11.4, "Configuring a VRF Interface".
4. Enable OSPF. For more information, refer to Section 12.9.2, "Configuring OSPF".
5. Configure one or more VRF instances for OSPF. For more information, refer to Section 12.9.2, "Configuring OSPF".
6. Add one or more BGP neighbors. For more information, refer to Section 12.8.6.2, "Adding a Neighbor".
7. Configure one or more IP/VPN tunnels for each interface. For more information, refer to Section 12.11.8.2, "Adding an IP/VPN Tunnel".
8. Add one or more BGP neighbors to the VPNv4 address family. For more information, refer to Section 12.11.9.2, "Adding a Neighbor".
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 Section 12.8.1, "Configuring BGP".
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to Section 12.11.5.2, "Adding a VRF Definition".
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to Section 12.11.4, "Configuring a VRF Interface".
4. Enable OSPF. For more information, refer to Section 12.9.2, "Configuring OSPF".
5. Configure one or more VRF instances for OSPF. For more information, refer to Section 12.9.2, "Configuring OSPF".
6. Configure an IPv4 address family for each VRF instance. For more information, refer to Section 12.11.10.2, "Adding an IPv4 Address Family".
7. Configure one or more static VRF routes. For more information, refer to Section 12.11.13.2, "Adding a Static VRF Route".
8. Verify the network configuration.

Section 12.11.4

Configuring a VRF Interface

Each VRF definition must be associated with at least one routable interface that has been assigned an IP address.

To configure a routable interface to forward VRF traffic for a specific VRF definition, do the following:

1. 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 Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.5

Managing VRF Definitions

VRF definitions represent individual Customer Edge (CE) routers in the VRF topology. RUGGEDCOM ROX II supports up to eight definitions in total, each composed of a unique VRF name, an optional description and a Route Distinguisher (RD). The Route Distinguisher is an 8 octet field typically made up of an AS number or IP address followed by a colon (:) and the site ID (e.g. 6500:20 or 172.20.120.12:10). When prefixed to the IPv4 address of the associated interface, it uniquely identifies each IP packet, allowing the Provider Edge (PE) to determine which VPN tunnel the packet belongs to.

Each VRF definition can also be associated with one or more route targets.

CONTENTS

- Section 12.11.5.1, "Viewing a List of VRF Definitions"
- Section 12.11.5.2, "Adding a VRF Definition"
- Section 12.11.5.3, "Deleting a VRF Definition"

Section 12.11.5.1
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 Section 12.11.5.2, "Adding a VRF Definition".

Section 12.11.5.2
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 0 to 256 characters long

Parameter	Description
	A string that can be used to describe the vrf. Maximum length 256 characters, including blanks.
rd { rd }	**Synopsis:** A string 0 to 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 Section 12.11.6.2, "Adding a Route Target".
5. Configure a routable interface for the VRF instance. For more information, refer to Section 12.11.4, "Configuring a VRF Interface".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.11.5.3
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 Section 12.11.7.3, "Deleting a VRF Instance".
4. Delete the associated IPv4 address family under BGP. For more information, refer to Section 12.11.10.3, "Deleting an IPv4 Address Family".
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, or type **`revert`** and press **Enter** to abort.

Section 12.11.6
Managing Route Targets

Route targets identify those routes to import/export within the Multi-Protocol BGP (MBGP) network. Similar to the normal global routing instance, the route target sets the route import and export parameters for BGP. This parameter enables users to specify which prefixes they wish to import to other neighbors and which ones to export.

CONTENTS

- Section 12.11.6.1, "Viewing a List of Route Targets"
- Section 12.11.6.2, "Adding a Route Target"
- Section 12.11.6.3, "Deleting a Route Target"

Section 12.11.6.1
Viewing a List of Route Targets

To view a list of VRF definitions, type:

```
show running-config global vrf definition name routing-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 Section 12.11.5.2, "Adding a VRF Definition".

Section 12.11.6.2
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, or type **revert** and press **Enter** to abort.

Section 12.11.6.3
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, or type **revert** and press **Enter** to abort.

Section 12.11.7
Managing VRF Instances and OSPF

OSPF can be configured for one or more VRF definitions. This is done by by enabling OSPF for a VRF instance and then configuring the required OSPF parameters.

OSPF can be run on any physical or switched interface, as well as VRF-Lite interfaces (IPv4) and full VRF interfaces (IP/VPN using MPLS).

CONTENTS

- Section 12.11.7.1, "Viewing a List of VRF Instances"
- Section 12.11.7.2, "Adding a VRF Instance and Configuring OSPF"
- Section 12.11.7.3, "Deleting a VRF Instance"

Section 12.11.7.1
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 Section 12.11.5.2, "Adding a VRF Definition".

Section 12.11.7.2
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 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:** A 32-bit unsigned 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:** A 32-bit unsigned integer between 0 and 16777214 The default metric of redistribute routes.
distance { distance }	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance.
opaque-lsa	Enables the Opaque-LSA capability (RFC2370).
passive-default	**Synopsis:** { true, false } **Default:** true Default passive value for new interface.
refresh-timer { refresh-timer }	**Synopsis:** A 16-bit unsigned integer between 10 and 1800 **Default:** 10 The refresh timer.
router-id { router-id }	**Synopsis:** A string 7 to 15 characters long The Router ID for OSPF.
always	**Synopsis:** { true, false } **Default:** false Always advertise default route even when there is no default route present in routing table.
metric { metric }	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The metric value for default route.
metric-type { metric-type }	**Synopsis:** An 8-bit signed integer between 1 and 2 **Default:** 2 The metric type for default route.
route-map { route-map }	**Synopsis:** A string The route map name.
external { external }	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for external routes.
inter-area { inter-area }	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for inter-area routes.
intra-area { intra-area }	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for intra-area routes.

3. Configure prefix list filters for the VRF instance. For more information, refer to Section 12.9.4.3, "Adding a Prefix List".
4. Configure areas for the VRF instance. For more information, refer to Section 12.9.5.2, "Adding an Area".
5. Configure route map filters for the VRF instance. For more information, refer to Section 12.9.6.3, "Adding a Route Map Filter".
6. Configure redistribution metrics for the VRF instance. For more information, refer to Section 12.9.8.2, "Adding a Redistribution Metric".
7. Configure interfaces for the VRF instance. For more information, refer to Section 12.9.9.2, "Configuring a Routing Interface".
8. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.11.7.3
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, or type **`revert`** and press **Enter** to abort.

Section 12.11.8
Managing IP/VPN Tunnels

IP/VPN tunnels use the VPNv4 protocol to exchange customer prefixes (i.e. route distributions and route targets) and labels between Provider Edge (PE) routers. IP/VPNs provide isolation of the interfaces connecting each end of the VPN.

NOTE
VRF maintains a table listing each interface belonging to each IP/VPN tunnel.

CONTENTS

- Section 12.11.8.1, "Viewing a List of IP/VPN Tunnels"
- Section 12.11.8.2, "Adding an IP/VPN Tunnel"
- Section 12.11.8.3, "Deleting an IP/VPN Tunnels"

Section 12.11.8.1
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

 !
!
```

Section 12.11.8.2
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, or type **revert** and press **Enter** to abort.

Section 12.11.8.3
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, or type **`revert`** and press **Enter** to abort.

Section 12.11.9
Managing VPNv4 Neighbors

VPNv4 neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for VRF-Lite to operate.

CONTENTS

- Section 12.11.9.1, "Viewing a List of Neighbors"
- Section 12.11.9.2, "Adding a Neighbor"
- Section 12.11.9.3, "Deleting a Neighbor"

Section 12.11.9.1
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 Section 12.11.12.2, "Adding a Neighbor".

Section 12.11.9.2
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, or type **revert** and press **Enter** to abort.

Section 12.11.9.3
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, or type **revert** and press **Enter** to abort.

Section 12.11.10
Managing IPv4 Address Families

IPv4 address families are configured when deploying VRF-Lite. Address families under BGP specify the neighbors with whom the router will share VRF routing information and what type of routing distribution method is permitted. One or more address families can be configured for each VRF instance.

Route distribution can be limited directly connected routes, static routes, or OSPF learned routes.

CONTENTS

- Section 12.11.10.1, "Viewing a List of IPv4 Address Families"
- Section 12.11.10.2, "Adding an IPv4 Address Family"
- Section 12.11.10.3, "Deleting an IPv4 Address Family"

Section 12.11.10.1
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 Section 12.11.10.2, "Adding an IPv4 Address Family".

Section 12.11.10.2
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 Section 12.11.12.2, "Adding a Neighbor".
4. [Optional] Add one or more redistributions. For more information, refer to Section 12.11.11.2, "Adding a Redistribution".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.10.3
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, or type **revert** and press **Enter** to abort.

Section 12.11.11

Managing Redistribution for IPv4 Address Families

Redistribution in general is the advertisement of routes by one protocol that have been learned via another dynamic routing protocol, a static route, or a directly connected router. It is deployed to promote interoperability between networks running different routing protocols. In the case of VRF, the OSPF dynamic routing protocol is supported.

For each VRF instance, one or more redistributions can be defined. A redistribution defines the source of the routing information, a metric and (optional) a pre-defined routing map.

The metric is used for route decision making within the Autonomous System (AS). Care must be taken to define a metric that is understood by the OSPF routing protocol.

CONTENTS

- Section 12.11.11.1, "Viewing a List of Redistributions"
- Section 12.11.11.2, "Adding a Redistribution"
- Section 12.11.11.3, "Deleting a Redistribution"

Section 12.11.11.1

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 redistribute | tab
                   ROUTE
SOURCE     METRIC  MAP
-------------------------
connected  -       -
ospf       -       -
static     -       -

  !
 !
!
```

If no redistributions have been configured, add them as needed. For more information, refer to Section 12.11.11.2, "Adding a Redistribution".

Section 12.11.11.2

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:** A 32-bit unsigned integer between 0 and 4294967295 The metric for redistributed routes.
route-map { route-map }	**Synopsis:** A string The route map name.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.11.3
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 redistribute [ connected | ospf | static ]
```

Where:

- *vrf* is the chosen VRF instance

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.12
Managing Neighbors for IPv4 Address Families

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for VRF to operate.

CONTENTS

- Section 12.11.12.1, “Viewing a List of Neighbors”
- Section 12.11.12.2, “Adding a Neighbor”
- Section 12.11.12.3, “Configuring the Distribution of Prefix Lists”
- Section 12.11.12.4, “Tracking Commands”
- Section 12.11.12.5, “Deleting a Neighbor”

Section 12.11.12.1
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 Section 12.11.12.2, "Adding a Neighbor".

Section 12.11.12.2
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 address
   ```

   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 { remote-as }	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 A BGP neighbor.

Parameter	Description
	This parameter is mandatory.
ebgp-multihop { ebgp-multihop }	**Synopsis:** An 8-bit unsigned integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
maximum-prefix { maximum-prefix }	**Synopsis:** A 32-bit unsigned 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 1 to 1024 characters long Password.
update-source { update-source }	**Synopsis:** A string 7 to 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:** A 16-bit unsigned 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 Apply route map to incoming routes.
out { out }	**Synopsis:** A string Apply route map to outbound routes.

5. Configure the prefix list distribution. For more information, refer to Section 12.11.12.3, "Configuring the Distribution of Prefix Lists".
6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.11.12.3
Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in an IPv4 address family, do the following:

1. Make sure the 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 Section 12.11.12.4, "Tracking Commands".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.12.4
Tracking Commands

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 12.5, "Managing Event Trackers".

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 Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state. This parameter is mandatory.
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, or type **revert** and press **Enter** to abort.

Section 12.11.12.5
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, or type **revert** and press **Enter** to abort.

Section 12.11.13

Managing Static VRF Routes

Routing information can be shared between routers using dynamic routing data or they can be manually configured. Static routes are explicit paths between routers that are manually configured. Static routes are commonly used for stable, often smaller networks whose configurations are not prone to change. They can be used to supplement dynamic routes.

CONTENTS

- Section 12.11.13.1, "Viewing a List of Static VRF Routes"
- Section 12.11.13.2, "Adding a Static VRF Route"
- Section 12.11.13.3, "Configuring a Black Hole Connection for a Static VRF Route"
- Section 12.11.13.4, "Deleting a Static VRF Route"

Section 12.11.13.1

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 Section 12.11.13.2, "Adding a Static VRF Route".

Section 12.11.13.2

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 Section 12.11.13.3, "Configuring a Black Hole Connection for a Static VRF Route".
5. If necessary, add gateways for the static route. For more information, refer to Section 12.11.14.2, "Adding a Gateway for a Static VRF Route".
6. If necessary, add interfaces for the static route. For more information, refer to Section 12.11.15.2, "Adding a Gateway for a Static VRF Route".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.11.13.3
Configuring a Black Hole Connection for a Static VRF Route

To configure a black hole connection for a static VRF route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the black hole connection by typing:

```
routing vrf vrf ipv4 route subnet blackhole distance 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, or type **`revert`** and press **Enter** to abort.

Section 12.11.13.4
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, or type **revert** and press **Enter** to abort.

Section 12.11.14
Managing Gateways for Static VRF Routes

This section describes how to configure and manage gateways for static VRF routes.

CONTENTS

- Section 12.11.14.1, "Viewing a List of Gateways for Static VRF Routes"
- Section 12.11.14.2, "Adding a Gateway for a Static VRF Route"
- Section 12.11.14.3, "Deleting a Gateway for a Static VRF Route"

Section 12.11.14.1
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 Section 12.11.14.2, "Adding a Gateway for a Static VRF Route".

Section 12.11.14.2
Adding a Gateway for a Static VRF Route

To add a gateway address for a static VRF route, do the following:

1. 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:** A 32-bit unsigned integer between 1 and 255 The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.14.3
Deleting a Gateway for a Static VRF Route

To delete a gateway address assigned to a static VRF route, do the following:

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

```
no 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. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.15
Managing Interfaces for Static VRF Routes

This section describes how to manage interfaces used for static VRF routes.

CONTENTS

- Section 12.11.15.1, "Viewing a List of Interfaces for Static VRF Routes"
- Section 12.11.15.2, "Adding a Gateway for a Static VRF Route"
- Section 12.11.15.3, "Deleting a Gateway for a Static VRF Route"

Section 12.11.15.1
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 gateway addresses 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 Section 12.11.15.2, "Adding a Gateway for a Static VRF Route".

Section 12.11.15.2
Adding a Gateway for a Static VRF Route

To add an interface for an static VRF route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   ```
   routing vrf vrf ipv4 route subnet dev interface
   ```

   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:** A 32-bit unsigned integer between 1 and 255 The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.11.15.3
Deleting a Gateway for a Static VRF Route

To delete an interface assigned to a static VRF route, do the following:

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

   ```
   no routing vrf vrf ipv4 route subnet dev gateway
   ```

   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, or type **revert** and press **Enter** to abort.

Section 12.12

Managing Static Routing

Static routes can be manually added to the routing table when there are no notifications sent by other routers regarding network topology changes.

CONTENTS

- Section 12.12.1, "Viewing a List of Static Routes"
- Section 12.12.2, "Adding an IPv4 Static Route"
- Section 12.12.3, "Adding an IPv6 Static Route"
- Section 12.12.4, "Deleting a Static Route"
- Section 12.12.5, "Configuring a Black Hole Connection for an IPv4 Static Route"
- Section 12.12.6, "Managing Gateways for Static Routes"
- Section 12.12.7, "Managing Interfaces for Static Routes"

Section 12.12.1

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    DISTANCE
-------------------------------------------------------------------------------------
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 Section 12.12.2, "Adding an IPv4 Static Route" or Section 12.12.3, "Adding an IPv6 Static Route".

Section 12.12.2

Adding an IPv4 Static Route

To add an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.

IMPORTANT!
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 Section 12.12.5, "Configuring a Black Hole Connection for an IPv4 Static Route".
5. [Optional] If the static route is not a black hole route, configure either the interface that connects to the next-hop router (if there is a direct connection) or the IP address (gateway) of the next-hop router. Only one can be configured per static route. For more information, refer to either Section 12.12.6.3, "Adding a Gateway for an IPv4 Static Route" or Section 12.12.7.3, "Adding an Interface for an IPv4 Static Route".
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.12.3
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 Section 12.12.6.1, "Configuring Gateways for IPv6 Static Routes" or Section 12.12.7.1, "Configuring Interfaces for IPv6 Static Routes".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.12.4
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, or type **revert** and press **Enter** to abort.

Section 12.12.5
Configuring a Black Hole Connection for an IPv4 Static Route

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:

Parameter	Description
distance { distance }	**Synopsis:** A 32-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 12.12.6
Managing Gateways for Static Routes

If the device is not directly connected to the next-hop router, configure a static route to forward traffic to the next-hop router's IP address. This is referred to as a *gateway*.

In the case of IPv6 static routes, only one gateway can be selected per route.

CONTENTS

- Section 12.12.6.1, “Configuring Gateways for IPv6 Static Routes”
- Section 12.12.6.2, “Viewing a List of Gateways for IPv4 Static Routes”
- Section 12.12.6.3, “Adding a Gateway for an IPv4 Static Route”
- Section 12.12.6.4, “Deleting a Gateway for an IPv4 Static Route”

Section 12.12.6.1
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 6 to 40 characters long The gateway for the static route. This parameter is mandatory.
distance { distance }	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The distance for the static route.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.12.6.2
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 Section 12.12.6.3, “Adding a Gateway for an IPv4 Static Route”.

Section 12.12.6.3
Adding a Gateway for an IPv4 Static Route

To add a gateway address for an IPv4 static route, do the following:

1. 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:** A 32-bit unsigned integer between 1 and 255 The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.12.6.4
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, or type **revert** and press **Enter** to abort.

Section 12.12.7
Managing Interfaces for Static Routes

Static routes can be configured to forward packets to an exit interface. Assuming the device is directly connected to a neighboring router, the device will send Address Resolution Protocol (ARP) requests to determines the next hop IP address.

In the case of IPv6 static routes, only one interface can be selected per route.

CONTENTS

- Section 12.12.7.1, “Configuring Interfaces for IPv6 Static Routes”
- Section 12.12.7.2, “Viewing a List of Interfaces for IPv4 Static Routes”
- Section 12.12.7.3, “Adding an Interface for an IPv4 Static Route”
- Section 12.12.7.4, “Deleting an Interface for an IPv4 Static Route”

Section 12.12.7.1
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. This parameter is mandatory.
distance { distance }	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The distance for the static route.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.12.7.2
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 Section 12.12.7.3, “Adding an Interface for an IPv4 Static Route”.

Section 12.12.7.3
Adding an Interface for an IPv4 Static Route

To add an interface for an IPv4 static route, do the following:

1. 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:** A 32-bit unsigned integer between 1 and 255 The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.12.7.4
Deleting an Interface for an IPv4 Static Route

To delete an interface for an IPv4 static route, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 12.13
Managing Static Multicast Routing

Static multicast routing allows network designers to control the flow of multicast traffic by manually adding static routes to the routing table.

CONTENTS

- Section 12.13.1, “Enabling/Disabling Static Multicast Routing”
- Section 12.13.2, “Managing Static Multicast Groups”
- Section 12.13.3, “Managing Out-Interfaces”

Section 12.13.1
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 static multicast routing by typing:

```
routing multicast static enable
```

Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables static multicast routing service

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.13.2
Managing Static Multicast Groups

Define a static multicast group for each multicast route. Multiple routes can be configured, as long as the source and multicast IP addresses are unique to the route.

IMPORTANT!
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).

CONTENTS

- Section 12.13.2.1, "Viewing a List of Static Multicast Groups"
- Section 12.13.2.2, "Adding a Static Multicast Group"
- Section 12.13.2.3, "Deleting a Static Multicast Group"

Section 12.13.2.1
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 Section 12.13.2.2, "Adding a Static Multicast Group".

Section 12.13.2.2
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
{ description }	**Synopsis:** A string 1 to 32 characters long Describes the multicast group, spaces are not allowed.

4. Configure out-interfaces. Refer to Section 12.13.3.2, "Adding an Out-Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.13.2.3
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.

Section 12.13.3
Managing Out-Interfaces

An out-interface is the interface to which multicast packets are forwarded. Multiple out-interfaces can be defined for each static multicast group.

CONTENTS

- Section 12.13.3.1, "Viewing a List of Out-Interfaces"
- Section 12.13.3.2, "Adding an Out-Interface"
- Section 12.13.3.3, "Deleting an Out-Interface"

Section 12.13.3.1
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 Section 12.13.3.2, “Adding an Out-Interface”.

Section 12.13.3.2
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-interface 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, or type **revert** and press **Enter** to abort.

Section 12.13.3.3
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-interface 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, or type **revert** and press **Enter** to abort.

Section 12.14
Managing Dynamic Multicast Routing

The PIM-SM feature is used for Dynamic Multicast Routing. PIM-SM stands for Protocol Independent Multicast - Sparse Mode. It 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".

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. The router with the highest IP address usually becomes the designated router.
- **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.
- **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.
- **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.

CONTENTS

- Section 12.14.1, “PIM-SM Concepts”
- Section 12.14.2, “Viewing the Status of PIM-SM”
- Section 12.14.3, “Viewing the Status of Dynamic Multicast Routing”
- Section 12.14.4, “Configuring PIM-SM”
- Section 12.14.5, “Setting the Device as a BSR Candidate”
- Section 12.14.6, “Setting the Device as an RP Candidate”
- Section 12.14.7, “Managing PIM-SM Interfaces”
- Section 12.14.8, “Managing Static RP Addresses”
- Section 12.14.9, “Managing Multicast Group Prefixes”

Section 12.14.1
PIM-SM Concepts

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 a PIM 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 suboptimal 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.

Section 12.14.2
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:** A 32-bit unsigned integer Virtual interface index.
local-address	**Synopsis:** A string 1 to 16 characters long Local address.
subnet	**Synopsis:** A string 1 to 20 characters long Subnet.
flags	**Synopsis:** A string 1 to 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.

3. At the command prompt, type **`show routing status pim-sm bsr`** and press **Enter**. The 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 1 to 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:** A 32-bit unsigned integer Virtual interface index.
local-address	**Synopsis:** A string 1 to 16 characters long Local address.
subnet	**Synopsis:** A string 1 to 20 characters long Subnet.
flags	**Synopsis:** A string 1 to 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.

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 1 to 16 characters long RP address.

Parameter	Description
prefix	**Synopsis:** A string 1 to 20 characters long Group prefix.
priority	**Synopsis:** A string 1 to 20 characters long Priority.
holdtime	**Synopsis:** A string 1 to 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 1 to 16 characters long Multicast group address.
source	**Synopsis:** A string 1 to 16 characters long Source IP address.
rp-addr	**Synopsis:** A string 1 to 16 characters long RP (Rendezvous Point) address.
flags	**Synopsis:** A string 1 to 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).

7. 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 1 to 16 characters long Multicast group address.
rp-addr	**Synopsis:** A string 1 to 16 characters long RP (Rendezvous Point) address.
flags	**Synopsis:** A string 1 to 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).

Section 12.14.3
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
```

Section 12.14.4
Configuring PIM-SM

PIM-SM can be used to establish and dynamically manage the Multicast Routing table.

To configure PIM-SM, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » multicast » dynamic » pim-sm***.
3. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enable PIM-SM service.
default-preference { default-preference }	**Synopsis:** A 16-bit unsigned integer equaling 1 or higher **Default:** 1024 Default preference value. Preferences are used by assert elections to determine upstream routers.
default-metric { default-metric }	**Synopsis:** A 16-bit unsigned integer equaling 1 or higher **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. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 12.14.5
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, or type **`revert`** and press **Enter** to abort.

Section 12.14.6
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-address 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, or type **revert** and press **Enter** to abort.

Section 12.14.7
Managing PIM-SM Interfaces

PIM-SM requires at least one interface on which to receive or transmit advertisements. The interface must be non-passive and be assigned an IP address.

CONTENTS

- Section 12.14.7.1, "Viewing a List of PIM-SM Interfaces"
- Section 12.14.7.2, "Enabling/Disabling a PIM-SM Interface"

Section 12.14.7.1
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
IFNAME       PASSIVE
----------------------
dummy0       false
fe-1-1       false
fe-1-16      false
fe-cm-1      true
ge-sm-1      false
switch.0001  true

 group-prefix
PREFIX
--------------
225.0.0.1/32
225.0.0.2/32

!
```

If no PIM-SM interfaces have been configured, enable interfaces as needed. For more information about enabling PIM-SM interfaces, refer to Section 12.14.7.2, "Enabling/Disabling a PIM-SM Interface".

Section 12.14.7.2
Enabling/Disabling a PIM-SM Interface

To enable or disable a PIM-SM interface, do the following:

NOTE
Enabling PIM-SM on an interface also enables IGMPv2 on the interface, wherein the interface with the lowest IP address becomes the IGMP querier and sends periodic query messages every 125 seconds.

1. Make sure the CLI is in Configuration mode.
2. The interface is passive by default. Make it active for PIM-SM by typing:

   ```
   no interface ifname passive
   ```

   Where:

   - *ifname* is the name of the interface
   - *passive* determines whether the interface is passive (default) or active (no passive)

   NOTE
   A maximum of 30 non-passive interfaces can be active for PIM-SM.
3. Make sure the chosen interface is assigned an IP address. For more information, refer to Section 7.1, "Managing IP Addresses for Routable Interfaces".
4. 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 Section 8.4.3.1, "Configuring IGMP Snooping".

   The same is required for any Layer 2 switches on the network.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.14.8
Managing Static RP Addresses

A commonly used method for locating Rendezvous Points (RPs) is to target them directly by IP address, as opposed to locating them dynamically. Use static IP addresses when there are only a small number of RPs on the network and/or the RP assignment does not change often. It is important though that all static RP addresses be mirrored on all PIM-SM enabled devices in the multicast domain.

CONTENTS

- Section 12.14.8.1, "Viewing a List of Static RP Addresses "
- Section 12.14.8.2, "Adding a Static RP Address"
- Section 12.14.8.3, "Deleting a Static RP Address"

Section 12.14.8.1
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-address
```

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 Section 12.14.8.2, "Adding a Static RP Address".

Section 12.14.8.2
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-address 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, or type **revert** and press **Enter** to abort.

Section 12.14.8.3
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 static-address
   ```

   Where *static-address* is the Static RP (Rendezvous Point) address
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 12.14.9

Managing Multicast Group Prefixes

When nominated to a Rendezvous Point (RP), the device can serve up to 20 groups of multicast devices. The device is associated with a multicast group by defining the prefix for the group's multicast IP address (e.g. 225.1.2.0/24).

CONTENTS

- Section 12.14.9.1, "Viewing a List of Multicast Group Prefixes"
- Section 12.14.9.2, "Adding a Multicast Group Prefix"
- Section 12.14.9.3, "Deleting a Multicast Group Prefix"

Section 12.14.9.1

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 Section 12.14.9.2, "Adding a Multicast Group Prefix".

Section 12.14.9.2

Adding a Multicast Group Prefix

To add a multicast group prefix, do the following:

NOTE
A maximum of 20 group prefixes can be defined for PIM-SM.

1. 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.

Section 12.14.9.3
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 prefix
   ```

   Where *prefix* is the chosen prefix.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

13 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.

CONTENTS

- Section 13.1, “Managing VRRP”
- Section 13.2, “Managing VRRP within VRF”
- Section 13.3, “Managing Link Failover Protection”
- Section 13.4, “Managing Spanning Tree Protocol”

Section 13.1

Managing VRRP

The Virtual Router Redundancy Protocol (VRRP) is a gateway redundancy protocol. It provides a gateway failover mechanism invisible to hosts and other devices that send traffic through the gateway.

VRRP eliminates a single point of failure associated with statically routed networks by providing automatic failover using alternate routers. The RUGGEDCOM ROX II VRRP daemon (keepalived) is an RFC 5798 [http://tools.ietf.org/html/rfc5798] 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.

CONTENTS

- Section 13.1.1, “VRRP Concepts”
- Section 13.1.2, “Viewing the Status of VRRP”
- Section 13.1.3, “Enabling/Disabling VRRP”
- Section 13.1.4, “Managing VRRP Trackers”
- Section 13.1.5, “Managing VRRP Groups”
- Section 13.1.6, “Managing VRRP Instances”
- Section 13.1.7, “Managing VRRP Monitors”
- Section 13.1.8, “Managing Track Scripts”
- Section 13.1.9, “Managing Virtual IP Addresses”
- Section 13.1.10, “Managing Connection Synchronization”

Section 13.1.1

VRRP Concepts

This section describes some of the concepts important to the implementation of the Virtual Router Redundancy Protocol (VRRP) in RUGGEDCOM ROX II.

CONTENTS

- Section 13.1.1.1, "Static Routing vs. VRRP"
- Section 13.1.1.2, "VRRP Terminology"
- Section 13.1.1.3, "Connection Synchronization"

Section 13.1.1.1

Static Routing vs. VRRP

Many network designs employ a statically configured default gateway in the network hosts. A static default gateway is simple to configure, requires little if any overhead to run, and is supported by virtually every IP implementation. When the Dynamic Host Configuration Protocol (DHCP) is employed, hosts may accept a configuration for only a single default gateway.

Unfortunately, this approach creates a single point of failure. Loss of the router supplying the default gateway, or the router's WAN connection, results in isolating the hosts that rely upon the default gateway.

There are a number of ways to provide redundant connections for the hosts. Some hosts can configure alternate gateways while others are intelligent enough to participate in dynamic routing protocols such as the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) routing protocol. Even when available, these approaches are not always practical due to administrative and operation overhead.

VRRP solves the problem by allowing the establishment of a *virtual router group*, composed of a number of routers that provide one gateway IP. VRRP uses an election protocol to dynamically assign responsibility for the gateway to one of the routers in the group. This router is called the Master.

If the Master (or, optionally, a condition) fails, the alternate (or backup) routers in the group elect a new Master. The new master owns the virtual IP address and issues a gratuitous ARP to inform the network of where the gateway can be reached.

Since the host's default route and MAC address does not change, packet loss at the hosts is limited to the amount of time required to elect a new router.

Section 13.1.1.2

VRRP Terminology

Each physical router running VRRP is known as a VRRP Router. Two or more VRRP Routers can be configured to form a *Virtual Router*. Each VRRP Router may participate in one or more Virtual Routers.

Each Virtual Router has a user-configured Virtual Router Identifier (VRID) and a Virtual IP address or set of IP addresses on the shared LAN. Hosts on the shared LAN are configured to use these addresses as the default gateway.

Each router in the Virtual Router Group has a specific priority, which is a number between 1 and 255. The router with the highest priority (or highest number) is elected the Master, while all other routers are considered Backups.

On RUGGEDCOM RX1400 devices with RUGGEDCOM ROX II v2.3 or higher installed, if the router with the highest priority is in a fault state, the backup VRRP Router can delay its transition to becoming the Master router. The length of the delay is user-defined.

VRRP can also monitor a specified interface and give up control of a gateway IP to another VRRP Router if that interface goes down.

An Example of VRRP

In the following example, host 1 uses a gateway of 1.1.1.253 and host 2 uses a gateway of 1.1.1.252. The 1.1.1.253 gateway is provided by VRID 10. In normal practice, router 1 will provide this virtual IP since its priority for VRID 10 is higher than that of router 2. If router 1 becomes inoperative or if its w1ppp link fails, it will relinquish control of gateway IP 1.1.1.253 to router 2.

In a similar fashion host 2 can use the VRID 11 gateway address of 1.1.1.252, which will normally be supplied by router 2.

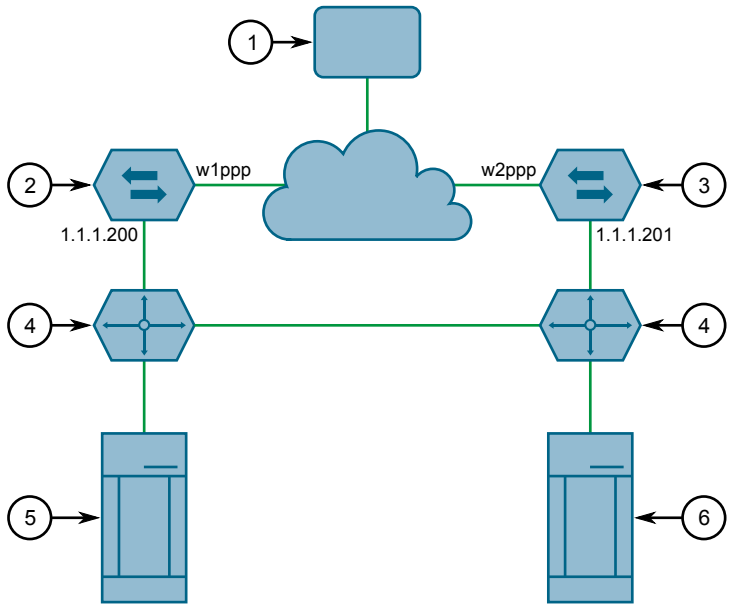


Figure 37: VRRP Example

1. Network **2.** Remote Router 1 **3.** Remote Router 2 **4.** Switch **5.** Host 1 **6.** Host 2

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.

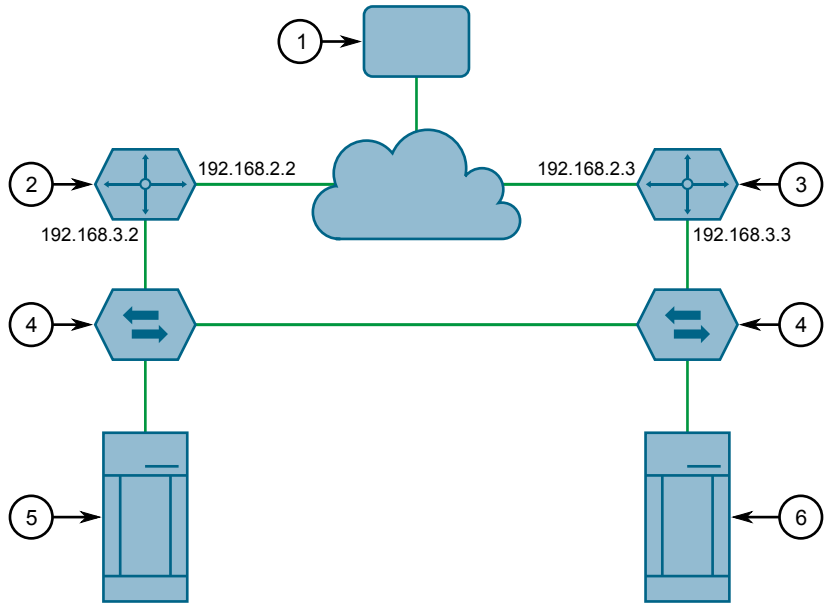


Figure 38: VRRP Group Example

1. Network **2.** Remote Router 1 **3.** Remote Router 2 **4.** Switch **5.** Host 1 **6.** Host 2

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.

Section 13.1.1.3

Connection Synchronization

When failover occurs, hosts must typically either reconnect manually to the backup firewall, or wait for the connection to automatically reconnect. This can sometimes take several minutes.

When connection synchronization is enabled, stateful connections are maintained when a VRRP master router fails, resulting in a seamless failover to the VRRP backup router. This is done by synchronizing the firewall and NAT states between the master and backup routers.

In the following example, when the master router (R1) fails, the firewall connection and NAT states are initialized automatically for the backup router (R2). The backup router then becomes the new VRRP master.

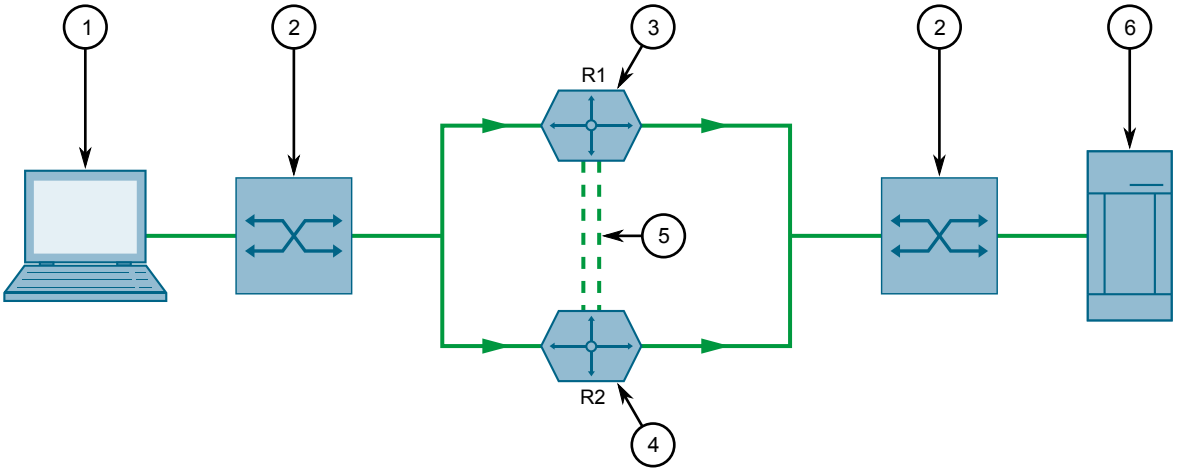


Figure 39: Connection Synchronization Example

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

Section 13.1.2

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 table or list provides the following information:

Parameter	Description
name	**Synopsis:** A string The VRRP instance name.

Parameter	Description
state	**Synopsis:** A string The VRRP instance state. This parameter is mandatory.
priority	**Synopsis:** A string The VRRP instance priority. This parameter is mandatory.
time-change	**Synopsis:** A string The time of change to the current state. This parameter is mandatory.
interface-state	**Synopsis:** A string The VRRP interface state. This parameter is mandatory.

Section 13.1.3
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, or type **`revert`** and press **Enter** to abort.

Section 13.1.4
Managing VRRP Trackers

VRRP trackers monitor the state/condition of a route. When the route is unavailable, VRRP will lower its priority or transition it to a fault state.

NOTE
The decision to increase or decrease the priority of a route must be done in coordination with any backup VRRP Routers since the priority decides whether a router becomes a Master or a Backup. For example, if Router X's priority is 150 and Router Y's priority is 145, Router X's priority must be lowered by 6 to make it a Backup router.

CONTENTS

- Section 13.1.4.1, “Viewing a List of VRRP Trackers”
- Section 13.1.4.2, “Adding a VRRP Tracker”

- Section 13.1.4.3, "Deleting a VRRP Tracker"

Section 13.1.4.1
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 Section 13.1.4.2, "Adding a VRRP Tracker".

Section 13.1.4.2
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 9 to 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:** A 32-bit unsigned integer between 1 and 120 The number of seconds between tracker queries. This parameter is mandatory.

Parameter	Description
weight { weight }	**Synopsis:** A 32-bit signed 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:** A 32-bit unsigned integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
fall { fall }	**Synopsis:** A 32-bit unsigned 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, or type **`revert`** and press **Enter** to abort.

Section 13.1.4.3
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, or type **`revert`** and press **Enter** to abort.

Section 13.1.5
Managing VRRP Groups

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

CONTENTS

- Section 13.1.5.1, “Viewing a List of VRRP Groups”
- Section 13.1.5.2, “Adding a VRRP Group”
- Section 13.1.5.3, “Deleting a VRRP Group”

Section 13.1.5.1
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 Section 13.1.5.2, "Adding a VRRP Group".

Section 13.1.5.2
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, or type **revert** and press **Enter** to abort.

Section 13.1.5.3
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, or type **revert** and press **Enter** to abort.

Section 13.1.6
Managing VRRP Instances

VRRP instances define the interfaces monitored by VRRP. Two or more instances can be added to the same VRRP group, which allows them to failover together.

CONTENTS

- Section 13.1.6.1, "Viewing a List of VRRP Instances"
- Section 13.1.6.2, "Adding a VRRP Instance"

- Section 13.1.6.3, "Deleting a VRRP Instance"

Section 13.1.6.1
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 Section 13.1.6.2, "Adding a VRRP Instance".

Section 13.1.6.2
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 Section 13.1.5.2, "Adding a VRRP Group".
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:

   IMPORTANT!
   *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 Section 6.8.10.2, "Adding an Interface".*

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 8-bit unsigned integer between 2 and 3 **Default:** 2 Configure VRRP version for this instance.
interface { interface }	**Synopsis:** A string The interface that will host the VRIP when the router becomes the VRRP Master. This parameter is mandatory.
vrid { vrid }	**Synopsis:** An 8-bit unsigned integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID. This parameter is mandatory.
priority { priority }	**Synopsis:** An 8-bit unsigned 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. This parameter is mandatory.
advert-interval { advert-interval }	**Synopsis:** An 8-bit unsigned integer between 1 and 255 **Default:** 1 VRRP2 advertisement interval, in seconds.
advert-interval-millisecond { advert-interval-millisecond }	**Synopsis:** A 32-bit unsigned integer between 20 and 3000 **Default:** 1000 VRRP3 advertisement interval in millisecond, must be multiple of 10.
garp-delay { garp-delay }	**Synopsis:** An 8-bit unsigned 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:** A 32-bit unsigned integer between 0 and 1000 **Default:** 0 The time, in seconds, after startup until preemption.
fault-to-master-delay { fault-to-master-delay }	**Synopsis:** A 32-bit unsigned 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 VRIP interface.
group { group }	**Synopsis:** A string Binds this VRRP instance to a VRRP group.

5. Add one or more VRRP monitors. For more information, refer to Section 13.1.7.2, "Adding a VRRP Monitor".
6. Add one or more track scripts. For more information, refer to Section 13.1.8.2, "Adding a Track Script".

7. Add one or more virtual IP addresses. For more information, refer to Section 13.1.9.2, "Adding a Virtual IP Address".
8. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 13.1.6.3
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, or type **revert** and press **Enter** to abort.

Section 13.1.7
Managing VRRP Monitors

A VRRP monitor selects an extra interface to monitor. If the interface becomes unavailable, the router will relinquish control of the gateway IP address to another VRRP Router.

CONTENTS

- Section 13.1.7.1, "Viewing a List of VRRP Monitors"
- Section 13.1.7.2, "Adding a VRRP Monitor"
- Section 13.1.7.3, "Deleting a VRRP Monitor"

Section 13.1.7.1
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 Section 13.1.7.2, "Adding a VRRP Monitor".

Section 13.1.7.2
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:** A 32-bit signed 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, or type **revert** and press **Enter** to abort.

Section 13.1.7.3
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, or type **revert** and press **Enter** to abort.

Section 13.1.8
Managing Track Scripts

Track scripts are used to associate VRRP trackers with VRRP instances.

CONTENTS

- Section 13.1.8.1, "Viewing a List of Track Scripts"
- Section 13.1.8.2, "Adding a Track Script"
- Section 13.1.8.3, "Deleting a Track Script"

Section 13.1.8.1
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 Section 13.1.8.2, "Adding a Track Script".

Section 13.1.8.2
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:** A 32-bit signed 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, or type **`revert`** and press **Enter** to abort.

Section 13.1.8.3
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 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. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 13.1.9
Managing Virtual IP Addresses

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

CONTENTS

- Section 13.1.9.1, “Viewing a List of Virtual IP Addresses”
- Section 13.1.9.2, “Adding a Virtual IP Address”
- Section 13.1.9.3, “Deleting a Virtual IP Address”

Section 13.1.9.1
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 Section 13.1.9.2, "Adding a Virtual IP Address".

Section 13.1.9.2
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, or type **revert** and press **Enter** to abort.

Section 13.1.9.3
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, or type **revert** and press **Enter** to abort.

Section 13.1.10
Managing Connection Synchronization

This section describes how to configure connection synchronization between two VRRP-enabled routers.

CONTENTS

- Section 13.1.10.1, "Configuring Connection Synchronization"

- Section 13.1.10.2, "Enabling/Disabling Connection Synchronization"
- Section 13.1.10.3, "Viewing a List of Dedicated LInks"
- Section 13.1.10.4, "Adding a Dedicated Link"
- Section 13.1.10.5, "Deleting a Dedicated Link"
- Section 13.1.10.6, "Selecting a Default Dedicated Link"
- Section 13.1.10.7, "Viewing the Status of Each Dedicated Link"

Section 13.1.10.1
Configuring Connection Synchronization

To configure connection synchronization, do the following for *each* VRRP-enabled device:

IMPORTANT!
Well-formed stateful firewall rules are required. For more information, refer to Section 6.8.1.1, "Stateless vs. Stateful Firewalls".

1. Configure a firewall with stateful firewall rules to control inbound and outbound traffic. For more information, refer to Section 6.8.3, "Adding a Firewall".
2. Make sure the VRRP service is enabled. For more information, refer to Section 13.1.3, "Enabling/Disabling VRRP".
3. Configure VRRP instances and groups. For more information, refer to Section 13.1.6.2, "Adding a VRRP Instance" and Section 13.1.5.2, "Adding a VRRP Group".
4. Define one or more dedicated links for each VRRP group. For more information, refer to Section 13.1.10.4, "Adding a Dedicated Link".
5. Select a link to be the default dedicated link for any VRRP group not assigned a dedicated link. For more information, refer to Section 13.1.10.6, "Selecting a Default Dedicated Link".
6. Enable the configuration synchronization service. For more information, refer to Section 13.1.10.2, "Enabling/Disabling Connection Synchronization".

Once the configuration is complete, verify the status of the service on both devices. For more information, refer to Section 13.1.10.7, "Viewing the Status of Each Dedicated Link".

Section 13.1.10.2
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, or type **`revert`** and press **Enter** to abort.

Section 13.1.10.3
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 Section 13.1.10.4, “Adding a Dedicated Link”.

Section 13.1.10.4
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 The interface name of the dedicated link.
ip { ip }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IPv4 or IPv6 address of the dedicated link interface.
mcast-ip { mcast-ip }	**Synopsis:** A string 7 to 15 characters long or a string 7 to 39 characters long **Default:** 225.0.0.50 The destination IPv4 or IPv6 multicast address of the dedicated link.
group { group }	**Synopsis:** A 16-bit unsigned integer between 1 and 65535 **Default:** 3780 The multicast group ID of the cluster.
send-buffer { send-buffer }	**Synopsis:** A 32-bit unsigned integer between 64 and 2560 **Default:** 1220 The sending socket buffer size in kB.

Parameter	Description
recv-buffer { recv-buffer }	**Synopsis:** A 32-bit unsigned integer between 64 and 2560 **Default:** 1220 The receiving socket buffer size in kB.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 13.1.10.5
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, or type **revert** and press **Enter** to abort.

Section 13.1.10.6
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, or type **revert** and press **Enter** to abort.

Section 13.1.10.7
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:** A 64-bit unsigned integer The number of bytes sent on conn-sync dedicated link.
byte-received	**Synopsis:** A 64-bit unsigned integer The number of bytes received on conn-sync dedicated link.
packet-sent	**Synopsis:** A 64-bit unsigned integer The number of packets sent on conn-sync dedicated link.
packet-received	**Synopsis:** A 64-bit unsigned integer The number of packets received on conn-sync dedicated link.
error-sent	**Synopsis:** A 64-bit unsigned integer The number of errors sent on conn-sync dedicated link.
error-received	**Synopsis:** A 64-bit unsigned integer The number of errors received on conn-sync dedicated link.

Section 13.2

Managing VRRP within VRF

RUGGEDCOM ROX II supports VRRP configuration within VRF definitions, for IPv4 addresses. This allows gateway redundancy to be applied to individual VRF instances.

For more information about virtual routing and forwarding, refer to Section 12.11.1, “VRF Concepts”.

CONTENTS

- Section 13.2.1, “Configuring VRRP within VRF”
- Section 13.2.2, “Viewing the VRRP Status for a VRF”
- Section 13.2.3, “Configuring VRRP Service for a VRF”

- Section 13.2.4, “Managing VRRP Trackers for a VRF”
- Section 13.2.5, “Managing VRRP Groups for a VRF”
- Section 13.2.6, “Managing VRRP Instances for a VRF”
- Section 13.2.7, “Managing VRRP Monitors for a VRF”
- Section 13.2.8, “Managing VRRP Track Scripts for a VRF”
- Section 13.2.9, “Managing Virtual IP Addresses for a VRF”
- Section 13.2.10, “Example: Configuring VRRP within a VRF”

Section 13.2.1

Configuring VRRP within VRF

To configure VRRP within a VRF, do the following:

1. Configure virtual routing and forwarding. For more information, refer to Section 12.11.3, “Configuring VRF”.
2. Enable the VRRP service for each VRF definition. For more information, refer to Section 13.2.3.2, “Adding VRRP Service to a VRF”.
3. [Optional] Add VRRP trackers as needed. For more information, refer to Section 13.2.4.2, “Adding a VRRP Tracker for a VRF”.
4. [Optional] Add VRRP groups as needed. For more information, refer to Section 13.2.5.2, “Adding a VRRP Group for a VRF”.
5. [Optional] Add VRRP monitors as needed. For more information, refer to Section 13.2.7.2, “Adding a VRRP Monitor to a VRF”.
6. [Optional] Add track scripts as needed. For more information, refer to Section 13.2.8.2, “Adding a VRRP Track Script to a VRF”.
7. Add a virtual IP address for the VRF. For more information, refer to Section 13.2.9.2, “Adding a Virtual IP Address to a VRF”.
8. Verify the network configuration.

Section 13.2.2

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. This parameter is mandatory.
priority	**Synopsis:** A string The VRRP instance priority. This parameter is mandatory.
time-change	**Synopsis:** A string The time of change to the current state. This parameter is mandatory.
interface-state	**Synopsis:** A string The VRRP interface state. This parameter is mandatory.

Section 13.2.3
Configuring VRRP Service for a VRF

This section describes how to view, add and delete VRRP for a VRF.

CONTENTS

- Section 13.2.3.1, "Viewing a List of VRFs Configured with VRRP Service"
- Section 13.2.3.2, "Adding VRRP Service to a VRF"
- Section 13.2.3.3, "Deleting VRRP Service from a VRF"

Section 13.2.3.1
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 Section 13.2.3.2, "Adding VRRP Service to a VRF".

Section 13.2.3.2
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, or type **revert** and press **Enter** to abort.

Section 13.2.3.3
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, or type **revert** and press **Enter** to abort.

Section 13.2.4
Managing VRRP Trackers for a VRF

VRRP trackers monitor the state/condition of a route. When the route is unavailable, VRRP will lower its priority or transition it to a fault state.

NOTE
The decision to increase or decrease the priority of a route must be done in coordination with any backup VRRP Routers since the priority decides whether a router becomes a Master or a Backup. For example, if Router X's priority is 150 and Router Y's priority is 145, Router X's priority must be lowered by 6 to make it a Backup router.

CONTENTS

- Section 13.2.4.1, "Viewing a List of VRRP Trackers for a VRF"
- Section 13.2.4.2, "Adding a VRRP Tracker for a VRF"
- Section 13.2.4.3, "Deleting a VRRP Tracker for a VRF"

Section 13.2.4.1
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 Section 13.2.4.2, "Adding a VRRP Tracker for a VRF".

Section 13.2.4.2
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 9 to 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:** A 32-bit unsigned integer between 1 and 120 The number of seconds between tracker queries. This parameter is mandatory.
weight { weight }	**Synopsis:** A 32-bit signed 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:** A 32-bit unsigned integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
fall { fall }	**Synopsis:** A 32-bit unsigned 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, or type **`revert`** and press **Enter** to abort.

Section 13.2.4.3
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, or type **`revert`** and press **Enter** to abort.

Section 13.2.5
Managing VRRP Groups for a VRF

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

CONTENTS

- Section 13.2.5.1, "Viewing a List of VRRP Groups for a VRF"
- Section 13.2.5.2, "Adding a VRRP Group for a VRF"
- Section 13.2.5.3, "Deleting a VRRP Group"

Section 13.2.5.1
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 Section 13.1.5.2, "Adding a VRRP Group".

Section 13.2.5.2
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 }	**Synopsis:** A string 1 to 64 characters long The VRRP group name.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 13.2.5.3
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, or type **revert** and press **Enter** to abort.

Section 13.2.6
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.

CONTENTS

- Section 13.2.6.1, “Viewing a List of VRRP Instances for a VRF”
- Section 13.2.6.2, “Adding a VRRP Instance for a VRF”
- Section 13.2.6.3, “Deleting a VRRP Instance for a VRF”

Section 13.2.6.1
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 Section 13.2.6.2, “Adding a VRRP Instance for a VRF”.

Section 13.2.6.2
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:

> **IMPORTANT!**
> *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 Section 6.8.10.2, "Adding an Interface".*

Parameter	Description
vrrp-version { vrrp-version }	**Synopsis:** An 8-bit unsigned integer between 2 and 3 **Default:** 2 Configure VRRP version for this instance.
interface { interface }	**Synopsis:** A string The interface that will host the VRIP when the router becomes the VRRP Master. This parameter is mandatory.
vrid { vrid }	**Synopsis:** An 8-bit unsigned integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID. This parameter is mandatory.
priority { priority }	**Synopsis:** An 8-bit unsigned 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. This parameter is mandatory.
advert-interval { advert-interval }	**Synopsis:** An 8-bit unsigned integer between 1 and 255 **Default:** 1 VRRP2 advertisement interval, in seconds.
advert-interval-millisecond { advert-interval-millisecond }	**Synopsis:** A 32-bit unsigned integer between 20 and 3000 **Default:** 1000 VRRP3 advertisement interval in millisecond, must be multiple of 10.
garp-delay { garp-delay }	**Synopsis:** An 8-bit unsigned 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:** A 32-bit unsigned integer between 0 and 1000 **Default:** 0 The time, in seconds, after startup until preemption.

Parameter	Description
fault-to-master-delay { fault-to-master-delay }	**Synopsis:** A 32-bit unsigned 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 VRIP interface.
group { group }	**Synopsis:** A string Binds this VRRP instance to a VRRP group.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 13.2.6.3
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, or type **`revert`** and press **Enter** to abort.

Section 13.2.7
Managing VRRP Monitors for a VRF

A VRRP monitor selects an extra interface to monitor. If the interface becomes unavailable, the router will relinquish control of the gateway IP address to another VRRP Router.

CONTENTS

- Section 13.2.7.1, “Viewing a List of VRRP Monitors for a VRF”
- Section 13.2.7.2, “Adding a VRRP Monitor to a VRF”
- Section 13.2.7.3, “Deleting a VRRP Monitor from a VRF”

Section 13.2.7.1
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 Section 13.2.7.2, "Adding a VRRP Monitor to a VRF".

Section 13.2.7.2
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:** A 32-bit signed 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, or type **revert** and press **Enter** to abort.

Section 13.2.7.3
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 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 delete

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 13.2.8
Managing VRRP Track Scripts for a VRF

Track scripts are used to associate VRRP trackers with VRRP instances.

CONTENTS

- Section 13.2.8.1, "Viewing a List of VRRP Track Scripts for a VRF"
- Section 13.2.8.2, "Adding a VRRP Track Script to a VRF"
- Section 13.2.8.3, "Deleting a VRRP Track Script from a VRF"

Section 13.2.8.1
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 Section 13.2.8.2, "Adding a VRRP Track Script to a VRF".

Section 13.2.8.2
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:** A 32-bit signed 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, or type **revert** and press **Enter** to abort.

Section 13.2.8.3
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, or type **revert** and press **Enter** to abort.

Section 13.2.9
Managing Virtual IP Addresses for a VRF

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

CONTENTS

- Section 13.2.9.1, “Viewing a List of Virtual IP Addresses”
- Section 13.2.9.2, “Adding a Virtual IP Address to a VRF”
- Section 13.2.9.3, “Deleting a Virtual IP Address from a VRF”

Section 13.2.9.1
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 Section 13.2.9.2, "Adding a Virtual IP Address to a VRF".

Section 13.2.9.2
Adding a Virtual IP Address to a VRF

IMPORTANT!
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, or type **revert** and press **Enter** to abort.

Section 13.2.9.3
Deleting a Virtual IP Address from a VRF

To delete a virtual IP address from a VRF, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 13.2.10

Example: Configuring VRRP within a VRF

This example demonstrates how to configure VRRP within a VRF instance.

The following topology depicts a scenario where a PC/host is attempting to send a packet to a destination via a default gateway (VRIP) owned by the VRRP routers. If the Master router (R1) fails, a backup router (R2) is elected Master and acts as the gateway. The previous Master then transitions to a fault state or becomes a backup.

IMPORTANT!
RUGGEDCOM ROX II supports VRRP within VRF for IPv4 addresses only.

IMPORTANT!
Connection synchronization is not supported for VRRPs within a VRF. For more information about connection synchronization, refer to Section 13.1.1.3, "Connection Synchronization".

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

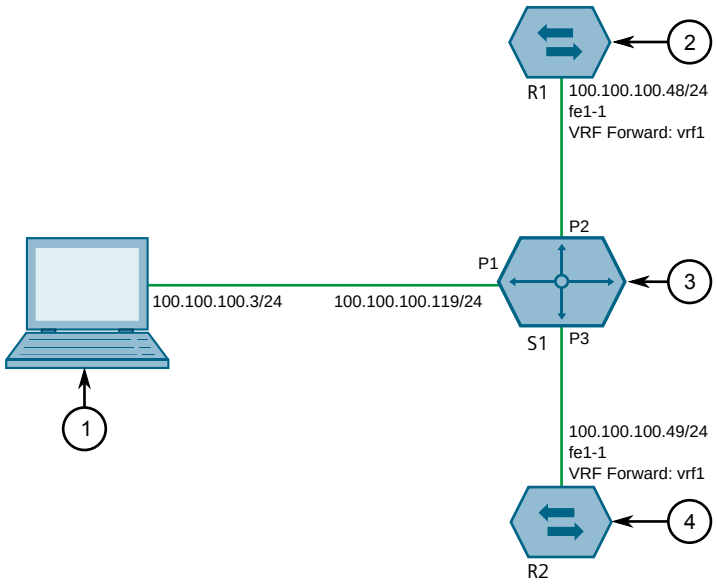


Figure 40: Topology – VRRP within a VRF

1. PC **2.** Router R1 **3.** Layer 2 Switch S1 **4.** Router R2

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 Section 8.5.5.2, "Adding a Static VLAN".

   b. Assign IP address *100.100.100.119* to VLAN 100. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

   c. Assign VLAN 100 to ports 1, 2 and 3. For more information, refer to Section 8.1.2, "Configuring a Switched Ethernet Port".

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 Section 12.11.5.2, "Adding a VRF Definition".

   b. Define a route target for vrf1 of type `both` with the export community set to **`100:1`**. For more information, refer to Section 12.11.6.2, "Adding a Route Target".

   c. Make sure interface fe-1-1 is configured with the IP address 100.100.100.48/24.

   d. Assign the interfaces in Step 5.c to forward traffic to vrf1. For more information, refer to Section 12.11.4, "Configuring a VRF Interface".

   e. Enable VRRP Service for VRF. For more information, refer to Section 13.2.3.2, "Adding VRRP Service to a VRF".

f. Configure a VRF instance with the folowing parameters:

Interface	Virtual Router ID	Priority
fe-1-1	101	150

For more information, refer to Section 13.2.6.2, "Adding a VRRP Instance for a VRF".

g. Add virtual IP address 100.100.100.101/24 to the VRF. For more information, refer to Section 13.2.9.2, "Adding a Virtual IP Address to a VRF".

6. Configure router R2:

a. Configure a VRF definition for *vrf1* with a route distinguisher of **100:1**. For more information, refer to Section 12.11.5.2, "Adding a VRF Definition".

b. Define a route target for vrf1 of type `both` with the export community set to **100:1**. For more information, refer to Section 12.11.6.2, "Adding a Route Target".

c. Make sure interface fe-1-1 is configured with the IP address 100.100.100.49/24.

d. Assign the interfaces in Step 6.c to forward traffic to vrf1. For more information, refer to Section 12.11.4, "Configuring a VRF Interface".

e. Enable VRRP Service for VRF. For more information, refer to Section 13.2.3.2, "Adding VRRP Service to a VRF".

f. Configure a VRF instance with the folowing parameters:

Interface	VRID	Priority
fe-1-1	101	130

For more information, refer to Section 13.2.6.2, "Adding a VRRP Instance for a VRF".

g. Add virtual IP address 100.100.100.101/24 to the VRF. For more information, refer to Section 13.2.9.2, "Adding a Virtual IP Address to a VRF".

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
```

Section 13.3
Managing Link Failover Protection

Link failover provides an easily configurable means of raising a backup link upon the failure of a designated main link. The main and backup links can be Ethernet and Cellular Modem.

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.

CONTENTS

- Section 13.3.1, “Viewing the Link Failover Log”
- Section 13.3.2, “Viewing the Link Failover Status”
- Section 13.3.3, “Managing Link Failover Parameters”
- Section 13.3.4, “Managing Link Failover Backup Interfaces”
- Section 13.3.5, “Managing Link Failover Ping Targets”
- Section 13.3.6, “Testing Link Failover”
- Section 13.3.7, “Canceling a Link Failover Test”

Section 13.3.1
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"
```

Section 13.3.2

Viewing the Link Failover Status

The Link Failover Status form displays the current link failover status. To view the link failover status, do the following:

```
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

Parameter	Description
	The backup link state.
backup-interface-in-use	**Synopsis:** A string The name of the backup interface that is being used.

Section 13.3.3
Managing Link Failover Parameters

This section describes how to manage parameter settings for link failover.

CONTENTS

- Section 13.3.3.1, “Viewing a List of Link Failover Parameters”
- Section 13.3.3.2, “Adding a Link Failover Parameter”
- Section 13.3.3.3, “Deleting a Link Failover Parameter”

Section 13.3.3.1
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 Section 13.3.3.2, “Adding a Link Failover Parameter”.

Section 13.3.3.2
Adding a Link Failover Parameter

To add a link failover parameter, do the following:

NOTE
The link failover feature can only be configured on a routable interface. For the link failover feature to be used on a switched port, another VLAN must be configured (for example, switch.0002) to logically differentiate the switched port from the default PVID VLAN 1 (switch.0001).

1. 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:** A 32-bit signed integer between 1 and 65536 **Default:** 2 The time interval, in seconds, before immediately retrying a ping.
ping-interval { ping-interval }	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 60 The time interval, in seconds, between ping tests.
ping-retry { ping-retry }	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 3 The number of ping retries before constructing a path failure.
start-delay { start-delay }	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 180 The delay time, in seconds, when first starting link failover.
main-down-timeout { main-down-timeout }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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, or type **revert** and press **Enter** to abort.

Section 13.3.3.3
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, or type **revert** and press **Enter** to abort.

Section 13.3.4
Managing Link Failover Backup Interfaces

A backup interface is the interface to which link failover switches when the main interface is determined to be down. You can add up to three backup interfaces to each link failover configuration.

CONTENTS

- Section 13.3.4.1, "Viewing a List of Link Failover Backup Interfaces"
- Section 13.3.4.2, "Adding a Link Failover Backup Interface"
- Section 13.3.4.3, "Deleting a Link Failover Backup Interface"

Section 13.3.4.1
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 Section 13.3.4.2, "Adding a Link Failover Backup Interface".

Section 13.3.4.2
Adding a Link Failover Backup Interface

To set a link failover backup interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the backup interface by typing:

```
services link-failover interface backup backup-interface
```

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 { backup-gateway }	**Synopsis:** A string 1 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, or type **revert** and press **Enter** to abort.

Section 13.3.4.3
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 backup-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, or type **revert** and press **Enter** to abort.

Section 13.3.5

Managing Link Failover Ping Targets

A link failover ping target is an IP address that link failover pings to determine if the main link is down. The address can be a dedicated host or a dummy address on a router. Up to three link failover ping targets can be added to each link failover configuration.

CONTENTS

- Section 13.3.5.1, "Viewing a List of Link Failover Ping Targets"
- Section 13.3.5.2, "Adding a Link Failover Ping Target"
- Section 13.3.5.3, "Deleting a Link Failover Ping target"

Section 13.3.5.1

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 target
```

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 Section 13.3.5.2, "Adding a Link Failover Ping Target".

Section 13.3.5.2

Adding a Link Failover Ping Target

To add a link failover ping target, do the following:

NOTE
Link failover pings each target separately. If all targets are down, the main link is considered to be down and it fails over to the backup interface. Backup links are used in the order of their Priority setting (first, second, and then third), always starting with the first priority interface. When a higher-priority interface becomes available again, the system reverts to the higher priority interface. For example, if the second priority interface is active, the system switches back to the first priority interface when the first priority interface becomes available again.

1. 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, or type **revert** and press **Enter** to abort.

Section 13.3.5.3
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, or type **revert** and press **Enter** to abort.

Section 13.3.6
Testing Link Failover

The link failover settings can be tested to confirm that each link failover configuration works properly. To launch the test, specify for how long the system should operate on the backup interface, and for how long the system should delay before starting the test. Canceling the test returns the interfaces to their pre-test condition.

While the test is running, monitor the status of the test to observe the main and backup link status, ping test results, state change, backup state, and backup interface information. As the test progresses, this information changes as link failover switches from the main interface to the backup interface. For more information on the **Link Fail Over Status** form, refer to Section 13.3.2, "Viewing the Link Failover Status".

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 Section 13.3.7, "Canceling a Link Failover Test".

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

Section 13.3.7
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

Section 13.4
Managing Spanning Tree Protocol

This section describes how to manage the Spanning Tree Protocol (STP).

CONTENTS

- Section 13.4.1, "RSTP Operation"
- Section 13.4.2, "RSTP Applications"
- Section 13.4.3, "MSTP Operation"
- Section 13.4.4, "Configuring STP Globally"
- Section 13.4.5, "Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces"
- Section 13.4.6, "Managing Multiple Spanning Tree Instances Globally"
- Section 13.4.7, "Managing Multiple Spanning Tree Instances Per-Port"
- Section 13.4.8, "Viewing the Status of RSTP"
- Section 13.4.9, "Viewing RSTP Per-Port Statistics"
- Section 13.4.10, "Clearing Spanning Tree Protocol Statistics"

Section 13.4.1
RSTP Operation

The IEEE 802.1D Spanning Tree Protocol (STP) was developed to enable the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer halt after a link outage until all bridges in the network are guaranteed to be aware of the new topology. Using the values recommended by IEEE 802.1D, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (RSTP), first introduced by IEEE 802.1w and significantly improved in IEEE 802.12D-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.

CONTENTS

- Section 13.4.1.1, “RSTP States and Roles”
- Section 13.4.1.2, “Edge Ports”
- Section 13.4.1.3, “Point-to-Point and Multipoint Links”
- Section 13.4.1.4, “Path and Port Costs”
- Section 13.4.1.5, “Bridge Diameter”
- Section 13.4.1.6, “eRSTP”
- Section 13.4.1.7, “Fast Root Failover”

Section 13.4.1.1

RSTP States and Roles

RSTP bridges have roles to play, either root or designated. One bridge – the Root Bridge – is the logical center of the network. All other bridges in the network are Designated bridges. RSTP also assigns each port of the bridge a state and a role. The RSTP state describes what is happening at the port in relation to address learning and frame forwarding. The RSTP role basically describes whether the port is facing the center or the edges of the network and whether it can currently be used.

State

There are three RSTP states: Discarding, Learning and Forwarding.

The discarding state is entered when the port is first put into service. The port does not learn addresses in this state and does not participate in frame transfer. The port looks for RSTP traffic in order to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to learning.

The learning state is entered when the port is preparing to play an active part in the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP bridges, the time spent in this state is usually quite short. RSTP bridges operating in STP compatibility mode will spend six to 40 seconds in this state.

After *learning*, the bridge will place the port in the forwarding state. The port both learns addresses and participates in frame transfer while in this state.

IMPORTANT!
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.

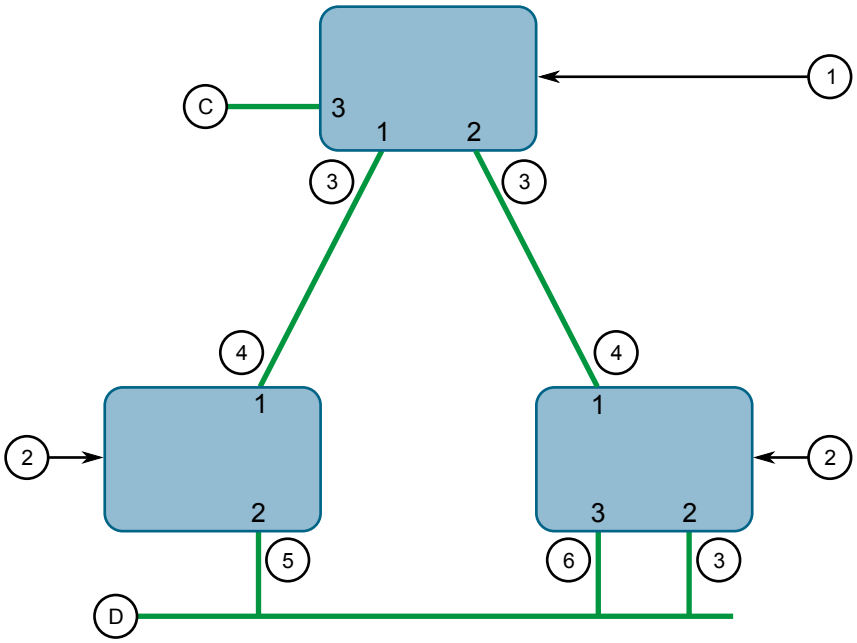


Figure 41: Bridge and Port Roles

1. Root Bridge **2.** Designated Bridge **3.** Designated Port **4.** Root Port **5.** Alternate Port **6.** Backup Port

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.

Section 13.4.1.2
Edge Ports

A port may be designated as an Edge Port if it is directly connected to an end station. As such, it cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages.

Edge ports that receive configuration messages immediately lose their Edge Port status and become normal spanning tree ports. A loop created on an improperly connected edge port is thus quickly repaired.

Because an Edge Port services only end stations, topology change messages are not generated when its link toggles.

Section 13.4.1.3
Point-to-Point and Multipoint Links

RSTP uses a peer-peer protocol called Proposing-Agreeing to ensure transitioning in the event of a link failure. This protocol is point-to-point and breaks down in multipoint situations, i.e. when more than two bridges operate on a shared media link.

If RSTP detects this circumstance (based upon the port's half duplex state after link up) it will switch off Proposing-Agreeing. The port must transition through the learning and forwarding states, spending one forward delay in each state.

There are circumstances in which RSTP will make an incorrect decision about the point-to-point state of the link simply by examining the half-duplex status, namely:

- The port attaches only to a single partner, but through a half-duplex link.
- The port attaches to a shared media hub through a full-duplex link. The shared media link attaches to more than one RSTP enabled bridge.

In such cases, the user may configure the bridge to override the half-duplex determination mechanism and force the link to be treated in the proper fashion.

Section 13.4.1.4
Path and Port Costs

The STP path cost is the main metric by which root and designated ports are chosen. The path cost for a designated bridge is the sum of the individual port costs of the links between the root bridge and that designated bridge. The port with the lowest path cost is the best route to the root bridge and is chosen as the root port.

NOTE
In actuality the primary determinant for root port selection is the root bridge ID. Bridge ID is important mainly at network startup when the bridge with the lowest ID is elected as the root bridge. After startup (when all bridges agree on the root bridge's ID) the path cost is used to select root ports. If the path costs of candidates for the root port are the same, the ID of the peer bridge is used to select the port. Finally, if candidate root ports have the same path cost and peer bridge ID, the port ID of the peer bridge is used to select the root port. In all cases the lower ID, path cost or port ID is selected as the best.

How Port Costs Are Generated

Port costs can be generated either as a result of link auto-negotiation or manual configuration. When the link auto-negotiation method is used, the port cost is derived from the speed of the link. This method is useful when a well-connected network has been established. It can be used when the designer is not too concerned with the resultant topology as long as connectivity is assured.

Manual configuration is useful when the exact topology of the network must be predictable under all circumstances. The path cost can be used to establish the topology of the network exactly as the designer intends.

STP vs. RSTP Costs

The STP specification limits port costs to values of 1 to 65536. Designed at a time when 9600 bps links were state of the art, this method breaks down in modern use, as the method cannot represent a link speed higher than 10 Gbit/s.

To remedy this problem in future applications, the RSTP specification limits port costs to values of 1 to 20000000, and a link speed up to 10 Tbit/s can be represented with a value of 2.

Section 13.4.1.5
Bridge Diameter

The bridge diameter is the maximum number of bridges between any two possible points of attachment of end stations to the network.

The bridge diameter reflects the realization that topology information requires time to propagate hop by hop through a network. If configuration messages take too long to propagate end to end through the network, the result will be an unstable network.

There is a relationship between the bridge diameter and the maximum age parameter.

NOTE
The RSTP algorithm is as follows:

- *STP configuration messages contain **age** information.*
- *Messages transmitted by the root bridge have an age of 0. As each subsequent designated bridge transmits the configuration message it must increase the age by at least 1 second.*
- *When the age exceeds the value of the maximum age parameter the next bridge to receive the message immediately discards it.*

To achieve extended ring sizes, Siemens's eRSTP™ uses an age increment of ¼ of a second. The value of the maximum bridge diameter is thus four times the configured maximum age parameter.

IMPORTANT!
Raise the value of the maximum age parameter if implementing very large bridged networks or rings.

Section 13.4.1.6
eRSTP

Siemens's enhanced Rapid Spanning Tree Protocol (eRSTP) improves the performance of RSTP in two ways:

- Improves the fault recovery time performance (< 5 ms per hop)
- Improves performance for large ring network topologies (up to 160 switches)

eRSTP is also compatible with standard RSTP for interoperability with commercial switches.

For example, in a network comprised of 15 RUGGEDCOM hardened Ethernet switches in a ring topology, the expected fault recovery time would be less than 75 ms (i.e. 5 ms x 15). However, with eRSTP, the worst case fault recovery time is less than 26 ms.

Section 13.4.1.7
Fast Root Failover

Siemens's *Fast Root Failover* feature is an enhancement to RSTP that may be enabled or disabled. Fast Root Failover improves upon RSTP's handling of root bridge failures in mesh-connected networks, resulting in slightly increased failover times for some non-root bridge scenarios.

IMPORTANT!
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

Section 13.4.2
RSTP Applications

This section describes various applications of RSTP.

CONTENTS

- Section 13.4.2.1, “RSTP in Structured Wiring Configurations”
- Section 13.4.2.2, “RSTP in Ring Backbone Configurations”
- Section 13.4.2.3, “RSTP Port Redundancy”

Section 13.4.2.1

RSTP in Structured Wiring Configurations

RSTP may be used to construct structured wiring systems where connectivity is maintained in the event of link failures. For example, a single link failure of any link between A and N in Figure 42 would leave all the ports of bridges 555 through 888 connected to the network.

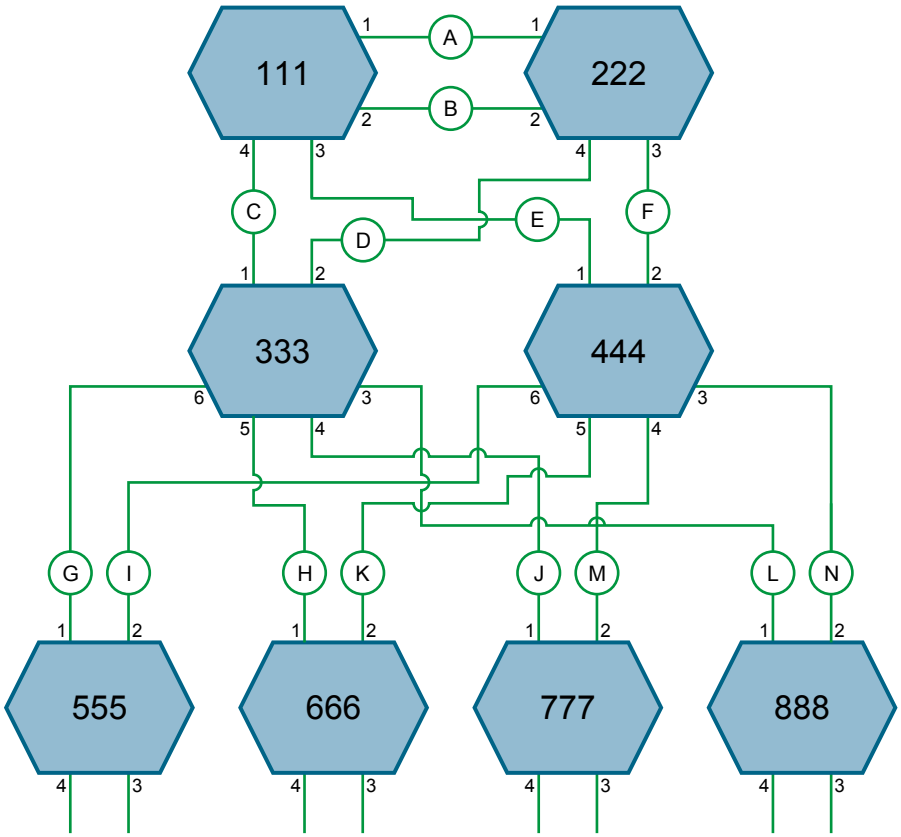


Figure 42: Example - Structured Wiring Configuration

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.

Section 13.4.2.2

RSTP in Ring Backbone Configurations

RSTP may be used in ring backbone configurations where rapid recovery from link failure is required. In normal operation, RSTP will block traffic on one of the links. For an example, refer to link H in Figure 43. 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.

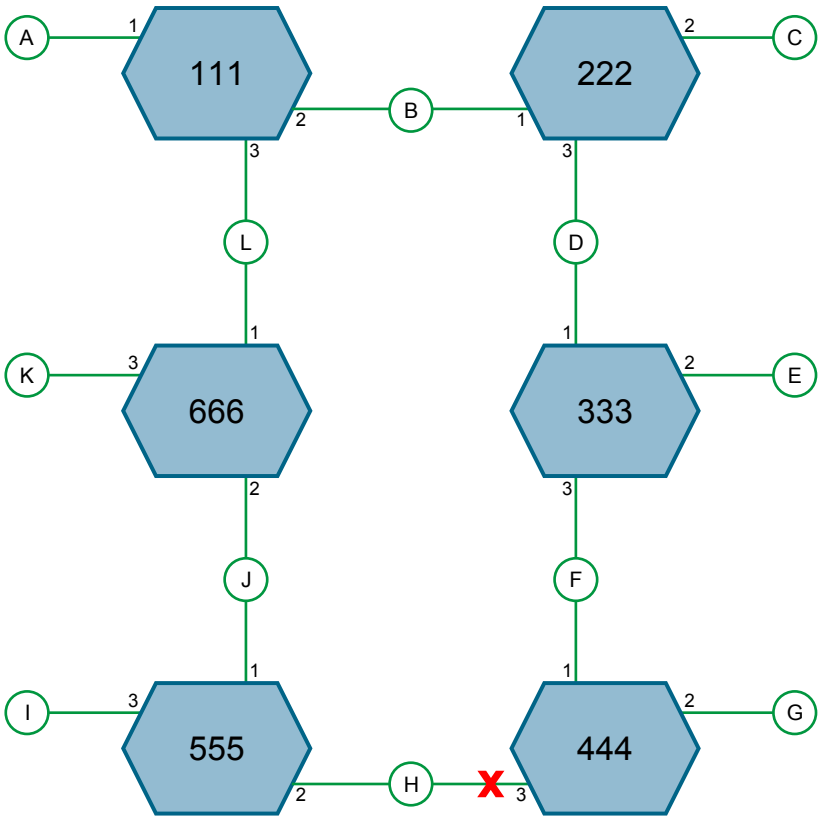


Figure 43: Example - Ring Backbone Configuration

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 RSTP in Ring Network Topologies* available on https://www.siemens.com/ruggedcom.

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.

Section 13.4.2.3
RSTP Port Redundancy

In cases where port redundancy is essential, RSTP allows more than one bridge port to service a LAN. In the following example, if port 3 is designated to carry the network traffic of LAN A, port 4 will block traffic. Should an interface failure occur on port 3, port 4 will assume control of the LAN.

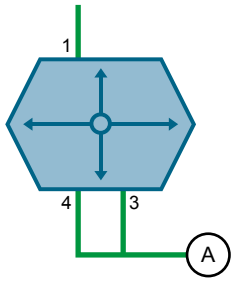


Figure 44: Example - Port Redundancy

Section 13.4.3
MSTP Operation

The Multiple Spanning Tree (MST) algorithm and protocol provide greater control and flexibility than RSTP and legacy STP. MSTP (Multiple Spanning Tree Protocol) is an extension of RSTP, whereby multiple spanning trees may be maintained on the same bridged network. Data traffic is allocated to one or several spanning trees by mapping one or more VLANs to different Multiple Spanning Tree Instances (MSTIs).

The sophistication and utility of the MSTP implementation on a given bridged network is proportional to the amount of planning and design invested in configuring MSTP.

If MSTP is activated on some or all of the bridges in a network with no additional configuration, the result will be a fully and simply connected network. At best though, the result will be the same as a network using only RSTP. Taking full advantage of the features offered by MSTP requires a potentially large number of configuration variables to be derived from an analysis of data traffic on the bridged network, and from requirements for load sharing, redundancy, and path optimization. Once these parameters have all been derived, it is also critical they are consistently applied and managed across all bridges in an MST region.

By design, MSTP processing time is proportional to the number of active STP instances. This means MSTP will likely be significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

CONTENTS

- Section 13.4.3.1, "MSTP Regions and Interoperability"
- Section 13.4.3.2, "MSTP Bridge and Port Roles"
- Section 13.4.3.3, "Benefits of MSTP"
- Section 13.4.3.4, "Implementing MSTP on a Bridged Network"

Section 13.4.3.1

MSTP Regions and Interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of interoperating 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.

Section 13.4.3.2

MSTP Bridge and Port Roles

MSTP supports the following bridge and port roles:

Bridge Roles

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.
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.

Role	Description
	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 MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.

Section 13.4.3.3
Benefits of MSTP

MSTP is configured by default to arrive automatically at a spanning tree solution for each configured MSTI. However, advantages may be gained from influencing the topology of MSTIs in an MST region by way of the Bridge Priority and the cost of each port.

Load Balancing

MSTP can be used to balance the data traffic load among sets of VLANs, enabling more complete utilization of a bridged network that has multiple redundant interconnections between bridges.

A bridged network controlled by a single spanning tree will block redundant links by design to avoid harmful loops. However, when using MSTP, any given link may have a different blocking state for MSTI, as maintained by MSTP. Any given link, therefore, might be in blocking state for some VLANs, and in forwarding state for other VLANs, depending on the mapping of VLANs to MSTIs.

It is possible to control the spanning tree solution for each MSTI, especially the set of active links for each tree, by manipulating per MSTI the bridge priority and the port costs of links in the network. If traffic is allocated judiciously to multiple VLANs, redundant interconnections in a bridged network, which would have gone unused when using a single spanning tree, can now be made to carry traffic.

Isolation of Spanning Tree Reconfiguration.

A link failure in an MSTP region that does not affect the roles of Boundary ports will not cause the CST to be reconfigured, nor will the change affect other MSTP regions. This is due to the fact that MSTP information does not propagate past a region boundary.

MSTP versus PVST

An advantage of MSTP over the Cisco Systems Inc. proprietary Per-VLAN Spanning Tree (PVST) protocol is the ability to map multiple VLANs onto a single MSTI. Since each spanning tree requires processing and memory, the expense of keeping track of an increasing number of VLANs increases much more rapidly for PVST than for MSTP.

» Compatibility with STP and RSTP

No special configuration is required for the bridges of an MST region to connect fully and simply to non-MST bridges on the same bridged network. Careful planning and configuration is, however, recommended to arrive at an optimal network design.

Section 13.4.3.4

Implementing MSTP on a Bridged Network

The following procedure is recommended for configuring MSTP on a network. Beginning with a set of MSTP-capable Ethernet bridges, do the following for each bridge on the network:

NOTE
Careful network analysis and planning should inform each step of creating an MSTP network.

NOTE
MSTP does not need to be enabled to map a VLAN to an MSTI. However, the mapping must be identical for each bridge that belongs to the MSTP region.

1. Disable STP. For more information, refer to Section 13.4.4, "Configuring STP Globally".
2. Configure one or more Multiple Spanning Tree Instances (MSTI), each with a unique bridge priority. For more information, refer to Section 13.4.6.3, "Adding a Multiple Spanning Tree Instance".
3. Create static VLANs and map them to the MSTIs. For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".
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 Section 13.4.7, "Managing Multiple Spanning Tree Instances Per-Port".
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 Section 13.4.4, "Configuring STP Globally".

Section 13.4.4

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	**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.
version { version }	**Synopsis:** { stp, rstp, mstp } **Default:** rstp

Parameter	Description
	The version (either only STP or Rapid STP or Multiple STP) of the Spanning Tree Protocol (STP) to support.
hello-time { hello-time }	**Synopsis:** A 32-bit unsigned 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:** A 32-bit unsigned 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:** A 32-bit unsigned 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:** A 32-bit unsigned 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:** A 32-bit unsigned 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.
mst-region-name { mst-region-name }	**Synopsis:** A string 1 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:** A 32-bit unsigned 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

Parameter	Description
	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:** A 32-bit unsigned 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. • 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	**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 Section 13.4.6.3, "Adding a Multiple Spanning Tree Instance".
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 13.4.5

Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces

To configure the Spanning Tree Protocol (STP) for a switched Ethernet port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to:
   - **For switched Ethernet ports:**
     interface » switch » swport » {port} » spanning-tree, where *{port}* is the port number of 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	**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.
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 a 32-bit unsigned integer between 0 and 65535 **Default:** auto-cost

Parameter	Description
	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 a 32-bit unsigned 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 Section 13.4.6.3, "Adding a Multiple Spanning Tree Instance".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 13.4.6
Managing Multiple Spanning Tree Instances Globally

MSTP (Multiple Spanning Tree Protocol), as defined by the IEEE 802.1 standard, maps multiple VLANs to a single Spanning Tree instance, otherwise referred to as a Multiple Spanning Tree Instance (MSTI).

Each MSTI is assigned an MST ID and a bridge priority:

- The MST ID is used to associate the MSTI with a VLAN.
- The bridge priority is used by all devices in the Spanning Tree topology to determine which device among them is elected the root device or backbone. An ideal root device is one that is central to the network and not connected to end devices.

For more information about MSTP, refer to Section 13.4.3, "MSTP Operation".

CONTENTS

- Section 13.4.6.1, "Viewing Statistics for Multiple Spanning Tree Instances"
- Section 13.4.6.2, "Viewing a List of Multiple Spanning Tree Instances"
- Section 13.4.6.3, "Adding a Multiple Spanning Tree Instance"
- Section 13.4.6.4, "Deleting a Multiple Spanning Tree Instance"

Section 13.4.6.1
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
```

This table or list provides the following information:

Parameter	Description
instance-id	**Synopsis:** A 32-bit signed 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. This parameter is mandatory.
root-priority	**Synopsis:** A 32-bit signed integer The bridge identifier of the root bridge. This parameter is mandatory.
root-mac	**Synopsis:** A string 17 characters long The bridge identifier of the root bridge. This parameter is mandatory.
bridge-priority	**Synopsis:** A 32-bit signed integer The bridge identifier of this bridge. This parameter is mandatory.
bridge-mac	**Synopsis:** A string 17 characters long The bridge identifier of this bridge. This parameter is mandatory.
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. This parameter is mandatory.
root-port-port	**Synopsis:** A 32-bit signed integer If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network. This parameter is mandatory.
root-path-cost	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	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. This parameter is mandatory.
total-top-changes	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.

Section 13.4.6.2
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 Section 13.4.6.3, “Adding a Multiple Spanning Tree Instance”.

Section 13.4.6.3
Adding a Multiple Spanning Tree Instance

To add a Multiple Spanning Tree Instance (MSTI), do the following:

NOTE
RUGGEDCOM ROX II supports up to 16 MSTIs.

1. Make sure the CLI is in Configuration mode.

   IMPORTANT!
   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 Section 8.5.5.2, "Adding a Static VLAN".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 13.4.6.4
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, or type **revert** and press **Enter** to abort.

Section 13.4.7
Managing Multiple Spanning Tree Instances Per-Port

This section describes how to configure and manage Multiple Spanning Tree Instances (MSTIs) for individual ports.

CONTENTS

- Section 13.4.7.1, "Viewing Per-Port Multiple Spanning Tree Instance Statistics"
- Section 13.4.7.2, "Viewing a List of Per-Port Multiple Spanning Tree Instances"
- Section 13.4.7.3, "Adding a Port-Specific Multiple Spanning Tree Instance"
- Section 13.4.7.4, "Deleting a Port-Specific Multiple Spanning Tree Instances"

Section 13.4.7.1

Viewing Per-Port Multiple Spanning Tree Instance Statistics

To view Multiple Spanning Tree Instance (MSTI) statistics for individual switched Ethernet ports and/or Ethernet trunk interfaces, 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:** A 32-bit signed integer between 1 and 16 The Multiple Spanning Tree Protocol (MSTP) Instance ID.
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:** A 32-bit signed 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. This parameter is mandatory.
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.

Parameter	Description
	• 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). This parameter is mandatory.
cost	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
desig-bridge-priority	**Synopsis:** A 32-bit signed integer The bridge identifier of this bridge. This parameter is mandatory.
desig-bridge-mac	**Synopsis:** A string 17 characters long The bridge identifier of this bridge. This parameter is mandatory.

Section 13.4.7.2
Viewing a List of Per-Port Multiple Spanning Tree Instances

To view a list of the Multiple Spanning Tree Instances (MSTIs) for switched Ethernet ports or Ethernet trunk interfaces, type:

- **For switched Ethernet ports:**

  ```
  show running-config interface switch swport port spanning-tree msti
  ```

  Where:

  - *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 Section 13.4.7.3, "Adding a Port-Specific Multiple Spanning Tree Instance".

Section 13.4.7.3

Adding a Port-Specific Multiple Spanning Tree Instance

To add a Multiple Spanning Tree Instance (MSTI) for a switched Ethernet port or an Ethernet trunk interface, do the following:

NOTE
RUGGEDCOM ROX II supports up to 16 MSTIs per port/interface.

1. Make sure the CLI is in Configuration mode.

IMPORTANT!
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 swport 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 a 32-bit unsigned 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 a 32-bit unsigned 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 Section 8.5.5.2, "Adding a Static VLAN".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 13.4.7.4
Deleting a Port-Specific Multiple Spanning Tree Instances

To delete a Multiple Spanning Tree Instance (MSTI) for a switched Ethernet port or an Ethernet trunk interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the MSTI by typing:
   - **For switched Ethernet ports:**
     ```
     no interface switch swport 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, or type **`revert`** and press **Enter** to abort.

Section 13.4.8
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           swport
 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. This parameter is mandatory.
bridge-priority	**Synopsis:** A 32-bit signed integer The bridge identifier of this bridge. This parameter is mandatory.
bridge-mac	**Synopsis:** A string 17 characters long The bridge identifier of this bridge. This parameter is mandatory.
root-priority	**Synopsis:** A 32-bit signed integer The ports to which the multicast group traffic is forwarded. This parameter is mandatory.
root-mac	**Synopsis:** A string 17 characters long The ports to which the multicast group traffic is forwarded. This parameter is mandatory.
regional-root-priority	**Synopsis:** A 32-bit signed integer The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to. This parameter is mandatory.

Parameter	Description
regional-root-mac	**Synopsis:** A string 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. This parameter is mandatory.
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. This parameter is mandatory.
root-port-port	**Synopsis:** A 32-bit signed integer If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network. This parameter is mandatory.
root-path-cost	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
regional-root-path-cost	**Synopsis:** A 32-bit unsigned 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 This parameter is mandatory.
configured-hello-time	**Synopsis:** A 32-bit signed integer The configured hello time from the Bridge RSTP Parameters menu. This parameter is mandatory.
learned-hello-time	**Synopsis:** A 32-bit signed integer The actual hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges. This parameter is mandatory.
configured-forward-delay	**Synopsis:** A 32-bit signed integer The configured forward delay time from the Bridge RSTP Parameters menu. This parameter is mandatory.
learned-forward-delay	**Synopsis:** A 32-bit signed integer The actual forward delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges. This parameter is mandatory.
configured-max-age	**Synopsis:** A 32-bit signed integer The configured maximum age time from the Bridge RSTP Parameters menu. This parameter is mandatory.
learned-max-age	**Synopsis:** A 32-bit signed integer The actual maximum age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.

Parameter	Description
	This parameter is mandatory.
total-top-changes	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.

Section 13.4.9
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 | tab
                                        DESG
                                        BRIDGE                          OPER  RX    TX     RX       TX
       RX    TX
SLOT    PORT  STP STATE   STP ROLE    COST  PRIORITY  DESG BRIDGE MAC    EDGE  RSTS  RSTS   CONFIGS
 CONFIGS  TCNS  TCNS
-------------------------------------------------------------------------------------------------
swport  4     forwarding  designated  19    0         00:00:00:00:00:00  true  0     43086  0        0
       0     0
```

This table or list provides the following information:

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:** A 32-bit signed 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. This parameter is mandatory.
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.

Parameter	Description
	• 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). This parameter is mandatory.
cost	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
desg-bridge-priority	**Synopsis:** A 32-bit signed 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. This parameter is mandatory.
desg-bridge-mac	**Synopsis:** A string 17 characters long Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to. This parameter is mandatory.
oper-edge	**Synopsis:** { true, false } Whether or not the port is operating as an edge port. This parameter is mandatory.
rx-rsts	**Synopsis:** A 32-bit unsigned integer The number of Rapid Spanning Tree Protocol (RSTP) configuration messages received on this port. This parameter is mandatory.
tx-rsts	**Synopsis:** A 32-bit unsigned integer The number of Rapid Spanning Tree Protocol (RSTP) configuration messages transmitted on this port. This parameter is mandatory.
rx-configs	**Synopsis:** A 32-bit unsigned integer The number of Spanning Tree Protocol (STP) configuration messages received on this port. This parameter is mandatory.
tx-configs	**Synopsis:** A 32-bit unsigned integer The number of Spanning Tree Protocol (STP) configuration messages transmitted on this port. This parameter is mandatory.
rx-tcns	**Synopsis:** A 32-bit unsigned integer The number of configuration change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems. This parameter is mandatory.
tx-tcns	**Synopsis:** A 32-bit unsigned integer The number of configuration messages transmitted from this port.

Parameter	Description
	This parameter is mandatory.

Section 13.4.10

Clearing Spanning Tree Protocol Statistics

To clear all Spanning Tree Protocol statistics, type:

```
switch spanning-tree clear-stp-stats
```

14 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.

CONTENTS

- Section 14.1, “Managing LLDP”
- Section 14.2, “Managing SNMP”
- Section 14.3, “Managing NETCONF”

Section 14.1

Managing LLDP

RUGGEDCOM ROX II supports the Link Layer Discovery Protocol (LLDP), a Layer 2 protocol for automated network discovery.

LLDP is an IEEE standard protocol (IEEE 802.11AB) that allows a networked device to advertise its own basic networking capabilities and configuration. It can simplify the troubleshooting of complex networks and can be used by Network Management Systems (NMS) to obtain and monitor detailed information about a network’s topology. LLDP data are made available via SNMP (through support of LLDP-MIB).

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device’s information at regular intervals, in 802.1AB 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.

CAUTION!
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.

CONTENTS

- Section 14.1.1, "Configuring LLDP"
- Section 14.1.2, "Viewing Global Statistics and Advertised System Information"
- Section 14.1.3, "Viewing Statistics for LLDP Neighbors"
- Section 14.1.4, "Viewing Statistics for LLDP Ports"

Section 14.1.1
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	**Synopsis:** { true, false } **Default:** true Enables LLDP, making the device an LLDP agent.
tx-interval { tx-interval }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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:** A 32-bit signed 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.
tx-delay { tx-delay }	**Synopsis:** A 32-bit signed integer between 1 and 8192 **Default:** 2

Parameter	Description
	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:** A 32-bit signed 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, or type **`revert`** and press **Enter** to abort.

Section 14.1.2
Viewing Global Statistics and Advertised System Information

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
```

This table or list displays the following information:

Parameter	Description
inserts	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of new hosts added to the LLDP Neighbor Information Table. This parameter is mandatory.
deletes	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of hosts deleted from the LLDP Neighbor Information Table. This parameter is mandatory.
drops	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of hosts detected that could not be added to the LLDP Neighbor Information Table. This parameter is mandatory.
ageouts	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
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

Parameter	Description
	(e.g. P1Y1M2W3DT2H3M30S represents 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30 seconds). This parameter is mandatory.

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
```

This 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 • 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 This parameter is mandatory.
local-chassis-id	**Synopsis:** A string 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. This parameter is mandatory.
local-system-name	**Synopsis:** A string 1 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. This parameter is mandatory.
local-system-desc	**Synopsis:** A string 1 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.

Parameter	Description
	This parameter is mandatory.
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 This parameter is mandatory.
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 • 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 This parameter is mandatory.

Section 14.1.3
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 swport 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
```

This 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.
port	**Synopsis:** A 32-bit signed integer between 1 and 16 The number of the port on which the device receives LLDP frames from the LLDP neighbor. Port numbers are indicated on the front plate silkscreen of the module. The port is contained in the slot module specified by the **Slot (slot)** parameter.
chassis-id	**Synopsis:** A string 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 17 characters long The remote port from which the LLDP neighbor sends LLDP frames to the device. The value of the **Port ID (port-id)** parameter is categorized by the **Port Subtype (port-subtype)** parameter.
system-name	**Synopsis:** A string 1 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 1 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 1 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 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:** A 32-bit signed 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

Parameter	Description
	• wlanAccessPoint - The neighbor host can forward network traffic to/from a WLAN • 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 • 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

Parameter	Description
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 • 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 • systemPortNumber - The **Management Address Interface ID (man-address-if-id)** corresponds with a locally defined port number
last-update	**Synopsis:** A string

Parameter	Description
	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).

Section 14.1.4
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
-------------------------------------------------------
swport  1     0    0    0    0    0        0     0
swport  2     0    0    0    0    0        0     0
swport  3     0    0    0    0    0        0     0
swport  4     0    0    208  209  0        0     0
swport  5     0    0    0    0    0        0     0
swport  6     0    0    0    0    0        0     0
```

This 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.
port	**Synopsis:** A 32-bit signed 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:** A 32-bit unsigned integer between 0 and 4294967295 The total number of incoming LLDP frames dropped by the port. This parameter is mandatory.
err-frm	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of incoming LLDP frames received on the port with detectable errors. This parameter is mandatory.
frm-in	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of incoming LLDP frames received on the port. This parameter is mandatory.
frm-out	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of outgoing LLDP frames broadcast on the port. This parameter is mandatory.
ageouts	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295

Parameter	Description
	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. This parameter is mandatory.
tlvs-drop	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of TLVs discarded from LLDP frames received on the port. This parameter is mandatory.
tlvs-unknown	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total number of unrecognized TLVs in LLDP frames received on the port. This parameter is mandatory.

Section 14.2

Managing SNMP

The Simple Network Management Protocol (SNMP) is used by network management systems and the devices they manage. It is used to report alarm conditions and other events that occur on the devices it manages.

In addition to SNMPv1 and SNMPv2, RUGGEDCOM ROX II also supports SNMPv3, which offers the following features:

- Provides the ability to send a notification of an event via *traps*. Traps are unacknowledged UDP messages and may be lost in transit.
- Provides the ability to notify via *informs*. Informs simply add acknowledgment 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

CONTENTS

- Section 14.2.1, “MIB Files and SNMP Traps”
- Section 14.2.2, “Enabling and Configuring SNMP Sessions”
- Section 14.2.3, “Viewing Statistics for SNMP”

- Section 14.2.4, “Discovering SNMP Engine IDs”
- Section 14.2.5, “Managing SNMP Communities”
- Section 14.2.6, “Managing SNMP Target Addresses”
- Section 14.2.7, “Managing SNMP Users”
- Section 14.2.8, “Managing SNMP Security Model Mapping”
- Section 14.2.9, “Managing SNMP Group Access”

Section 14.2.1

MIB Files and SNMP Traps

The current MIB files supported by RUGGEDCOM ROX II can be downloaded from the https://www.siemens.com/ruggedcom.

NOTE
SNMP traps are not configurable in RUGGEDCOM ROX II.

The MIB files support the following SNMP traps:

Standard	MIB	Trap and Description
RFC 3418	SNMPv2-MIB	**authenticationFailure** 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.
		coldStart 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 A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.
RFC 4188	BRIDGE-MIB	**newRoot** 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 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.
IEEE Std 802.1AB-2005	LLDP-MIB	**lldpRemTablesChange** 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.

Standard	MIB	Trap and Description
RFC 1229, 2863, 2233, 1573	IF-MIB	**linkUp** 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 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.
RuggedCom	RUGGEDCOM-TRAPS-MIB	**genericTrap** A generic trap generated by RUGGEDCOM devices.
		rcSuccessChgPwdTrap A trap used when a password change is successful.
		rcUserLoginFailureTrap Reports the user, reason, IP address, context and protocol linked to a login failure.
		powerSupplyTrap A trap generated when a power supply fails or is restored.
		swUpgradeTrap A generic trap generated upon software upgrade.
		cfgChangeTrap A generic trap generated upon configuration change.
		fanBankTrap A trap generated when a fan bank fails or fails to come up.
		hotswapModuleStateChangeTrap A trap generated when a RUGGEDCOM ROX II module changes state.
		rcCellularModemStatsTrap A trap generated when a cell modem SIM failover event occurs.
RFC 3895	DS1-MIB	**ds1LineStatusChange** A ds1LineStatusChange trap is sent when the status of a dsx1Line instance changes. The value of the trap is the value of one or more of the following instances: • **dsx1RcvFarEndLOF** – Far end Loss of Frames (i.e. yellow alarm or RAI) • **dsx1RcvAIS** – Far end sending AIS • **dsx1LossOfFrame** – Near end Loss of Frame (i.e. red alarm) • **dsx1LossofSignal** – Near end Loss of Signal • **dsx1OtherFailure** – Out of Frame • **dsx1NoAlarm**

Section 14.2.2
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:

IMPORTANT!
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.*

IMPORTANT!
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 Section 14.2.1, "MIB Files and SNMP Traps".*

Parameter	Description
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:** A 16-bit unsigned 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:** a 32-bit unsigned 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. Engine IDs consist of 5 to 32 colon-separated octets (e.g. nn:nn:nn:nn:nn). Each octet is a 2-digit hexadecimal number. The default ID is the enterprise number of the device followed by its MAC address. 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	**Synopsis:** { true, false } **Default:** false Enables/disables the SNMP to send generic authentication traps.
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 8-bit unsigned 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, or type **`revert`** and press **Enter** to abort.

Section 14.2.3
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
```

This table or list provides the following information:

Parameter	Description
unsupported-sec-levels	**Synopsis:** A 32-bit unsigned integer The total number of incoming SNMP packets dropped because they requested an unknown or unavailable security level. This parameter is mandatory.
not-in-time-windows	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The total number of incoming SNMP packets dropped because they were received after the authoritative SNMP engine's time out period expired. This parameter is mandatory.
unknown-user-names	**Synopsis:** A 32-bit unsigned integer The total number of incoming SNMP packets dropped because they referenced an unknown user. This parameter is mandatory.
unknown-engine-ids	**Synopsis:** A 32-bit unsigned integer The total number of incoming SNMP packets dropped because they referenced an unknown SNMP Engine ID. This parameter is mandatory.
wrong-digests	**Synopsis:** A 32-bit unsigned integer The total number of incoming SNMP packets dropped because they contained an unexpected digest value (i.e. authentication key). This parameter is mandatory.
decryption-errors	**Synopsis:** A 32-bit unsigned integer The total number of incoming SNMP packets dropped because they could not be decrypted. This parameter is mandatory.

Section 14.2.4
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
```

Section 14.2.5
Managing SNMP Communities

This section describes how to manage SNMP communities.

CONTENTS

- Section 14.2.5.1, “Viewing a List of SNMP Communities”
- Section 14.2.5.2, “Adding an SNMP Community”
- Section 14.2.5.3, “Deleting an SNMP Community”

Section 14.2.5.1
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 Section 14.2.5.2, “Adding an SNMP Community”.

Section 14.2.5.2
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 The user name associated with the community string. This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 14.2.5.3
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, or type **revert** and press **Enter** to abort.

Section 14.2.6
Managing SNMP Target Addresses

This section describes how to manage SNMP target addresses.

CONTENTS

- Section 14.2.6.1, "Viewing a List of SNMP Target Addresses"
- Section 14.2.6.2, "Adding an SNMP Target Address"
- Section 14.2.6.3, "Deleting an SNMP Target Address"

Section 14.2.6.1
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 Section 14.2.6.2, "Adding an SNMP Target Address".

Section 14.2.6.2
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 1 to 32 characters long

Parameter	Description
	The unique name for the SNMP target.
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. This parameter is mandatory.
trap-port { trap-port }	**Synopsis:** A 16-bit unsigned 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 The recognized user name. Only this user name is permitted to exchange SNMP packets with the target. This parameter is mandatory.
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*.
control-community { control-community }	**Synopsis:** A string 1 to 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

Parameter	Description
	NOTE *Multiple options can be selected.*
inform-timeout { inform-timeout }	**Synopsis:** A 32-bit signed 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:** A 32-bit signed 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. Engine IDs consist of 5 to 32 colon-separated octets (e.g. nn:nn:nn:nn:nn). Each octet is a 2-digit hexadecimal number.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 14.2.6.3
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, or type **`revert`** and press **Enter** to abort.

Section 14.2.7
Managing SNMP Users

This section describes how to manage SNMP users.

CONTENTS

- Section 14.2.7.1, “Viewing a List of SNMP Users”
- Section 14.2.7.2, “Adding an SNMP User”
- Section 14.2.7.3, “Deleting an SNMP User”

Section 14.2.7.1
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 Section 14.2.7.2, “Adding an SNMP User”.

Section 14.2.7.2
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

   CAUTION!
   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:

Parameter	Description
	• 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 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 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, or type **`revert`** and press **Enter** to abort.

Section 14.2.7.3
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, or type **`revert`** and press **Enter** to abort.

Section 14.2.8
Managing SNMP Security Model Mapping

This section describes how to manage the mapping of SNMP security models.

CONTENTS

• Section 14.2.8.1, “Viewing a List of SNMP Security Models”

- Section 14.2.8.2, “Adding an SNMP Security Model”
- Section 14.2.8.3, “Deleting an SNMP Security Model”

Section 14.2.8.1
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 Section 14.2.8.2, “Adding an SNMP Security Model”.

Section 14.2.8.2
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, or type **`revert`** and press **Enter** to abort.

Section 14.2.8.3
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, or type **revert** and press **Enter** to abort.

Section 14.2.9

Managing SNMP Group Access

This section describes how to manage access for SNMP groups.

CONTENTS

- Section 14.2.9.1, "Viewing a List of SNMP Groups"
- Section 14.2.9.2, "Adding an SNMP Group"
- Section 14.2.9.3, "Deleting an SNMP Group"

Section 14.2.9.1

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 Section 14.2.9.2, "Adding an SNMP Group".

Section 14.2.9.2

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 • 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, or type **revert** and press **Enter** to abort.

Section 14.2.9.3
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, or type **revert** and press **Enter** to abort.

Section 14.3
Managing NETCONF

The Network Configuration Protocol (NETCONF) is a network configuration protocol developed by the Internet Engineering Task Force (IETF). NETCONF provides functions to download, upload, change, and delete the configuration data on network devices. RUGGEDCOM ROX II devices also support the ability to collect data and perform direct actions on the device, such as rebooting the device, clearing statistics, and restarting services.

NOTE
For more information about NETCONF and its use, refer to the NETCONF Reference Guide for RUGGEDCOM ROX II v2.13.

CONTENTS

- Section 14.3.1, "Enabling and Configuring NETCONF Sessions"
- Section 14.3.2, "Viewing NETCONF Statistics"

Section 14.3.1
Enabling and Configuring NETCONF Sessions

To enable and configure NETCONF sessions, do the following:

1. Make sure the CLI is in Configuration mode.

CAUTION!
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).

IMPORTANT!
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	**Synopsis:** { true, false } **Default:** true

Parameter	Description
	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:** A 16-bit unsigned 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:** a 32-bit unsigned 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, or type **`revert`** and press **Enter** to abort.
4. [Optional] Enable the NETCONF summary log (saved under `/var/log/netconf.log`) to record all NETCONF protocol transactions. For more information, refer to Section 4.12.4.3, “Enabling/Disabling the NETCONF Summary Log”.
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 Section 4.12.4.4, “Enabling/Disabling the NETCONF Trace Log”.

Section 14.3.2
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
```

This table or list provides the following information:

Parameter	Description
in-bad-hellos	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
in-sessions	**Synopsis:** A 32-bit unsigned integer The total number of NETCONF sessions initiated on the device. This parameter is mandatory.
dropped-sessions	**Synopsis:** A 32-bit unsigned integer The total number of NETCONF sessions dropped on the device. This parameter is mandatory.
in-rpcs	**Synopsis:** A 32-bit unsigned integer The total number of NETCONF requests (i.e. rpc messages) received. This parameter is mandatory.
in-bad-rpcs	**Synopsis:** A 32-bit unsigned integer The total number of NETCONF requests (i.e. rpc messages) dropped because they contained non-conformant XML. This parameter is mandatory.
out-rpc-errors	**Synopsis:** A 32-bit unsigned 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 a client that one or more errors occurred in processing its NETCONF request (i.e. rpc message). This parameter is mandatory.
out-notifications	**Synopsis:** A 32-bit unsigned integer The total number of notification messages sent. This parameter is mandatory.

15 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.

CONTENTS

- Section 15.1, “Managing Port Mirroring”
- Section 15.2, “Managing Traffic Control”
- Section 15.3, “Managing Classes of Service”
- Section 15.4, “Managing NetFlow Data Export”
- Section 15.5, “Managing Port Rate Limiting”

Section 15.1

Managing Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to another mirror port. If a protocol analyzer were attached to the target port, the traffic stream of valid frames on any source port is made available for analysis.

Select a target port that has a higher speed than the source port. Mirroring a 100 Mbps port onto a 10 Mbps port may result in an improperly mirrored stream.

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port’s transmission rate. This problem reaches its extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.

Invalid frames received on the source port will not be mirrored. These include CRC errors, oversized and undersized packets, fragments, jabbers, collisions, late collisions and dropped events).

NOTE

Port mirroring has the following limitations:

- *The target port may sometimes incorrectly show the VLAN tagged/untagged format of the mirrored frames.*
- *Network management frames (such as RSTP, GVRP, etc.) may not be mirrored.*
- *Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) may not be mirrored.*

CONTENTS

- Section 15.1.1, “Configuring Port Mirroring”

- Section 15.1.2, "Managing Egress Source Ports"
- Section 15.1.3, "Managing Ingress Source Ports"

Section 15.1.1
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***.

   IMPORTANT!
   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 Section 8.5.3, "Enabling/Disabling Ingress Filtering".
3. Configure port mirroring for a specific port by typing:

   ```
   switch port-mirroring enabled target-slot swport target-port port egress-src egress ingress-src ingress
   ```

   Where:
   - *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 Section 15.1.2.2, "Adding an Egress Source Port" and Section 15.1.3.2, "Adding an Ingress Source Port".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.1.2
Managing Egress Source Ports

This section describes how to configure and manage egress source ports for port mirroring.

CONTENTS

- Section 15.1.2.1, "Viewing a List of Egress Source Ports"
- Section 15.1.2.2, "Adding an Egress Source Port"
- Section 15.1.2.3, "Deleting an Egress Source Port"

Section 15.1.2.1
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 swport 1
 !
!
```

If no egress source ports have been configured, add egress source ports as needed. For more information, refer to Section 15.1.2.2, “Adding an Egress Source Port”.

Section 15.1.2.2
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 swport port
   ```

   Where:

   - *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.

Section 15.1.2.3
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 swport port
   ```

   Where:

   - *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.

Section 15.1.3
Managing Ingress Source Ports

This section describes how to configure and manage egress source ports for port mirroring.

CONTENTS

- Section 15.1.3.1, “Viewing a List of Ingress Source Ports”
- Section 15.1.3.2, “Adding an Ingress Source Port”
- Section 15.1.3.3, “Deleting an Ingress Source Port”

Section 15.1.3.1
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 swport 1
 !
!
```

If no ingress source ports have been configured, add ingress source ports as needed. For more information, refer to Section 15.1.3.2, “Adding an Ingress Source Port”.

Section 15.1.3.2
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 swport port
   ```

   Where:

   - *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.

Section 15.1.3.3
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 swport port
```

Where:

- *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.

Section 15.2

Managing Traffic Control

Traffic control is a firewall subsystem that manages the amount of bandwidth for each network interface that different types of traffic are permitted to use. For a traffic control configuration to work, a firewall must be configured.

NOTE
For more information about firewalls, refer to Section 6.8, "Managing Firewalls".

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.

CONTENTS

- Section 15.2.1, "Enabling and Configuring Traffic Control"
- Section 15.2.2, "Managing Traffic Control Interfaces"
- Section 15.2.3, "Managing Traffic Control Priorities"
- Section 15.2.4, "Managing Traffic Control Classes"
- Section 15.2.5, "Managing Traffic Control Devices"
- Section 15.2.6, "Managing Traffic Control Rules"
- Section 15.2.7, "Managing QoS Mapping for VLANs"
- Section 15.2.8, "Managing Egress Markers for QoS Maps"
- Section 15.2.9, "Viewing QoS Statistics"

Section 15.2.1

Enabling and Configuring Traffic Control

Traffic control functions are divided into two modes:

- **Basic Mode**
  Basic mode offers a limited set of options and parameters. Use this mode to set the outgoing bandwidth for an interface, the interface priority (high, medium or low), and some simple traffic control characteristics. Basic traffic shaping affects traffic identified by protocol, port number, address and interface. Note that some of these options are mutually exclusive. Refer to the information given for each option.

  In basic mode, a packet is categorized based on the contents of its Type of Service (ToS) field if it does not match any of the defined classes.

- **Advanced Mode**
  In advanced mode, each interface to be managed is assigned a total bandwidth for incoming and outgoing traffic. Classes are then defined for each interface, each with its own minimum assured bandwidth and a maximum permitted bandwidth. The combined minimum of the classes on an interface must be no more than the total outbound bandwidth specified for the interface. Each class is also assigned a priority, and any bandwidth left over after each class has received its minimum allocation (if needed) will be allocated to the lowest priority class up until it reaches its maximum bandwidth, after which the next priority is allocated more bandwidth. When the specified total bandwidth for the interface is reached, no further packets are sent, and any further packets may be dropped if the interface queues are full.

  Packets are assigned to classes on the outbound interface based on either a mark assigned to the packet, or the Type of Service (ToS) field in the IP header. If the ToS field matches a defined class, the packet is allocated to that class. Otherwise, it is allocated to any class that matches the mark assigned to the packet. If no class matches the mark, the packet is assigned to the default class.

  Marks are assigned to packets by traffic control rules that are based on a number of parameters, such as IP address, port number, protocol, packet length, and more.

The two modes cannot be accessed simultaneously. Only the mode that is currently configured can be accessed.

To enable and configure traffic control, do the following:

1. 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 Section 15.2.2.2, “Adding a Traffic Control Interface”.
   b. Add traffic control priorities. For more information, refer to Section 15.2.3.2, “Adding a Traffic Control Priority”.
4. If advanced mode is enabled, do the following:
   a. Add traffic control classes. For more information, refer to Section 15.2.4.2, “Adding a Traffic Control Class”.
   b. Add traffic control devices. For more information, refer to Section 15.2.5.2, “Adding a Traffic Control Device”.

c. Add traffic control rules. For more information, refer to Section 15.2.6.2, "Adding a Traffic Control Rule".

5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 15.2.2
Managing Traffic Control Interfaces

Traffic control interfaces define interfaces used for traffic shaping, mainly for outbound bandwidth and the outgoing device.

NOTE
Traffic control interfaces can only be configured in basic mode. For more information about setting the traffic control mode, refer to Section 15.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

- Section 15.2.2.1, "Viewing a List of Traffic Control Interfaces"
- Section 15.2.2.2, "Adding a Traffic Control Interface"
- Section 15.2.2.3, "Deleting a Traffic Control Interface"

Section 15.2.2.1
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 tcinterfaces
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 Section 15.2.2.2, "Adding a Traffic Control Interface".

Section 15.2.2.2
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 interface
```

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 { inbandwidth }	**Synopsis:** A 16-bit unsigned 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 { outbandwidth }	**Synopsis:** A 16-bit unsigned integer The outgoing bandwidth for this interface. Specify only the number here. The unit (kilobits, megabits) is specified in the out-unit. This parameter is mandatory.
out-unit { out-unit }	**Synopsis:** { kilobits, megabits } **Default:** megabits The unit for outgoing bandwidth, per second.
description { description }	**Synopsis:** A string A description for this configuration item.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.2.2.3
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, or type **revert** and press **Enter** to abort.

Section 15.2.3
Managing Traffic Control Priorities

Traffic control priorities define priorities used for traffic shaping.

NOTE
Traffic control priorities can only be configured in basic mode. For more information about setting the traffic control mode, refer to Section 15.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

- Section 15.2.3.1, "Viewing a List of Traffic Control Priorities"
- Section 15.2.3.2, "Adding a Traffic Control Priority"
- Section 15.2.3.3, "Deleting a Traffic Control Priority"

Section 15.2.3.1
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 tcpriorities
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 Section 15.2.3.2, "Adding a Traffic Control Priority".

Section 15.2.3.2
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), mmc+mr+mt (0x0e).
protocol { protocol }	**Synopsis:** { tcp, udp, icmp, all } or a string (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 { interface }	**Synopsis:** A string 1 to 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 { description }	**Synopsis:** A string (optional) A description for this configuration.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 15.2.3.3
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, or type **revert** and press **Enter** to abort.

Section 15.2.4
Managing Traffic Control Classes

Traffic control classes define classes for traffic shaping. Optionally, they can also define parameters for Type of Service (ToS), which is an eight-bit field in the IPv4 header. Traffic control can inspect the ToS value of an incoming IP frame and classify traffic to provide preferential service in the outgoing queue. Traffic classification is done based on the ToS value and the ToS options defined for each traffic control class and traffic control rule. IP Traffic matching with the ToS options takes precedence over the mark rules.

NOTE
One traffic control class must be added for each network interface.

NOTE
Type of Service (ToS) is defined by the Internet Engineering Task Force (IETF). For more information about ToS, refer to RFC 1349 [http://tools.ietf.org/html/rfc1349].

CONTENTS

- Section 15.2.4.1, “Viewing a List of Traffic Control Classes”
- Section 15.2.4.2, “Adding a Traffic Control Class”
- Section 15.2.4.3, “Deleting a Traffic Control Class”

Section 15.2.4.1
Viewing a List of Traffic Control Classes

To view a list of traffic control classes, type:

```
show running-config qos traffic-control advanced-configuration 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 tcclasses
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 Section 15.2.4.2, "Adding a Traffic Control Class".

Section 15.2.4.2
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. This parameter is mandatory.
mark { mark }	**Synopsis:** A 16-bit unsigned 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. This parameter is mandatory.
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: • 'full/3' for a third of the bandwidth and • 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any minbw-unit. This parameter is mandatory.
minbw-unit { minbw-unit }	**Synopsis:** { none, kilobits, megabits } **Default:** none

Parameter	Description
	(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: • 'full/3' for a third of the bandwidth and • 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any maxbw-unit. This parameter is mandatory.
maxbw-unit { maxbw-unit }	**Synopsis:** { none, kilobits, megabits } **Default:** none (per second) only if max-bandwidth is a **single numerical value**
priority { priority }	**Synopsis:** A 16-bit unsigned 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, or type **`revert`** and press **Enter** to abort.

Section 15.2.4.3
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, or type **`revert`** and press **Enter** to abort.

Section 15.2.5
Managing Traffic Control Devices

Traffic control devices define devices used for traffic shaping.

NOTE
Traffic control devices can only be configured in advanced mode. For more information about setting the traffic control mode, refer to Section 15.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

- Section 15.2.5.1, "Viewing a List of Traffic Control Devices"
- Section 15.2.5.2, "Adding a Traffic Control Device"
- Section 15.2.5.3, "Deleting a Traffic Control Device"

Section 15.2.5.1
Viewing a List of Traffic Control Devices

To view a list of traffic control devices, type:

```
show running-config qos traffic-control advanced-configuration 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 tcdevices
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 Section 15.2.5.2, "Adding a Traffic Control Device".

Section 15.2.5.2
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 }

Parameter	Description
	Default: ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
inbandwidth { inbandwidth }	**Synopsis:** A 16-bit unsigned 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 { outbandwidth }	**Synopsis:** A 16-bit unsigned 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. This parameter is mandatory.
out-unit { out-unit }	**Synopsis:** { kilobits, megabits } **Default:** megabits Unit for outgoing bandwidth, per second.
description { description }	**Synopsis:** A string A description for this configuration item.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 15.2.5.3
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, or type **`revert`** and press **Enter** to abort.

Section 15.2.6
Managing Traffic Control Rules

Traffic control rules define rules for packet marking.

NOTE
Traffic control rules can only be configured in advanced mode. For more information about setting the traffic control mode, refer to Section 15.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

- Section 15.2.6.1, "Viewing a List of Traffic Control Rules"
- Section 15.2.6.2, "Adding a Traffic Control Rule"
- Section 15.2.6.3, "Configuring QoS Marking"
- Section 15.2.6.4, "Deleting aTraffic Control Rule"

Section 15.2.6.1
Viewing a List of Traffic Control Rules

To view a list of traffic control rules, type:

```
show running-config qos traffic-control advanced-configuration 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 Section 15.2.6.2, "Adding a Traffic Control Rule".

Section 15.2.6.2
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 This parameter is mandatory.
destination { destination }	**Synopsis:** A string IF name, comma-separated list of hosts or IPs, or 'all'. This parameter is mandatory.
protocol { protocol }	**Synopsis:** { tcp, udp, icmp, all } or a string **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 (Optional) Defines a test on the existing packet or connection mark. The default is a packet mark. For testing a connection mark, add ':C' at the end of the test value. Ex.: Test if the packet mark is not zero: **!0** Test if the connection mark is not zero: **!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 **65:** Lesser or equal to 65 **:65** In-between 64 and 768 **64:768**
tos { tos }	**Synopsis:** { minimize-delay, maximize-throughput, maximize-reliability, minimize-cost, normal-service } or a string (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, or type **`revert`** and press **Enter** to abort.

Section 15.2.6.3
Configuring QoS Marking

Quality of Service (QoS) marking applies a mark to important data packets that should receive preferential treatment as they travel through the network. Only one QoS mark is allowed for each traffic control rule. Options include:

- **Set:** Determines whether the packet or the connection is assigned the QoS mark.
- **Modify:** Changes the QoS mark value using an AND or OR argument.
- **Save/Restore:** Replaces the connection's QoS mark value with an assigned value.
- **Continue:** If the packet matches, no more traffic control rules are checked and the packet is automatically forwarded to the specified chain.
- **DSCP Marking:** Determines whether the packet is assigned the DSCP mark.

To configure the QoS mark for a traffic control rule, do the following:

Configuring a Set Mark

1. 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).

Parameter	Description
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, or type **`revert`** and press **Enter** to abort.

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, or type **`revert`** and press **Enter** to abort.

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

Parameter	Description
	A chain in which the operation will take place.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

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, or type **revert** and press **Enter** to abort.

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, or type **revert** and press **Enter** to abort.

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, or type **revert** and press **Enter** to abort.

Section 15.2.6.4
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, or type **revert** and press **Enter** to abort.

Section 15.2.7
Managing QoS Mapping for VLANs

Quality of Service (QoS) mapping is used to map QoS traffic. It assigns a traffic control mark to incoming IP traffic based on the priority value of a tagged frame. The incoming traffic is then classified and placed in the priority queues according to the traffic control rules specified for the marked rule. In addition, traffic control can assign the same priority or a different priority value when a frame needs to be egressed with a VLAN tag through a traffic control interface.

QoS maps can be configured for VLAN connections on virtual switches.

CONTENTS

- Section 15.2.7.1, “Viewing a List of QoS Maps for VLANs”
- Section 15.2.7.2, “Adding a QoS Map”
- Section 15.2.7.3, “Deleting a QoS Map”

Section 15.2.7.1
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 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

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 Section 15.2.7.2, "Adding a QoS Map".

Section 15.2.7.2
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 priority
     ```

     Where:

     - *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

3. Configure the following parameter(s) as required:

Parameter	Description
ingress { ingress }	**Synopsis:** An 8-bit unsigned integer between 0 and 255 Map ingress to mark. This parameter is mandatory.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.2.7.3
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 priority
     ```

     Where:
     - *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
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.2.8
Managing Egress Markers for QoS Maps

Egress markers for QoS maps are used to assign priority to traffic that shares the same mark as one of the egress marks configured for the device.

CONTENTS

- Section 15.2.8.1, “Viewing a List of Egress Marks”
- Section 15.2.8.2, “Adding an Egress Mark”
- Section 15.2.8.3, “Deleting an Egress Mark”

Section 15.2.8.1
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 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

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 Section 15.2.8.2, “Adding an Egress Mark”.

Section 15.2.8.2
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 priority 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 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

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.2.8.3
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 priority 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 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

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.2.9
Viewing QoS Statistics

RUGGEDCOM ROX II provides statistics for traffic going through each class that has been configured. Packets are assigned to classes on the outbound interface based on rules. If a packet matches the specified criteria, it is considered to be a member of the class and is forwarded to that class. If the packet does not match any rule, it is forwarded to the default class.

For more information about traffic control classes, refer to Section 15.2.4, "Managing Traffic Control Classes".

NOTE
Statistics are only available when traffic control is enabled in advanced mode. For more information about enabling traffic control, refer to Section 15.2.1, "Enabling and Configuring Traffic Control".

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
```

This table provides the following information:

Parameter	Description
classname	**Synopsis:** A string
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.
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.

Section 15.3
Managing Classes of Service

Classes of Service (CoS) provides the ability to expedite the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High or Critical. By default, RUGGEDCOM ROX II enforces Normal CoS for all traffic.

IMPORTANT!
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.

CONTENTS

- Section 15.3.1, "Configuring Classes of Service"
- Section 15.3.2, "Managing Priority-to-CoS Mapping"
- Section 15.3.3, "Managing DSCP-to-CoS Mapping"

Section 15.3.1

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 Section 15.3.2.2, "Adding a Priority-to-CoS Mapping Entry" or Section 15.3.3.2, "Adding a DSCP-to-CoS Mapping Entry".

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.3.2
Managing Priority-to-CoS Mapping

Assigning CoS to different IEEE 802.1p priority values in the frame is done by defining priority-to-CoS mapping table entries.

CONTENTS

- Section 15.3.2.1, "Viewing a List of Priority-to-CoS Mapping Entries"
- Section 15.3.2.2, "Adding a Priority-to-CoS Mapping Entry"
- Section 15.3.2.3, "Deleting a Priority-to-CoS Mapping Entry"

Section 15.3.2.1
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 Section 15.3.2.2, "Adding a Priority-to-CoS Mapping Entry".

Section 15.3.2.2
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, or type **`revert`** and press **Enter** to abort.

Section 15.3.2.3
Deleting a Priority-to-CoS Mapping Entry

To delete a priority-to-CoS mapping entry, do the following:

> **NOTE**
> *Deleting an entry sets the CoS to Normal.*

1. 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, or type **`revert`** and press **Enter** to abort.

Section 15.3.3
Managing DSCP-to-CoS Mapping

Assigning CoS to different values of the Differentiated Services Code Point (DSCP) field in the IP header of received packets is done by defining DSCP-to-CoS mapping table entries.

CONTENTS

- Section 15.3.3.1, “Viewing a List of DSCP-to-CoS Mapping Entries”
- Section 15.3.3.2, “Adding a DSCP-to-CoS Mapping Entry”
- Section 15.3.3.3, “Deleting a DSCP-to-CoS Mapping Entry”

Section 15.3.3.1
Viewing a List of DSCP-to-CoS Mapping Entries

To view a list of priorites, 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 Section 15.3.3.2, "Adding a DSCP-to-CoS Mapping Entry".

Section 15.3.3.2
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 Section 8.1.2, "Configuring a Switched Ethernet Port" and/or Section 8.2.2, "Adding an Ethernet Trunk Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.3.3.3
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, or type **revert** and press **Enter** to abort.

Section 15.4

Managing NetFlow Data Export

RUGGEDCOM ROX II supports the collection and forwarding of flow records to NetFlow-enabled servers, or NetFlow Collectors.

IMPORTANT!
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 Section 15.4.5, "Controlling the NetFlow Cache".

CONTENTS

- Section 15.4.1, "Understanding NetFlow Data Export"
- Section 15.4.2, "Configuring NetFlow Data Export"
- Section 15.4.3, "Enabling/Disabling NetFlow"
- Section 15.4.4, "Setting the NetFlow Engine ID"
- Section 15.4.5, "Controlling the NetFlow Cache"
- Section 15.4.6, "Controlling Active/Inactive Flows"
- Section 15.4.7, "Managing NetFlow Interfaces"
- Section 15.4.8, "Managing NetFlow Collectors"
- Section 15.4.9, "Viewing the Status of NetFlow"
- Section 15.4.10, "Example: Exporting Flows to Multiple Collectors"

Section 15.4.1

Understanding NetFlow Data Export

NetFlow is a traffic analysis tool developed by Cisco that allows network operators to characterize traffic flows across their networks. It provides information that allows operators to identify security vulnerabilities, assess network productivity and resource utilization, determine the causes of congestion, and more.

A basic NetFlow monitoring setup consists of the following components

- **Flow Exporter**
  The exporter aggregates data packets into flows, which are forwarded to one or more flow collectors.
- **Flow Collector**
  The collector receives, stores and pre-processes flow data received from one or more flow exporters.
- **Flow Analyzer**
  The flow analyzer queries one or more flow collectors for flow data and then analyzes the data with a focus on intrusion detection and traffic profiling.

RUGGEDCOM ROX II acts as a *flow exporter*, collecting data from ingress (incoming) and/or egress (outgoing) packets and then forwarding them as flow records to one or more collectors.

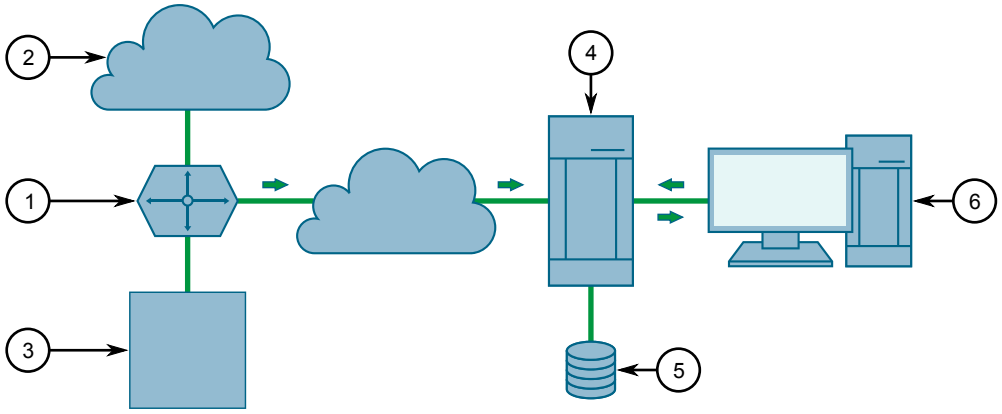


Figure 45: NetFlow

1. NetFlow Exporter (RUGGEDCOM ROX II) **2.** WAN **3.** LAN **4.** NetFlow Collector **5.** Flow Storage **6.** Analysis Console

NOTE
RUGGEDCOM ROX II supports NetFlow version 5.

CONTENTS

• Section 15.4.1.1, “Flow Records”

Section 15.4.1.1

Flow Records

A flow record, as defined by the Cisco standard, is a unidirectional sequence of packets that share the same:

- Ingress interface
- Source and destination IP address
- IP protocol
- Source and destination port for TCP and UDP
- Type of Service (ToS)

Each flow record is exported using the User Datagram Protocol (UDP), which requires each packet to include the IP address of the target NetFlow collector and its designated UDP port.

A flow record is considered ready to export when either of the following conditions are met:

- The flow has been inactive (e.g. no new packets) for a specific period of time
- The flow has been active for longer than allowed by the configuration
- A TCP flag indicates the flow has been terminated

RUGGEDCOM ROX II includes user-configurable timers for inactive and active flows.

NOTE
RUGGEDCOM ROX II does not retain a record of flows sent. Therefore, any NetFlow packets dropped due to congestion or packet corruption will be lost permanently.

Section 15.4.2
Configuring NetFlow Data Export

To configure the device to send flows to a NetFlow collector, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

   IMPORTANT!
   NetFlow does not support Layer 3 switching functions. Layer 3 switching must be disabled before NetFlow is enabled.

2. Enable the NetFlow service. For more information, refer to Section 15.4.3, "Enabling/Disabling NetFlow".
3. [Optional] Set the engine ID that is assigned to each flow record. For more information, refer to Section 15.4.4, "Setting the NetFlow Engine ID".
4. [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 Section 15.4.5, "Controlling the NetFlow Cache".
5. [Optional] Control how RUGGEDCOM ROX II manages active and inactive flows. For more information, refer to Section 15.4.6, "Controlling Active/Inactive Flows".
6. Define one or more interfaces from which to monitor traffic. For more information, refer to Section 15.4.7.2, "Adding a NetFlow Interface".
7. Define one or more NetFlow collectors to which RUGGEDCOM ROX II can send flows. For more information, refer to Section 15.4.8.2, "Adding a NetFlow Collector".

Section 15.4.3
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, or type **`revert`** and press **Enter** to abort.

Section 15.4.4
Setting the NetFlow Engine ID

An engine ID can be assigned to flow records to uniquely link them to the device from which they were sent. This can be useful information to network analysts wishing to further categorize NetFlow data by device, region, etc.

The engine ID is defined in the header of the data export.

To set an engine ID for the device, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 15.4.5
Controlling the NetFlow Cache

NetFlow consumes memory and CPU resources during operation, which may affect the performance of the device during times of high traffic. To reduce NetFlow's effect on performance, consider reducing the number of active flows tracked by NetFlow. This will reduce the cache and free resources for other processes.

To control the NetFlow cache, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 15.4.6
Controlling Active/Inactive Flows

NetFlow considers a flow to be ready for export when it has been inactive for a specific period of time or the flow has been active (long lived) for too long. By default, a flow is considered inactive if no new packets have been received for 15 seconds. An active flow is considered ready if it has received packets for longer than 30 minutes. Both durations can be adjusted to reduce or increase either the size of the NetFlow packets and/or the speed at which they are delivered.

To control how RUGGEDCOM ROX II manages active and inactive flows, do the following:

1. 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:** A 32-bit signed integer equaling 1 or higher **Default:** 1800 The time in seconds (s) an active flow remains active.
inactive-timeout { inactive-timeout }	**Synopsis:** A 32-bit signed integer equaling 1 or higher **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, or type **revert** and press **Enter** to abort.

Section 15.4.7

Managing NetFlow Interfaces

RUGGEDCOM ROX II requires an interface from which to collect NetFlow data, but can be configured to monitor multiple interfaces if needed. Each interface can be configured to monitor packets entering (ingress) and/or exiting (egress).

IMPORTANT!
RUGGEDCOM ROX II does not support Netflow data collection on hardware-accelerated interfaces.

CONTENTS

- Section 15.4.7.1, "Viewing a List of NetFlow Interfaces"
- Section 15.4.7.2, "Adding a NetFlow Interface"
- Section 15.4.7.3, "Deleting a NetFlow Interface"

Section 15.4.7.1

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 Section 15.4.7.2, "Adding a NetFlow Interface".

Section 15.4.7.2

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 direction
   ```

   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, or type **`revert`** and press **Enter** to abort.

Section 15.4.7.3
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, or type **`revert`** and press **Enter** to abort.

Section 15.4.8
Managing NetFlow Collectors

RUGGEDCOM ROX II can be configured to forward flows to up to four NetFlow collectors.

CONTENTS

- Section 15.4.8.1, "Viewing a List of NetFlow Collectors"
- Section 15.4.8.2, "Adding a NetFlow Collector"
- Section 15.4.8.3, "Enabling/Disabling a NetFlow Collector"
- Section 15.4.8.4, "Deleting a NetFlow Collector"

Section 15.4.8.1
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 Section 15.4.8.2, "Adding a NetFlow Collector".

Section 15.4.8.2
Adding a NetFlow Collector

To define a NetFlow collector to which RUGGEDCOM ROX II will send flows, do the following:

1. 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 Section 15.4.8.3, "Enabling/Disabling a NetFlow Collector".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 15.4.8.3
Enabling/Disabling a NetFlow Collector

To enable or disable a NetFlow collector defined in RUGGEDCOM ROX II, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 15.4.8.4
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, or type **revert** and press **Enter** to abort.

Section 15.4.9
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:** A 32-bit unsigned integer The current rate in bits/s.
pkts-sec	**Synopsis:** A 32-bit unsigned integer The current rate in packets/s.
bits-sec-min	**Synopsis:** A 32-bit unsigned integer The average rate in bits/s over a minute.
pkts-sec-min	**Synopsis:** A 32-bit unsigned integer The average rate in packets/s over a minute.

Section 15.4.10
Example: Exporting Flows to Multiple Collectors

This example describes how to configure RUGGEDCOM ROX II to forward NetFlow data to two NetFlow collectors.

In the following topology, the NetFlow exporter (RUGGEDCOM ROX II) is collecting data on packets traversing two interfaces. Packets sharing the same characteristics (i.e. source, destination, port, etc.) are placed into flows.

When each flow is either deemed inactive, has exceeded the active timer, or is flagged as terminated, the exporter forwards the flow to the specified collectors.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

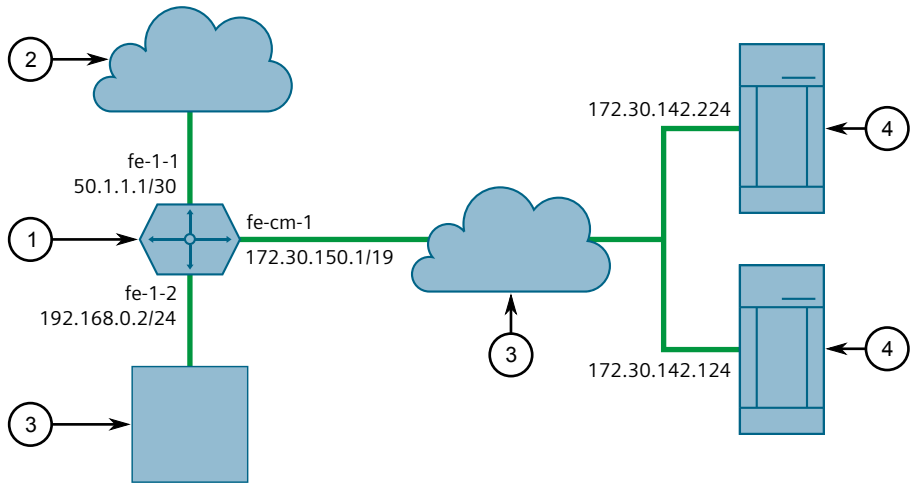


Figure 46: Topology – Exporting Data to Multiple Collectors

1. NetFlow Exporter (RUGGEDCOM ROX II) **2.** WAN **3.** LAN **4.** NetFlow Collector

Configuration

To configure RUGGEDCOM ROX II to export NetFlow packets to two NetFlow collectors, do the following:

1. Enable NetFlow. For more information, refer to Section 15.4.3, "Enabling/Disabling NetFlow".
2. Define two NetFlow collectors and make sure they are both enabled. For more information, refer to Section 15.4.8.2, "Adding a NetFlow Collector".
3. Define the interface that will be monitored by NetFlow. For more information, refer to Section 15.4.7.2, "Adding a NetFlow Interface".
4. Send traffic to the interface monitored by RUGGEDCOM ROX II.
5. 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
  !
 !
!
```

Section 15.5
Managing Port Rate Limiting

This section describes how to manage port rate limiting.

CONTENTS

- Section 15.5.1, “Understanding Port Rate Limiting”
- Section 15.5.2, “Configuring Port Rate Limiting”

Section 15.5.1
Understanding Port Rate Limiting

Rate limiting restricts the bandwidth for a specific interface. The restriction can be applied to ingress and/or egress traffic, and to a specific type of traffic (e.g. unicast, multicast, broadcast, etc.). In some applications, controlling bandwidth may be required to maintain quality of service.

Rate limiting also provides a layer of defense against Denial of Service (DoS) and Distributed Denial of Service (DDos) attacks. These attacks exhaust network resources by flooding a device with requests.

Section 15.5.2
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 » swport » {port}***, where *{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:** { disabled } or a 32-bit signed integer between 62 and 256000 **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. 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.

Parameter	Description
	• 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 a 32-bit signed 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, or type **`revert`** and press **Enter** to abort.

16 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

CONTENTS

- Section 16.1, "Configuring the Time Synchronization Settings"
- Section 16.2, "Configuring the System Time and Date"
- Section 16.3, "Configuring the System Time Zone"
- Section 16.4, "Configuring the Local Time Settings"
- Section 16.5, "Enabling and Configuring the NTP Service"
- Section 16.6, "Viewing the NTP Service Status"
- Section 16.7, "Viewing the Status of Reference Clocks"
- Section 16.8, "Managing NTP Servers"
- Section 16.9, "Managing NTP Broadcast/Multicast Clients"

Section 16.1

Configuring the Time Synchronization Settings

To configure the time synchronization settings, do the following:

1. Configure the system time and date. For more information, refer to Section 16.2, "Configuring the System Time and Date".
2. Configure the system time zone. For more information, refer to Section 16.3, "Configuring the System Time Zone".
3. Configure the local time settings. For more information, refer to Section 16.4, "Configuring the Local Time Settings".
4. If multicast addresses will be configured for the NTP server, enable and configure the NTP multicast client. For more information, refer to Section 16.9.1, "Enabling and Configuring NTP Multicast Clients".
5. If broadcast addresses will be configured for the NTP server, enable and configure the NTP broadcast client. For more information, refer to Section 16.9.2, "Enabling and Configuring NTP Broadcast Clients".
6. Add remote NTP servers. For more information, refer to Section 16.8.3, "Adding an NTP Server".
7. Add broadcast/mutlicast addresses for the NTP server. For more information, refer to Section 16.9.3.2, "Adding a Broadcast/Multicast Address".
8. If required, add server authentication keys. For more information, refer to Section 16.8.5.2, "Adding a Server Key".

9. Add restrictions for the remote NTP servers. For more information, refer to Section 16.8.6.2, "Adding a Server Restriction".
10. Enable and configure the NTP service. For more information, refer to Section 16.5, "Enabling and Configuring the NTP Service".
11. View the status of the NTP service. For more information, refer to Section 16.6, "Viewing the NTP Service Status".

Section 16.2
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, or type **revert** and press **Enter** to abort.

Section 16.3
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, or type **revert** and press **Enter** to abort.

Section 16.4
Configuring the Local Time Settings

The local time settings configure the local clock on the device as the NTP time source.

To configure the local NTP time settings, do the following:

1. 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, or type **revert** and press **Enter** to abort.

Section 16.5
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.

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** false Enables NTP service.
bind-interface { bind-interface }	**Synopsis:** A string Sets the 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.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 16.6
Viewing the NTP Service Status

To view the status of the NTP service, do the following:

1. Make sure the NTP service is enabled. For more information, refer to Section 16.5, "Enabling and Configuring the NTP Service".
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
```

This table provides the following information:

Parameter	Description
remote	**Synopsis:** A string 1 to 40 characters long Remote address.
reference-id	**Synopsis:** A string 1 to 40 characters long The identification of the reference clock.
stratum	**Synopsis:** A string 1 to 32 characters long The stratum number of the reference clock.
address-type	**Synopsis:** A string 1 to 32 characters long The address type of the remote machine.
when	**Synopsis:** A string 1 to 32 characters long The number of seconds since the last poll of the reference clock.
poll	**Synopsis:** A string 1 to 32 characters long The polling interval in seconds.
reach	**Synopsis:** A string 1 to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
delay	**Synopsis:** A string 1 to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
offset	**Synopsis:** A string 1 to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
jitter	**Synopsis:** A string 1 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.

Tally Code	Description
o	This tally code indicates the peer is the system peer, but the synchronization distance is derived from a Pulse-Per-Second (PPS) signal.

Section 16.7
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       l        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
```

This table provides the following information:

Parameter	Description
address	**Synopsis:** A string 1 to 40 characters long The IP address of the reference clock.
state	**Synopsis:** A string 1 to 32 characters long The state of the clock.
reference-id	**Synopsis:** A string 1 to 40 characters long The identification of the reference clock.
stratum	**Synopsis:** A string 1 to 32 characters long The stratum number of the reference clock.
address-type	**Synopsis:** A string 1 to 32 characters long The address type of the remote machine.
when	**Synopsis:** A string 1 to 32 characters long The number of seconds since the last poll of the reference clock.
poll	**Synopsis:** A string 1 to 32 characters long The polling interval in seconds.
reach	**Synopsis:** A string 1 to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
delay	**Synopsis:** A string 1 to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
offset	**Synopsis:** A string 1 to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
jitter	**Synopsis:** A string 1 to 32 characters long

Parameter	Description
	The observed jitter (in milliseconds).

Section 16.8
Managing NTP Servers

RUGGEDCOM ROX II can periodically refer to a remote NTP server to correct any accumulated drift in the onboard clock. RUGGEDCOM ROX II can also serve time via SNTP (Simple Network Time Protocol) to hosts that request it.

NTP servers can be added with or without authentication keys. To associate an authentication key with an NTP server, first define a server key. For information about adding server keys, refer to Section 16.8.5.2, "Adding a Server Key".

CONTENTS

- Section 16.8.1, "Viewing a List of NTP Servers"
- Section 16.8.2, "Monitoring Subscribers"
- Section 16.8.3, "Adding an NTP Server"
- Section 16.8.4, "Deleting an NTP Server"
- Section 16.8.5, "Managing Server Keys"
- Section 16.8.6, "Managing Server Restrictions"

Section 16.8.1
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 Section 16.8.3, "Adding an NTP Server".

Section 16.8.2
Monitoring Subscribers

RUGGEDCOM ROX II monitors the subscriptions of up to 600 hosts (e.g. clients, servers and peers) that are connected to the NTP server.

To view the list of subscriber hosts, 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 1 to 40 characters long Remote address.
port	**Synopsis:** A 16-bit signed integer UDP port number.
count	**Synopsis:** A 32-bit signed integer Number of packets received.
mode	**Synopsis:** An 8-bit signed integer Mode of last packet.
version	**Synopsis:** An 8-bit signed integer Version of last packet.
restrict	**Synopsis:** { ignore, kod, limited, lowpriotrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version } Restrict flags.
average-interval	**Synopsis:** A 32-bit signed integer Average interval (in seconds) between packets from this address.
last-interval	**Synopsis:** A 32-bit signed integer Interval (in seconds) between the receipt of the most recent packet from this address and the completion of the retrieval of the status.

Section 16.8.3
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 Section 16.8.5, "Managing Server Keys".
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.
minpoll { minpoll }	**Synopsis:** An 8-bit unsigned 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 8-bit unsigned 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:** A 32-bit signed 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:** A string 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 Section 16.8.6.2, "Adding a Server Restriction".
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 16.8.4
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, or type **revert** and press **Enter** to abort.

Section 16.8.5
Managing Server Keys

Server keys are used to authenticate NTP communications and prevent tampering with NTP timestamps. When using authentication, both the local and remote servers must share the same key and key identifier. Packets sent to and received from the server/peer include authentication fields encrypted using the key.

CONTENTS

- Section 16.8.5.1, "Viewing a List of Server Keys"
- Section 16.8.5.2, "Adding a Server Key"
- Section 16.8.5.3, "Deleting a Server Key"

Section 16.8.5.1
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 Section 16.8.5.2, "Adding a Server Key".

Section 16.8.5.2
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 1 to 1024 characters long The key. This parameter is mandatory.
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, or type **revert** and press **Enter** to abort.

Section 16.8.5.3
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, or type **revert** and press **Enter** to abort.

Section 16.8.6
Managing Server Restrictions

Server restrictions control access to the NTP servers.

CONTENTS

- Section 16.8.6.1, “Viewing a List of Server Restrictions”
- Section 16.8.6.2, “Adding a Server Restriction”
- Section 16.8.6.3, “Deleting a Server Restriction”

Section 16.8.6.1
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 Section 16.8.6.2, "Adding a Server Restriction".

Section 16.8.6.2
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:

   CAUTION!
   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.

Parameter	Description
	• 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, or type **`revert`** and press **Enter** to abort.

Section 16.8.6.3
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, or type **`revert`** and press **Enter** to abort.

Section 16.9
Managing NTP Broadcast/Multicast Clients

Set the device to NTP broadcast or multicast client mode if the NTP server issues regular time-of-day advertisements.

CONTENTS

- Section 16.9.1, “Enabling and Configuring NTP Multicast Clients”
- Section 16.9.2, “Enabling and Configuring NTP Broadcast Clients”
- Section 16.9.3, “Managing NTP Broadcast/Multicast Addresses”

Section 16.9.1
Enabling and Configuring NTP Multicast Clients

The NTP multicast client enables the NTP server to receive advertisements from other NTP servers.

To enable and configure the NTP multicast client, do the following:

1. 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 1 to 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 Section 16.9.3.2, "Adding a Broadcast/Multicast Address".
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 16.9.2
Enabling and Configuring NTP Broadcast Clients

The NTP broadcast client enables the NTP server to receive advertisements from other NTP servers and send advertisements of its own.

To enable and configure the NTP broadcast client, do the following:

1. 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 Section 16.9.3.2, "Adding a Broadcast/Multicast Address".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 16.9.3
Managing NTP Broadcast/Multicast Addresses

When broadcast or multicast addresses for known NTP servers are configured, the NTP daemon monitors advertisements from each address and chooses the server with the lowest stratum to use as the NTP host. This is opposed to manually configuring a list of servers or peers.

CONTENTS

- Section 16.9.3.1, "Viewing a List of Broadcast/Multicast Addresses"

- Section 16.9.3.2, "Adding a Broadcast/Multicast Address"
- Section 16.9.3.3, "Deleting a Broadcast/Multicast Address"

Section 16.9.3.1
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 Section 16.9.3.2, "Adding a Broadcast/Multicast Address".

Section 16.9.3.2
Adding a Broadcast/Multicast Address

To add a broadcast/multicast address for an NTP server, do the following:

IMPORTANT!
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 Section 16.8.5.2, "Adding a Server Key".
2. Make sure the CLI is in Configuration mode.
3. Add the address by typing:

   IMPORTANT!
   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.

Parameter	Description
key { key }	**Synopsis:** A string Authentication key.
ntp-version { ntp-version }	**Synopsis:** A 32-bit signed 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 8-bit unsigned integer between 1 and 127 **Default:** 1 Time to live.

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 16.9.3.3
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, or type **revert** and press **Enter** to abort.

Virtualization

RUGGEDCOM ROX II supports kernel-based virtualization systems on the RUGGEDCOM RX1400.

The Virtual Processing Engine (VPE) provides a Linux-based platform for third-party applications to use, without impacting RUGGEDCOM RX1400 core services running on the system. Virtualization allows a full Linux image (with dedicated storage media and I/O ports) to run in parallel with the RUGGEDCOM ROX II, using a KVM (Kernel Virtual Machine) based solution.

A front-end management interface is added for the deployment and configuration of virtual machines.
Once installed and configured, users can launch a Linux-based guest operating system and install third party applications on top of the image. Third-party applications will have access to network and serial interfaces on the system, based on the configuration.

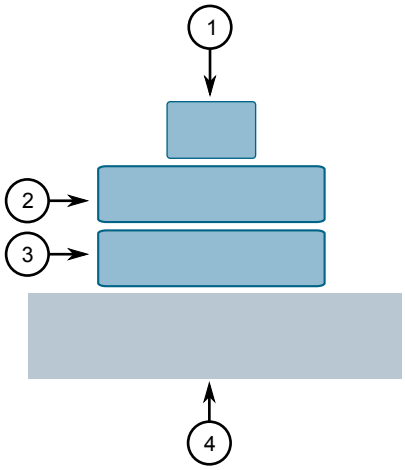


Figure 47: System Block Diagram

1. Apps **2.** Guest Linux Kernel **3.** QEMU **4.** ROXII Linux Kernel ARM

IMPORTANT!
A separate VPE feature key (VIRTUALM) must be installed before enabling the virtualization service. For more information about obtaining this feature key, contact a Siemens Sales representative or Customer Support.

IMPORTANT!
Virtual machine images must be run from the microSD/microSDHC drive. For more information, refer to *Section 1.1, "Features and Benefits"*.

NOTE
Multiple virtual machines can be installed, but only one virtual machine can be run at a time.

To aid in the deployment of large virtual machine images, setup of the VPE requires the Linux OS and applications to be compressed in a tar archive. This file is transferred to a microSD card, which is then installed in the RUGGEDCOM RX1400. The RUGGEDCOM ROX II virtualization service will mount the microSD card, extract the image file, and use it as the file system for the Linux OS and applications.

CONTENTS

- Section 17.1, "Configuring Virtualization"
- Section 17.2, "Enabling/Disabling the Virtualization Service"
- Section 17.3, "Configuring Global Settings"
- Section 17.4, "Issuing VM Commands"
- Section 17.5, "Assigning a Network Interface"
- Section 17.6, "Accessing the Active Virtual Machine"
- Section 17.7, "Querying the Device Serial Number"
- Section 17.8, "Managing Virtual Machines"
- Section 17.9, "Managing Serial Port Assigments"
- Section 17.10, "Managing Virtual Interfaces"
- Section 17.11, "Managing VPE Adapters"
- Section 17.12, "Example: Enabling a Virtual Machine to Access a WLAN via a WLAN Client Interface"

Section 17.1

Configuring Virtualization

To configure a virtual machine on the RUGGEDCOM RX1400, perform the following basic steps:

1. Obtain and install the VPE feature key (VIRTUALM).
2. Enable the RUGGEDCOM ROX II virtualization service.
3. Configure the global settings for the virtualization service.
4. Add and extract the virtual machine image.
5. Configure the network interface.
6. Start the virtual machine image.

Once the virtual machine is started, it can be accessed for the first time via the virtual machine console using the **`vm-console`** command. Once logged in via console, standard Linux commands can be used to set up networking and other configuration parameters.

Section 17.2

Enabling/Disabling the Virtualization Service

To enable or disable the virtualization service, do the following:

NOTE
A pre-built virtual machine image for Debian Linux is available upon request from Siemens. For more information, refer to Siemens Customer Support.

1. Insert the microSD/microSDHC drive containing the virtual machine image into the microSD/microSDHC drive slot. For more information, refer to the *RUGGEDCOM RX1400 Installation Guide*.
2. Make sure the CLI is in Configuration mode.
3. Enable or disable the virtualization service by typing:

   ```
   services virtualization enabled [ true | false ]
   ```

   Where:

   - *true* enables the virtualization service
   - *false* disables the virtualization service
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.3
Configuring Global Settings

To configure the global settings, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the global settings by typing:

   ```
   services virtualization virtual-machines basic-parameters cpu cpu vpe-boot-partition parition
   machine machine memory memory auto-start auto-start
   ```

   Where:

   - *cpu* is the CPU type to emulate.
   - *partition* is the primary virtual disk partition that VPE will boot from. The value can be any number between 1 and 4. The default value is 1.
   - *machine* is the machine type to emulate.
   - *memory* is the memory allocation in MB. The allocation can be any value between 200 and 512 MB.
   - *auto-start* is the name of the virtual machine to start on system restart.
3. Assign one or more serial ports to the virtualization service. For more information, refer to Section 17.9.1, "Assigning a Serial Port".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.4
Issuing VM Commands

To issue a virtual machine command, do the following:

1. Issue a virtual machine command by typing:

   ```
   services virtualization vm-command cmd [ kill | quit | status | stop ]
   ```

Where:

- `kill` forcefully terminates the virtual machine process
- `quit` systematically terminates the process from the host
- `status` queries the status of the Quick Emulator
- `stop` pauses the virtual machine

2. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 17.5

Assigning a Network Interface

The network configuration is divided into two sections: the network interface configuration on the guest, and the back end interface on the host side. The available network interfaces on the guest are *eth0*, *eth1*, and *eth2*. Network interfaces are bridged to the external network via a Linux kernel virtual bridge.

To assign a network interface to the virtual machine, do the following:

1. Make sure the CLI is in Configuration mode.

   NOTE
   Any VLAN interface or dedicated port can be assigned to the virtual switch.

2. Add a virtual machine. For more information, refer to Section 17.8.4, "Adding a Virtual Machine".
3. Make sure the VPE Network Interface for the virtual machine is enabled. For more information, refer to Section 17.10.3, "Enabling/Disabling the VPE Network Interface".

   NOTE
   Up to three network interfaces can be added for each VPE.

4. Add one or more network interfaces. For more information, refer to Section 17.10.2, "Adding a Virtual Interface".
5. Configure a virtual switch for the virtualization service. For more information, refer to Section 11.1.2, "Adding a Virtual Switch".
6. Start the virtual machine. For more information, refer to Section 17.8.9, "Starting a Virtual Machine".
7. Access the virtual machine console window. For more information, refer to Section 17.6, "Accessing the Active Virtual Machine".
8. Log in to the virtual machine.
9. Navigate to ***etc » network » interfaces***.
10. Add an entry for the desired interface by typing an appropriate Linux command, such as:

    NOTE
    IP addresses can be assigned either manually or via DHCP. The following example uses DHCP.

```
allow-hotplug interface
iface interface inet dhcp
```

Where:

- *interface* is the interface to be used. Options include `eth0`, `eth1`, `eth2`.

11. Activate the network interface by typing:

```
ifup interface
```

Where:

- *interface* is the interface to be used. Options include `eth0`, `eth1`, `eth2`.

Section 17.6

Accessing the Active Virtual Machine

The CLI includes a built-in Command Line Interface (CLI) for accessing and interacting with the active virtual machine. To access the active virtual machine, type:

```
vm-console
```

The prompt for the virtual machine appears. For example:

```
ruggedcom# vm-console
Trying 127.0.0.1...
Connected to ruggedcom.localdomain.
Escape character is '^]'.

ruggedcom login:
```

Section 17.7

Querying the Device Serial Number

To query the serial number of the RUGGEDCOM RX1400 using SNMP, do the following:

1. Log in to the active virtual machine. For more information, refer to Section 17.6, "Accessing the Active Virtual Machine".
2. Make sure the SNMP utility is installed on the virtual machine. If it is not, install the utility by typing:

```
apt-get install snmp
```

> **IMPORTANT!**
> *The appropriate community string or password configured for the RUGGEDCOM RX1400 must be used.*

3. Query the OID of the serial number by typing:

```
snmpget -v version -c id -u user address 1.3.6.1.4.1.15004.4.2.3.1.0
```

Where:

- *version* is the SNMP version to be used. Options include `1`, `2c`, `3`
- *id* is the name of the community string configured for the device
- *user* is the name of the ROX user
- *address* is the IP address of the RUGGEDCOM ROX II device

The following is an example of a successful query output:

```
1.3.6.1.4.1.15004.4.2.3.1.0 = STRING: RUMED22080400
```

Section 17.8

Managing Virtual Machines

This section describes how to configure and manage virtual machines.

CONTENTS

- Section 17.8.1, "Building/Obtaining a Virtual Machine Image"
- Section 17.8.2, "Determining the Active Virtual Machine"
- Section 17.8.3, "Viewing a List of Virtual Machine Names"
- Section 17.8.4, "Adding a Virtual Machine"
- Section 17.8.5, "Extracting a Virtual Machine Archive"
- Section 17.8.6, "Loading an Existing Virtual Machine Image"
- Section 17.8.7, "Deleting a Virtual Machine"
- Section 17.8.8, "Deleting a Virtual Machine Archive"
- Section 17.8.9, "Starting a Virtual Machine"
- Section 17.8.10, "Stopping a Virtual Machine"

Section 17.8.1

Building/Obtaining a Virtual Machine Image

Detailed instructions for creating the Linux image .tar.gz file are described in the Building a Linux-Based Virtual Machine Image [https://support.industry.siemens.com/cs/ww/en/view/109482423].

Alternatively, Siemens has sample Debian Linux images available on request from the support portal, in both 1 GB and 3.5 GB file system sizes. Either of these images can be successfully extracted onto a FAT32 formatted SD card, allowing transfer via a Windows PC. If a larger image is created, and the extracted image size is > 4 GB, an EXT4 formatted card is required, and will require a Linux PC to format and transfer.

Section 17.8.2

Determining the Active Virtual Machine

To determine which virtual machine is active, type:

```
show services virtualization status
```

If a virtual machine has been activated, a list similar to the following example appears:

```
ruggedcom# show services virtualization status
status
 active-guest
  name   linux1
  pid    28579
```

```
  state  Started
  status Normal
```

NOTE
*The active virtual machine is referred to as the **active guest**.*

This list displays the following information:

Parameter	Description
name	**Synopsis:** A string 1 to 64 characters long The name of the active guest. This parameter is mandatory.
pid	**Synopsis:** A string The Process ID (PID) associated with the active guest.
state	**Synopsis:** A string The state of the active guest. Possible values include started, stopped, failed or no reply. This parameter is mandatory.
status	**Synopsis:** A string The status of the active guest. This parameter is mandatory.

Section 17.8.3
Viewing a List of Virtual Machine Names

To view a list of installed virtual machines, type:

```
show running-config services virtualization virtual-machines
```

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

```
ruggedcom# show running-config services virtualization virtual-machines linux-guests | tab
        LINUX                  LINUX
NAME    ARCHIVE       ARCHIVE  IMAGE      LINUX KERNEL               DEVICE TREE               INIT
 RAM DISK
-------------------------------------------------------------------------------------------------------
linux1  demo2.tar.gz  tar.gz   linux.img  vmlinuz-3.16.0-4-armmp.knl  vexpress-v2p-ca15-tc1.dtb
 initrd.img.ird

 !
!
```

If no virtual machines have been configured, add images as needed. For more information, refer to Section 17.8.4, “Adding a Virtual Machine”.

Section 17.8.4
Adding a Virtual Machine

Users can add a virtual machine to RUGGEDCOM ROX II using a micoSD card containing the virtual machine image.

IMPORTANT!
When preparing a virtual machine image, note the following requirements:

- *At least one user profile and password must be configured when building the virtual machine image. This is required to access the virtual machine via RUGGEDCOM ROX II. For more information about accessing the virtual machine once installed and activated, refer to Section 17.6, "Accessing the Active Virtual Machine".*
- *Each virtual machine image must be compressed into one of the following tar archive file formats: *.tar, *.tar.gz or *.tar.bz2*
- *Each virtual machine archive must consist of the following files: the initial RAM disk (initrd) file (if required by the image), a Linux image file (*.img), a Linux kernel file (*.knl), a device tree file (*.dtb) and a manifest file (*vmconfig.txt).*

To add a virtual machine, do the following:

1. Make sure the virtual machine image is installed on the device. For more information, refer to Section 4.11.1, "Installing Files".
2. Make sure the CLI is in Configuration mode.
3. Add the virtual machine by typing:

   ```
   services virtualization virtual-machines linux-guests name
   ```

   Where:

   - *name* is the name of the virtual machine to be added

   NOTE
   If an image with the same name already exists in the file system, the user will be prompted to either overwrite the image in the file system or load the existing image. For more information, refer to either Section 17.8.5, "Extracting a Virtual Machine Archive" or Section 17.8.6, "Loading an Existing Virtual Machine Image".
4. Type **commit** and press **Enter** to save the changes.

Section 17.8.5
Extracting a Virtual Machine Archive

NOTE
The extraction process can take several minutes to complete.

IMPORTANT!
Do not extract an archive for the active virtual machine.

To extract a virtual machine archive, do the following:

1. Make sure the CLI is in Configuration mode.
2. Determine which virtual machine is active. For more information, refer to Section 17.8.2, "Determining the Active Virtual Machine".
3. If the virtual machine is active, stop the machine. For more information, refer to Section 17.8.10, "Stopping a Virtual Machine".

4. Extract a virtual machine archive by typing:

```
services virtualization vm-extract-archive vm-name name archive-name archive
```

   Where:

   - *name* is the name of the virtual machine
   - *archive* is the name of the archive file to extract

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.8.6
Loading an Existing Virtual Machine Image

A user may load an existing virtual machine image from the file system.

To load an existing virtual machine image, do the following:

1. Make sure the CLI is in Configuration mode.
2. Load a virtual machine image by typing:

```
services virtualization vm-load-image vm-name name
```

   Where:

   - *name* is the name of the virtual machine

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.8.7
Deleting a Virtual Machine

To delete a virtual machine, do the following:

IMPORTANT!
Deleting a virtual machine removes the image from RUGGEDCOM ROX II and the microSD/microSDHC drive.

1. Make sure the CLI is in Configuration mode.
2. Determine which virtual machine is active. For more information, refer to Section 17.8.2, "Determining the Active Virtual Machine".
3. If the virtual machine is active, stop the machine. For more information, refer to Section 17.8.10, "Stopping a Virtual Machine".
4. Delete the virtual machine by typing:

```
no services virtualization virtual-machines linux-guests name
```

   Where:

   - *name* is the name of the virtual machine to be deleted

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.8.8
Deleting a Virtual Machine Archive

To delete a virtual machine archive, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete a virtual machine archive by typing:

   ```
   services virtualization vm-delete-archive archive-name name
   ```

   Where:

   - *name* is the name of the archive file to delete
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.8.9
Starting a Virtual Machine

To start a virtual machine, do the following:

1. Start a virtual machine by typing:

   ```
   services virtualization vm-start name console-wait [ true | false ]
   ```

   Where:

   - *name* is the name of the virtual machine
   - *console-wait* is an optional parameter. When set to true, the virtual machine waits for a console connection before starting. The default value is false.
2. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.8.10
Stopping a Virtual Machine

To stop a virtual machine, do the following:

1. Log in to the active virtual machine. For more information, refer to Section 17.6, “Accessing the Active Virtual Machine”.
2. Shut down the active virtual machine by typing an appropriate Linux command (e.g. *poweroff*).

Section 17.9
Managing Serial Port Assigments

This section describes how to assign serial ports to the virtual machine, as well as how to unassign them.

The serial ports are mapped within the virtual machine as follows:

- Port 1: /dev/ttyAMA1

- Port 2: /dev/ttyAMA2

CONTENTS

- Section 17.9.1, "Assigning a Serial Port"
- Section 17.9.2, "Unassigning a Serial Port"

Section 17.9.1

Assigning a Serial Port

To assign a serial port to the virtual machine service, do the following:

IMPORTANT!
When serial ports are assigned to the virtual machine service, they are dedicated to the service and cannot be used for any other purpose by RUGGEDCOM ROX II.

1. Make sure the CLI is in Configuration mode.
2. Define a protocol for the desired serial port. For more information, refer to Section 9.2.3, "Adding a Serial Port Protocol".
3. Assign a serial port, type:

   ```
   services virtualization virtual-machines basic-parameters serials serial-port
   ```

   Where:

   - *serial-port* the host serial interface port, redirected to the virtual machine
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.9.2

Unassigning a Serial Port

To unassign a serial port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Unassign the chosen serial port by typing:

   ```
   no services virtualization virtual-machines basic-parameters serials serial-port
   ```

   Where:

   - *serial-port* the host serial interface port, mapped to the ttyAMA device
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.10

Managing Virtual Interfaces

This section describes how to configure and manage virtual interfaces for the virtual machine.

CONTENTS

- Section 17.10.1, "Viewing a List of Virtual Interfaces"
- Section 17.10.2, "Adding a Virtual Interface"
- Section 17.10.3, "Enabling/Disabling the VPE Network Interface"
- Section 17.10.4, "Deleting a Virtual Interface"

Section 17.10.1

Viewing a List of Virtual Interfaces

To view a list of available virtual interfaces, type:

```
show running-config services virtualization virtual-machines basic-parameters network-interfaces
```

A table or list similar to the following appears:

```
ruggedcom# show running-config services virtualization virtual-machines basic-parameters network-
interfaces | tab
IFNAME
----------
vma.0001

 !
!
```

If a virtual interface is not listed, configure one. For more information, refer to Section 17.10.2, "Adding a Virtual Interface".

Section 17.10.2

Adding a Virtual Interface

Users can add up to three network interfaces to support the virtual processing engine.

To add a virtual interface, do the following:

1. Make sure the virtual machine image is installed on the device. For more information, refer to Section 4.11.1, "Installing Files".
2. Make sure the CLI is in Configuration mode.
3. Add the virtual interface by typing:

   ```
   services virtualization virtual-machines basic-parameters network-interfaces name
   ```

   Where:

   - *name* is the name of the interface to be added. Options include vma.0001, vma.0002, vma.0003.
4. Type **commit** and press **Enter** to save the changes.

Section 17.10.3
Enabling/Disabling the VPE Network Interface

The VPE Network Interface must be enabled to allow network access for virtual machines.

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the VPE Network Interface by typing the following commands:

   Enable

   ```
   interface VPE name enabled
   ```

   Where:

   - *name* is the name of the emulated network interface

   Disable

   ```
   no interface VPE name enabled
   ```

   Where:

   - *name* is the name of the emulated network interface
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.10.4
Deleting a Virtual Interface

To delete a virtual interface, do the following:

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

   ```
   no services virtualization virtual-machines basic-parameters network-parameters name
   ```

   Where:

   - *name* is the name of the interface to be deleted
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 17.11
Managing VPE Adapters

This section describes how to configure and manage VPE adaptors within the virtual machine image from the RUGGEDCOM ROX II CLI.

CONTENTS

- Section 17.11.1, “Viewing the Status of the VPE Adapter”
- Section 17.11.2, “Configuring a VPE Adapter”
- Section 17.11.3, “Starting/Stopping a VPE Adapter”

Section 17.11.1
Viewing the Status of the VPE Adapter

To view the current status and configuration settings of a VPE adapter, do the following:

1. Exit all vm-console sessions via the CLI.
2. View the stats of the VPE adapter by typing:

```
services virtualization vm-network-query adaptor> [ eth0 | eth1 | eth2 ] user username password
password
```

Where:

- *username* is the username required to access the VPE adapter.
- *password* is the password associated with the VPE username.

A table or list similar to the following appears:

NOTE
A blank field indicates the associated parameter is not configured.

```
ruggedcom# services virtualization vm-networking-query adaptor eth0 password admin user root
 vm-adaptor-status   UP
 vm-ipv4-source   static
 vm-ipv4-address   172.30.143.173/19    172.30.142.173/19
 vm-ipv4-gateway   172.30.128.1
 vm-ipv6-source
 vm-ipv6-address   fe80::96b8:c5ff:fe24:849b/64
 vm-ipv6-gateway
 vm-dns-nameservers   172.30.128.8    172.30.128.12
```

Section 17.11.2
Configuring a VPE Adapter

To configure a VPE adapter in the virtual machine image, do the following:

1. [Optional] Review the current configuraton of the VPE adapter. For more information, refer to Section 17.11.1, “Viewing the Status of the VPE Adapter”.
2. Exit all vm-console sessions.
3. Enter **services** virtualization vm-networking-state and then define the following settings:

Parameter	Description
adaptor { adaptor }	**Synopsis:** { eth0, eth1, eth2 } The interface used by the VPE adapter. This parameter is mandatory.
ipv4-src { ipv4-src }	**Synopsis:** { none, static, dhcp } The source of the virtual machine's IPv4 address. Options include • none - The source is not configured • static - The IP address is static • dhcp - The IP address is obtained from a DHCP server This parameter is mandatory.

Parameter	Description
ipv4 { ipv4 }	**Synopsis:** A string 9 to 18 characters long or a string 0 characters long The virtual machine's IPv4 address, including the subnet (i.e. 172.30.10.12/19).
ipv4-gateway { ipv4-gateway }	**Synopsis:** A string 7 to 15 characters long or a string 0 characters long The virtual machine's IPv4 gateway.
ipv6-src { ipv6-src }	**Synopsis:** { none, static, auto } The source of the virtual machine's IPv6 address. Options include: • none - The source is not configured • static - The IP address is static • auto - The source is selected automatically by the virtual machine This parameter is mandatory.
ipv6 { ipv6 }	**Synopsis:** A string 4 to 43 characters long or a string 0 characters long The virtual machine's IPv6 address, including the subnet (i.e. fe80::96b8:c5ff:fe24:849b/64
ipv6-gateway { ipv6-gateway }	**Synopsis:** A string 6 to 40 characters long or a string 0 characters long The virtual machine's IPv6 gateway
dns-nameserver-1 { dns-nameserver-1 }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long or a string 0 characters long The IP address of the primary DNS server.
dns-nameserver-2 { dns-nameserver-2 }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long or a string 0 characters long The IP address of the secondary DNS server
user { user }	**Synopsis:** A string 1 to 128 characters long **Default:** root The name of the VPE user.
password { password }	**Synopsis:** A string 1 to 128 characters long **Default:** admin The password associated with the VPE user.

4. Press **Enter**.
5. To verify the configuration, query the VPE adapter to view its current settings. For more information, refer to Section 17.11.1, "Viewing the Status of the VPE Adapter".

Section 17.11.3
Starting/Stopping a VPE Adapter

To stop or start a VPE adapter, do the following:

1. Exit all vm-console sessions.
2. Start or stop the VPE adapter by typing:

```
services virtualization vm-networking-state adaptor> [ eth0 | eth1 | eth2 ] state [ start | stop ]
user username password password
```

Where:

- *username* is the username required to access the VPE adapter.

- *password* is the password associated with the VPE username.

Section 17.12

Example: Enabling a Virtual Machine to Access a WLAN via a WLAN Client Interface

This example demonstrates how to enable a virtual machine to access a TCP/IP WLAN. This is necessary if a virtual machine hosts an application that either requires access to the Internet or is a resource that other hosts on the network can access.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

The following topology consists of two networks:

- The first network (`192.168.1.0/24`) connects a VPE's *eth* interface to a router's (R1) virtual machine interface (vma.0001).
- The second network (`192.168.2.0/24`) is a WLAN that connects a router's (R2) *wlan-cl1* interface to a wireless access point (R2) and Linux host.

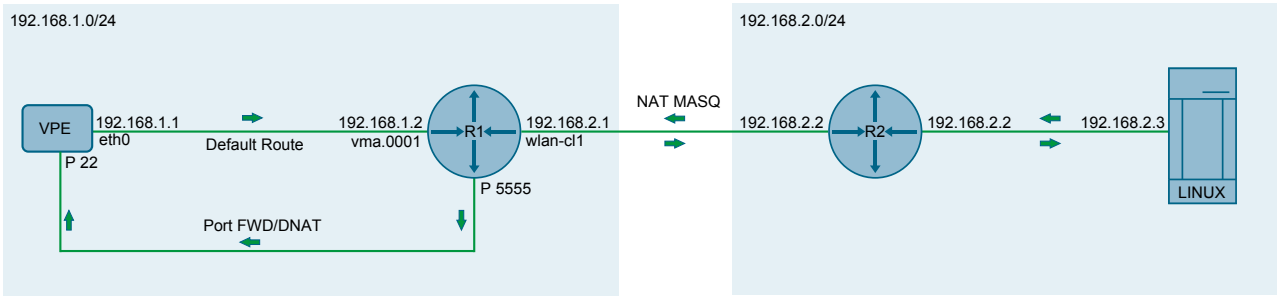


Figure 48: Virtual Machine to WLAN Topology

The following components exist in this topology:

- The **VPE** is a Linux guest that uses an ETH interface to access a host. In this scenario, the host is *R1*.
- **R1** is a RUGGEDCOM RX1400 running a virtual machine interface (vma.0001).
- **R2** is a RUGGEDCOM RX1400 acting as an access point.

In the topology, the default route forwards packets from the *eth* interface. This allows packets from the VPE to be sent to the *vma.0001* interface, where they can enter the RUGGEDCOM RX1400 routing system. Once in the routing system, any packets destined for the WLAN are forwarded to the *wlan-cl1* interface.

The masquerading NAT on *wlan-cl1* allows the VPE to initiate communications with a host on the WLAN and to receive replies from this host without requiring the WLAN to have a route to the VPE. The NAT does this by performing the following operations on packets passing through *wlan-cl1*:

- For packets egressing from the VPE (192.168.1.1), the masquerading NAT replaces the source IP address with the address of wlan-cl1 (192.168.2.1).
- For reply packets from the WLAN and destined to address 192.168.2.1, the masquerading NAT replaces the destination address with the IP address of the VPE (192.168.1.1). The packet is then forwarded to the VPE.

To enable hosts on the WLAN to communicate with the VPE, a Destination Network Address Translation (DNAT)/ port forward is configured on the firewall to map port 5555 on *wlan-cl1* (192.168.2.1:5555) to port 22 on the VPE's *eth* interface (192.168.1.1:22). Port forwarding/DNAT allows hosts on the WLAN to initiate communications with the VPE without requiring the WLAN to have an access route. In this scenario, the DNAT/port forward configuration enables WLAN hosts to start an SSH session with the VPE.

To replicate the topology, do the following:

Step 1: Configuring the Access Point (R2)

1. Enable the WLAN interface.
2. Set the SSID to **`RX1400-WLAN`**.
3. Assign the IP address `192.168.2.2/24` to the access point's interface. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

Step 2: Configuring the Linux Host

1. Connect the PC running the Linux host to the access point.
2. Assign the IP address `192.168.2.3/24` to the PC.

Step 3: Configuring the RUGGEDCOM RX1400 (R1)

1. Enable the WLAN interface.
2. Enable the virtualization service. For more information, refer to Section 17.2, "Enabling/Disabling the Virtualization Service".
3. Add a virtual machine and name it *vm1*. For more information, refer to Section 17.8.4, "Adding a Virtual Machine".
4. Select *vma.0001* as the virtual interface. For more information, refer to Section 17.10.2, "Adding a Virtual Interface".
5. Set the virtual machine to start automatically to make sure the source interface for the NAT masquerade (vma.001) is enabled before the firewall rules are applied. For more information, refer to Section 17.3, "Configuring Global Settings".
6. Start the virtual machine. For more information, refer to Section 17.8.9, "Starting a Virtual Machine".
7. Assign the IP address `192.168.1.2` to the virtual machine (vma.0001). For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".
8. Access the virtual machine via the virtual console using the following command:

   ```
   telnet localhost 4444
   ```

   For more information, refer to Section 17.6, "Accessing the Active Virtual Machine".
9. Enter the following command to bring up eth0:

   ```
   ip link set eth0 up # set eth0 up
   ```

10. Enter the following to assign the IP address `192.168.1.1/24` to eth0:

```
ip addr add 192.168.1.1/24 dev eth0
```

11. Enter the following to set a default route through vma.0001:

```
ip route add default via 192.168.1.2
```

12. Exit the virtual console.

Step 4: Configuring the WLAN Client

1. Add a WLAN client, making sure to select the access point. The IP address source must also be set to `static`. For more information, refer to Section 10.1.3.3, "Adding a WLAN Client".
2. Assign the IP address `192.168.2.1/24` to the WLAN client. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

Step 5: Configuring the Firewall

1. Create a firewall configuration named *wlan-vpe*.
2. Add the following zones:
   - *wlan*
   - *fw*
   - *vpe*

   For information about adding a zone, refer to Section 6.8.9.2, "Adding a Zone".
3. Add an interface named *wlan-cl1* and select `wlan` as the predefined zone. For more information, refer to Section 6.8.10.2, "Adding an Interface" and Section 6.8.10.3, "Associating an Interface with a Zone".
4. Add an interface named *vma.0001* and select `vpe` as the predefined zone. For more information, refer to Section 6.8.10.2, "Adding an Interface" and Section 6.8.10.3, "Associating an Interface with a Zone".
5. Add a policy named *allow* and configure it as follows:

Policy	Accept
Source Zone	All
Destination Zone	All

   This policy disables the firewall's packet filtering capabilities by allow the firewall to accept all packets from any interface.

   For more information, refer to:
   - Section 6.8.12.2, "Adding a Policy"
   - Section 6.8.12.3, "Configuring the Source Zone"
   - Section 6.8.12.4, "Configuring the Destination Zone"
6. Add a rule named *dnat* and configure it as follows:

Action	dnat
Destination Zone Hosts	192.168.1.1:22
Protocol	tcp

Destination Port	5555
Source Zone	wlan
Destination Zone	vpe

This rule forwards any TCP packets arriving on *wlan-cl1* with source IP address `192.168.2.1:5555` to `192.168.1.1:22` via *vma.0001*. This allows hosts on the WLAN to SSH to the Linux guest.

NOTE
To provide access to other services hosted by the Linux guest, add other DNAT rules with a destination port and protocol to match the service.

For more information, refer to:

- Section 6.8.15.2, "Adding a Rule"
- Section 6.8.15.3, "Configuring the Source Zone"
- Section 6.8.15.4, "Configuring the Destination Zone"

7. Add a masquerade rule named *masq* and configure it as follows:

Outgoing Interface List	wlan-cli
Source Hosts	vma.0001

This rule replaces the source address of any packet forwarded via *wlan-cl1* with the IP address of *wlan-cl1* and replaces the destination address of reply packets with the IP address of *vma.0001*. This rule allows the WLAN to send reply packets to the Linux guest without a gateway.

For more information, refer to Section 6.8.14.2, "Adding Masquerade or SNAT Settings".

8. Set *wlan-vpe* as the working configuration and validate the settings. For more information, refer to Section 6.8.16, "Validating a Firewall Configuration".
9. Set *wlan-vpe* as the active configuration. For more information, refer to Section 6.8.5, "Working with Multiple Firewall Configurations".
10. Enable the active firewall configuration. For more information, refer to Section 6.8.17, "Enabling/Disabling a Firewall".

» Step 4: Verifying the Configuration

1. To test the NAT, make sure the VPE can ping `192.168.2.3` (the Linux host).
2. To test the DNAT, make sure the Linux host can ssh into the VPE via R1 by typing the following:

```
ssh -p5555 192.168.2.1
```

» Final Configuration Example

Access Point Configuration

```
ruggedcom# show running-config interface wlan wlanport 1 access-point
interface
 wlan wlanport 1
  access-point ssids RX1400-WLAN
   enabled
   interface  wlan-ap1
   channel    6
   passphrase $4$wIw1bIIIw2BwhYYI0d4IDw==
```

```
  !
 !
!
```

Virtual Machine (VM) Configuration

```
ruggedcom# show running-config services virtualization
services
 virtualization
  enabled true
  virtual-machines basic-parameters auto-start vm1
  virtual-machines basic-parameters network-interfaces vma.0001
  !
  virtual-machines linux-guests vm1
   linux-image   linux.img
   linux-kernel  vmlinuz-3.16.0-4-armmp.knl
   device-tree   vexpress-v2p-ca15-tc1.dtb
   init-ram-disk initrd.img-3.16.0-4-armmp.ird
  !
 !
!
```

WLAN Client Configuration

```
Interface
 wlan wlanport 1
  client wireless-lans rx1400-wlan
   enabled
   ssid-security    RX1400-WLAN--WPA2
   password         $4$wIw1bIIIw2BwhYYI0d4IDw==
   ip-address-src   static
   ipv6-address-src static
  !
 !
!
```

Firewall Configuration

```
Security
 firewall
  enable
  work-config   wlan-vpe
  active-config wlan-vpe
  fwconfig wlan-vpe
   fwzone wlan
    no description
   !
   fwzone fw
    type firewall
    no description
   !
   fwzone vpe
    no description
   !
   fwinterface wlan-cl1
    zone wlan
    no description
   !
   fwinterface vma.0001
    zone vpe
    no description
   !
   fwpolicy allow
    source-zone all
    destination-zone all
    policy accept
```

```
    no description
   !
   fwrule dnat
    action                dnat
    source-zone wlan
    destination-zone vpe
    destination-zone-hosts 192.168.1.1:22
    protocol              tcp
    destination-ports     5555
    no description
   !
   fwmasq masq
    out-interface wlan-cl1
    no out-interface-specifics
    no ipalias
    source-hosts  vma.0001
    no address
    no description
   !
  !
 !
!
```

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 setting up an upgrade server, refer to Section 4.15.2, "Setting Up an Upgrade Server".

CONTENTS

- Section 18.1, "Viewing a List of Installed Applications"
- Section 18.2, "Installing an Application"
- Section 18.3, "Upgrading an Application"
- Section 18.4, "Uninstalling an Application"
- Section 18.5, "Managing Application Repositories"
- Section 18.6, "Managing the RUGGEDCOM CROSSBOW Application"

Section 18.1

Viewing a List of Installed Applications

To view a list of RUGGEDCOM ROX II applications installed on the device, type:

```
show admin software-upgrade apps installed-apps
```

If applications have been installed, a table or list similar to the following example appears:

```
ruggedcom# show admin software-upgrade apps installed-apps
APP NAME  VERSION
------------------
crossbow  4.1.2
elan      8.0.2
```

If no applications have been installed, install applications as needed. For more information, refer to Section 18.2, "Installing an Application".

Section 18.2

Installing an Application

To install an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a repository for the application has been configured before installing the application. For more information, refer to Section 18.5.3, "Adding a Repository".
3. Install the application by typing:

   ```
   admin software-upgrade apps install-app app-name name
   ```

   Where:

   - *name* is the name of the application to install as it appears in the repository configuration. To install more than one application, use a comma separated list.

Section 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 software-upgrade apps upgrade-app app-name name
   ```

   Where:

   - *name* is the name of the application to upgrade as it appears in the repository configuration. To upgrade more than one application, use a comma separated list.

Section 18.4
Uninstalling an Application

To uninstall an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Install the application by typing:

   ```
   admin software-upgrade apps uninstall-app app-name name
   ```

   Where:

   - *name* is the name of the application to uninstall as it appears in the repository configuration. To uninstall more than one application, use a comma separated list.

Section 18.5
Managing Application Repositories

Before any RUGGEDCOM ROX II application can be installed or upgraded, a connection to its repository on the upgrade server must be configured.

CONTENTS

- Section 18.5.1, "Viewing a List of Repositories"
- Section 18.5.2, "Checking the Repository Connection"
- Section 18.5.3, "Adding a Repository"
- Section 18.5.4, "Deleting a Repository"

Section 18.5.1
Viewing a List of Repositories

To view a list of RUGGEDCOM ROX II application repositories, type:

```
show running-config admin software-upgrade apps repository
```

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

```
ruggedcom# show running-config admin software-upgrade apps repository | tab
APP NAME  URL                                              VERSION
-----------------------------------------------------------------
crossbow  http://10.200.20.231/crossbow-repo/debianppc  rs2

 !
!
```

If no repositories have been configured, add repositories as needed. For more information, refer to Section 18.5.3, "Adding a Repository".

Section 18.5.2
Checking the Repository Connection

To check the connection with a repository, type:

```
admin software-upgrade apps check-repository-connection app-name name
```

Where:

- *name* is the name of the repository as it appears in the repository configuration. To check the connection with more than one repository, use a comma separated list.

The connection results are displayed.

Section 18.5.3
Adding a Repository

To add an application repository, do the following:

NOTE
An application repository must be configured before an application can be installed or upgraded.

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

```
admin software-upgrade apps repository app-name name
```

Where:

- *name* is the name of the repository as it appears in the application configuration. Consult the release notes for the appplication.

3. Configure the following parameter(s) as required:

Parameter	Description
url { url }	**Synopsis:** A string 1 to 1024 characters long The URL of the upgrade server hosting the app repository (http, https, and ftp are supported).
version { version }	**Synopsis:** A string 1 to 64 characters long The version of the app you are installing or upgrading.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 18.5.4
Deleting a Repository

To delete an application repository, do the following:

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

```
no admin software-upgrade apps repository app-name name
```

Where:

- *name* is the name of the repository as it appears in the application configuration. Consult the release notes for the application.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 18.6

Managing the RUGGEDCOM CROSSBOW Application

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.

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.

CONTENTS

- Section 18.6.1, "Enabling/Disabling CROSSBOW"
- Section 18.6.2, "Configuring the Client Connection"
- Section 18.6.3, "Configuring CROSSBOW Certificates and Private Keys"
- Section 18.6.4, "Managing SAC Connections"
- Section 18.6.5, "Managing CROSSBOW CA Certificate Lists"
- Section 18.6.6, "Viewing the Status of RUGGEDCOM CROSSBOW"
- Section 18.6.7, "Viewing the RUGGEDCOM CROSSBOW Log"

Section 18.6.1

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, or type **revert** and press **Enter** to abort.

Section 18.6.2
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*** and configure the following parameter(s):

Parameter	Description
ipaddr { ipaddr }	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address to which a client will connect to the Station Access Controller (SAC).
port { port }	**Synopsis:** A 16-bit unsigned 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:** A 32-bit unsigned integer **Default:** 15 The Client Connection Timeout in minutes (set to 0 for no timeout).
DeviceSessionTimeout { DeviceSessionTimeout }	**Synopsis:** A 32-bit unsigned integer **Default:** 15 The Device Session Timeout in minutes (set to 0 for no timeout).

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 18.6.3
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 Section 6.7.7.3, “Adding a Certificate”.
3. Add a private key. For more information, refer to Section 6.7.5.2, “Adding a Private Key”.
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, or type **revert** and press **Enter** to abort.

Section 18.6.4
Managing SAC Connections

This section describes how to configure and manage Station Access Controller (SAC) connections for RUGGEDCOM CROSSBOW.

CONTENTS

- Section 18.6.4.1, "Viewing a List of SAC Connections"
- Section 18.6.4.2, "Adding a SAC Connection"
- Section 18.6.4.3, "Deleting a SAC Connection"

Section 18.6.4.1
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 Section 18.6.4.2, "Adding a SAC Connection".

Section 18.6.4.2
Adding a SAC Connection

To add a SAC connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tracker 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 1 to 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). This parameter is mandatory.
sam-port { sam-port }	**Synopsis:** A 16-bit unsigned 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, or type **revert** and press **Enter** to abort.

Section 18.6.4.3
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, or type **revert** and press **Enter** to abort.

Section 18.6.5
Managing CROSSBOW CA Certificate Lists

This section describes how to configure CA (Certified Authority) certificates for the RUGGEDCOM CROSSBOW application.

CONTENTS

- Section 18.6.5.1, "Viewing a List of RUGGEDCOM CROSSBOW Certificate Lists"
- Section 18.6.5.2, "Adding a CA Certificate List"
- Section 18.6.5.3, "Deleting a CA Certificate List"

Section 18.6.5.1
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 Section 18.6.5.2, "Adding a CA Certificate List".

Section 18.6.5.2
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 Section 6.7.4.3, "Adding a CA Certificate and CRL".
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, or type **revert** and press **Enter** to abort.

Section 18.6.5.3
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, or type **revert** and press **Enter** to abort.

Section 18.6.6
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"
```

Section 18.6.7
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:

```
apps crossbow status log
```

A table or list similar to the following appears:

```
ruggedcom# apps crossbow status log
crossbowd-log /var/log/syslog:Jan 31 15:15:21 ruggedcom crossbowd[24762]: ssl2tcp (MutulAuth)
[1208114224], elan_init_ctx():179: Unable to loa
d cert chain file '/etc/certs/cxb_test_generated_cert.pem'.
/var/log/syslog:Jan 31 15:15:21 ruggedcom crossbowd[24762]: ssl2tcp (MutulAuth)[1208114224],
 gethostbyname() failed using ip= -
```

```
> Resource temporarily unavailable
/var/log/syslog:Jan 31 15:15:21 ruggedcom crossbowd[24762]: ssl2tcp (MutulAuth)[1208114224], Create
 socket error: :21005 ->Reso
urce temporarily unavailable
/var/log/syslog:Jan 31 15:15:21 ruggedcom crossbowd[24762]: ssl2tcp (MutulAuth)[1208114224],
 main():193: Could not create SERVE
R Socket (errno 11: Resource temporarily unavailable): fd: -1, bailing.
/var/log/syslog:Jan 31 15:15:22 ruggedcom crossbowd[24763]: ssl2tcp (ClentConn)[1208114224], Log
 Level set to 2
/var/log/syslog:Jan 31 15:15:22 ruggedcom crossbowd[24763]: ssl2tcp (ClentConn)[1208114224],
 elan_init_security():100: Unable
to load random seed file.
.
.
.
```

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:

IMPORTANT!
For further assistance, contact Siemens Customer Support.

NOTE
For a description of pre-configured alarms, refer to Section 5.7.1, "Pre-Configured Alarms".

CONTENTS

- Section 19.1, "Ethernet Ports"
- Section 19.2, "Multicast Filtering"
- Section 19.3, "Spanning Tree"
- Section 19.4, "VLANs"
- Section 19.5, "Firmware Updates"

Section 19.1

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.

Section 19.2
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. For more information, refer to Section 8.1.3, "Viewing Switched Ethernet Port Statistics". 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. **IMPORTANT!** *Multicasting will introduce latency in all traffic on the network. Plan the network carefully in order 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.

Section 19.3
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 port status LEDs are flashing rapidly.	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 connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	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. 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 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 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.

Problem	Solution
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.

Section 19.4
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 send messages to devices in the other VLAN.	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.

Section 19.5
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.

Error Message	Solution
	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.