

# SIEMENS

## RUGGEDCOM ROX II v2.9

### Web Interface User Guide

For RX5000, MX5000, MX5000RE

**01/2016**  
RC1244-EN-02

### Preface

---

### Introduction

---

**1**

### Using RUGGEDCOM ROX II

---

**2**

### Device Management

---

**3**

### System Administration

---

**4**

### Setup and Configuration

---

**5**

### Troubleshooting

---

**6**

Copyright © 2016 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) [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 <http://www.siemens.com/industrialsecurity>.

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

## » Warranty

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

For warranty details, visit [www.siemens.com/ruggedcom](http://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](mailto:ruggedcom.info.i-ia@siemens.com)

### **Web**

[www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom)





# Table of Contents

Preface .....	xxxiii
Alerts .....	xxxiii
Related Documents .....	xxxiii
System Requirements .....	xxxiv
Accessing Documentation .....	xxxiv
License Conditions .....	xxxiv
Training .....	xxxiv
Customer Support .....	xxxv
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
Chapter 2	
Using RUGGEDCOM ROX II .....	15
2.1 Connecting to RUGGEDCOM ROX II .....	15
2.1.1 Connecting Directly .....	15
2.1.2 Connecting Through the Network .....	16
2.2 Default User Names and Passwords .....	17
2.3 Logging In .....	17
2.4 Logging Out .....	18
2.5 Navigating the Interface .....	19
2.5.1 Menus .....	19
2.5.2 Modes .....	20
2.5.3 Edit Toolbar .....	21
2.5.4 Using the Navigation Menu .....	21
2.5.5 Icons .....	22
2.5.6 Common Controls .....	23
2.6 Using Network Utilities .....	24
2.6.1 Pinging a Host .....	24

2.6.2 Dumping Raw Data to a Terminal or File .....	26
2.6.3 Tracing the Route to a Remote Host .....	28
2.6.4 Pinging an IPv4 Address Using MPLS Protocols .....	29
2.6.5 Tracing the Route of an IPv4 Address Using MPLS Protocols .....	30
2.7 Using the Command Line Interface .....	30

## Chapter 3

<b>Device Management .....</b>	<b>33</b>
3.1 Determining the Product Version .....	33
3.2 Viewing Chassis Information and Status .....	34
3.2.1 Viewing the Slot Hardware .....	35
3.2.2 Viewing Module Information .....	35
3.2.3 Viewing Flash Card Storage Utilization .....	36
3.2.4 Viewing CPU/RAM Utilization .....	37
3.2.5 Viewing the Slot Status .....	38
3.2.6 Viewing the Slot Sensor Status .....	39
3.2.7 Viewing the Power Controller Status .....	40
3.3 Viewing the Parts List .....	40
3.4 Shutting Down the Device .....	41
3.5 Rebooting the Device .....	42
3.6 Restoring Factory Defaults .....	42
3.7 Decommissioning the Device .....	44
3.8 Managing Files .....	44
3.8.1 Uploading Files .....	45
3.8.2 Downloading Files .....	45
3.8.3 Installing Files .....	46
3.8.4 Backing Up Files .....	47
3.9 Managing Logs .....	49
3.9.1 Viewing Logs .....	50
3.9.2 Deleting Logs .....	51
3.9.3 Configuring a Source IP Address for Remote Syslog Messages .....	52
3.9.4 Managing Diagnostic Logs .....	53
3.9.4.1 Enabling/Disabling the Developer's Log .....	53
3.9.4.2 Enabling/Disabling the SNMP Log .....	54
3.9.4.3 Enabling/Disabling the NETCONF Summary Log .....	55
3.9.4.4 Enabling/Disabling the NETCONF Trace Log .....	56
3.9.4.5 Enabling/Disabling the XPATH Trace Log .....	57
3.9.4.6 Enabling/Disabling the WebUI Trace Log .....	57
3.9.5 Configuring Secure Remote Syslog .....	58
3.9.5.1 Enabling/Disabling Secure Remote Syslog .....	58
3.9.5.2 Viewing a List of Permitted Peers .....	59

3.9.5.3	Adding a Permitted Peer .....	60
3.9.5.4	Deleting a Permitted Peer .....	61
3.9.6	Managing Remote Syslog Servers .....	61
3.9.6.1	Viewing a List of Remote Servers .....	61
3.9.6.2	Adding a Remote Server .....	62
3.9.6.3	Deleting a Remote Server .....	63
3.9.7	Managing Remote Server Selectors .....	64
3.9.7.1	Viewing a List of Remote Server Selectors .....	64
3.9.7.2	Adding a Remote Server Selector .....	65
3.9.7.3	Deleting a Remote Server Selector .....	67
3.10	Managing the Software Configuration .....	68
3.10.1	Saving the Configuration .....	68
3.10.2	Loading a Configuration .....	69
3.11	Upgrading/Downgrading the RUGGEDCOM ROX II Software .....	70
3.11.1	Configuring the Upgrade Source .....	71
3.11.2	Setting Up an Upgrade Server .....	72
3.11.2.1	Configuring the Upgrade Server .....	72
3.11.2.2	Adding Software Releases to the Upgrade Server .....	73
3.11.3	Upgrading the RUGGEDCOM ROX II Software .....	74
3.11.4	Stopping/Declining a Software Upgrade .....	76
3.11.5	Downgrading the RUGGEDCOM ROX II Software .....	77
3.11.5.1	Rolling Back a Software Upgrade .....	77
3.11.5.2	Downgrading Using ROXflash .....	78
3.12	Managing RUGGEDCOM ROX II Applications .....	80
3.12.1	Viewing a List of Installed Applications .....	81
3.12.2	Installing an Application .....	81
3.12.3	Upgrading an Application .....	82
3.12.4	Uninstalling an Application .....	83
3.12.5	Managing Application Repositories .....	84
3.12.5.1	Viewing a List of Repositories .....	84
3.12.5.2	Checking the Repository Connection .....	85
3.12.5.3	Adding a Repository .....	86
3.12.5.4	Deleting a Repository .....	87
3.13	Managing Feature Keys .....	88
3.14	Managing the Fan Controller .....	89
3.14.1	Viewing the Fan Controller Status .....	89
3.14.2	Configuring the Activation Temperature .....	90
3.15	Managing Fixed Modules .....	91
3.15.1	Viewing a List of Fixed Module Configurations .....	91
3.15.2	Adding a Fixed Module Configuration .....	91

3.15.3	Deleting a Fixed Module Configuration .....	93
3.16	Managing Line Modules .....	93
3.16.1	Removing a Line Module .....	93
3.16.2	Installing a New Line Module .....	94
3.16.3	Viewing a List of Line Module Configurations .....	95
3.16.4	Configuring a Line Module .....	95
3.17	Managing Event Trackers .....	96
3.17.1	Viewing a List of Event Trackers .....	96
3.17.2	Viewing Event Tracker Statistics .....	97
3.17.3	Adding an Event Tracker .....	98
3.17.4	Deleting an Event Tracker .....	100
3.18	Managing Switched Ethernet Ports .....	101
3.18.1	Viewing a List of Switched Ethernet Ports .....	101
3.18.2	Configuring a Switched Ethernet Port .....	101
3.18.3	Configuring Port Security .....	108
3.18.4	Viewing Switched Ethernet Port Statistics .....	112
3.18.5	Viewing RMON Port Statistics .....	113
3.18.6	Clearing Switched Ethernet Port Statistics .....	116
3.18.7	Resetting a Switched Ethernet Port .....	117
3.18.8	Testing Switched Ethernet Port Cables .....	117
3.18.8.1	Running a Cable Diagnostic Test .....	118
3.18.8.2	Viewing Cable Diagnostic Statistics .....	119
3.18.8.3	Clearing Cable Diagnostic Statistics .....	121
3.19	Managing Routable Ethernet Ports .....	122
3.19.1	Viewing a List of Routable Ethernet Ports .....	122
3.19.2	Configuring a Routable Ethernet Port .....	122
3.20	Managing Serial Ports .....	125
3.20.1	Viewing Transport Connection Statistics .....	125
3.20.2	Viewing DNP Device Table Statistics .....	127
3.20.3	Restarting the Serial Server .....	128
3.20.4	Resetting a Serial Port .....	128
3.21	Managing Serial Port Protocols .....	129
3.21.1	Serial Port Protocol Concepts .....	129
3.21.1.1	Raw Socket Applications .....	129
3.21.1.2	Modbus TCP Applications .....	130
3.21.1.3	DNP Applications .....	131
3.21.1.4	Incoming/Outgoing Serial Connections .....	132
3.21.2	Viewing a List of Serial Port Protocols .....	132
3.21.3	Adding a Serial Port Protocol .....	133
3.21.4	Configuring the DNP Protocol .....	133

3.21.5	Configuring the Modbus TCP Protocol .....	134
3.21.6	Configuring the Raw Socket Protocol .....	136
3.21.7	Deleting a Serial Port Protocol .....	139
3.21.8	Managing Device Address Tables .....	139
3.21.8.1	Viewing a List of Device Address Tables .....	139
3.21.8.2	Adding a Device Address Table .....	140
3.21.8.3	Deleting a Device Address Table .....	141
3.21.9	Managing Remote Hosts .....	142
3.21.9.1	Viewing a List of Remote Hosts .....	142
3.21.9.2	Adding a Remote Host .....	143
3.21.9.3	Deleting a Remote Host .....	143
3.22	Managing Ethernet Trunk Interfaces .....	144
3.22.1	Viewing a List of Ethernet Trunk Interfaces .....	144
3.22.2	Adding an Ethernet Trunk Interface .....	145
3.22.3	Deleting an Ethernet Trunk Interface .....	149
3.22.4	Managing Ethernet Trunk Ports .....	150
3.22.4.1	Viewing a List of Ethernet Trunk Ports .....	150
3.22.4.2	Adding an Ethernet Trunk Port .....	150
3.22.4.3	Deleting an Ethernet Trunk Port .....	151
3.23	Managing Virtual Switches .....	152
3.23.1	Viewing a List of Virtual Switches .....	153
3.23.2	Adding a Virtual Switch .....	154
3.23.3	Deleting a Virtual Switch .....	156
3.23.4	Managing Virtual Switch Interfaces .....	156
3.23.4.1	Viewing a List of Virtual Switch Interfaces .....	157
3.23.4.2	Adding a Virtual Switch Interface .....	157
3.23.4.3	Deleting a Virtual Switch Interface .....	158
3.23.5	Filtering Virtual Switch Traffic .....	159
3.23.5.1	Enabling/Disabling Virtual Switch Filtering .....	159
3.23.5.2	Viewing a List of Virtual Switch Filters .....	160
3.23.5.3	Adding a Virtual Switch Filter .....	160
3.23.5.4	Deleting a Virtual Switch Filter .....	161
3.23.6	Managing Filtering Rules .....	162
3.23.6.1	Viewing a List of Rules .....	162
3.23.6.2	Viewing a List of Rules Assigned to a Virtual Switch Filter .....	163
3.23.6.3	Adding a Rule .....	163
3.23.6.4	Adding a Rule to a Virtual Switch Filter .....	165
3.23.6.5	Deleting a Rule .....	166
3.23.6.6	Deleting a Rule from a Virtual Switch Filter .....	167
3.23.7	Managing In/Out Interfaces .....	167

3.23.7.1	Viewing a List of In/Out Interfaces .....	167
3.23.7.2	Adding In/Out Interfaces .....	168
3.23.7.3	Deleting an In/Out Interface .....	169
3.24	Managing a Domain Name System (DNS) .....	169
3.24.1	Managing Domain Names .....	169
3.24.1.1	Viewing a List of Domain Names .....	170
3.24.1.2	Adding a Domain Name .....	170
3.24.1.3	Deleting a Domain Name .....	171
3.24.2	Managing Domain Name Servers .....	171
3.24.2.1	Viewing a List of Domain Name Servers .....	172
3.24.2.2	Adding a Domain Name Server .....	172
3.24.2.3	Deleting a Domain Name Server .....	173

## Chapter 4

<b>System Administration</b> .....	<b>175</b>
4.1 Configuring the System Name and Location .....	175
4.2 Configuring the Hostname .....	176
4.3 Customizing the Welcome Screen .....	177
4.4 Setting the User Authentication Mode .....	178
4.5 Setting the Maximum Number of Sessions .....	179
4.6 Managing Alarms .....	180
4.6.1 Pre-Configured Alarms .....	181
4.6.2 Viewing a List of Active Alarms .....	182
4.6.3 Clearing and Acknowledging Alarms .....	182
4.6.3.1 Clearing Alarms .....	182
4.6.3.2 Acknowledging Alarms .....	183
4.6.4 Configuring an Alarm .....	184
4.7 Managing Certificates and Keys .....	186
4.7.1 Managing CA Certificates and CRLs .....	186
4.7.1.1 Viewing a List of CA Certificates and CRLs .....	187
4.7.1.2 Viewing the Status of a CA Certificate and CRL .....	187
4.7.1.3 Adding a CA Certificate and CRL .....	189
4.7.1.4 Deleting a CA Certificate and CRL .....	191
4.7.2 Managing Private Keys .....	191
4.7.2.1 Viewing a List of Private Keys .....	192
4.7.2.2 Adding a Private Key .....	192
4.7.2.3 Deleting a Private Key .....	193
4.7.3 Managing Public Keys .....	194
4.7.3.1 Viewing a List of Public Keys .....	194
4.7.3.2 Adding a Public Key .....	195
4.7.3.3 Adding an IPSec-Formatted Public Key .....	197

4.7.3.4	Deleting a Public Key .....	198
4.7.4	Managing Certificates .....	199
4.7.4.1	Viewing a List of Certificates .....	199
4.7.4.2	Viewing the Status of a Certificate .....	199
4.7.4.3	Adding a Certificate .....	200
4.7.4.4	Deleting a Certificate .....	202
4.8	Managing RADIUS Authentication .....	202
4.8.1	Configuring RADIUS Authentication for LOGIN Services .....	204
4.8.2	Configuring RADIUS Authentication for PPP Services .....	206
4.8.3	Configuring RADIUS Authentication for Switched Ethernet Ports .....	207
4.9	Managing Users .....	209
4.9.1	Viewing a List of Users .....	210
4.9.2	Adding a User .....	210
4.9.3	Deleting a User .....	211
4.9.4	Monitoring Users .....	212
4.9.4.1	Kicking Users from the Network .....	213
4.9.4.2	Sending Messages to Users .....	214
4.10	Managing Passwords and Passphrases .....	215
4.10.1	Configuring Password/Passphrase Complexity Rules .....	216
4.10.2	Setting a User Password/Passphrase .....	218
4.10.3	Setting the Boot Password/Passphrase .....	219
4.10.4	Setting the Maintenance Password/Passphrase .....	221
4.10.5	Resetting Passwords and Passphrases .....	222
4.11	Scheduling Jobs .....	222
4.11.1	Viewing a List of Scheduled Jobs .....	223
4.11.2	Adding Scheduled Jobs .....	223
4.11.3	Deleting a Scheduled Job .....	227
Chapter 5		
<b>Setup and Configuration .....</b>		<b>229</b>
5.1	Configuring a Basic Network .....	230
5.1.1	Configuring a Basic IPv4 Network .....	230
5.1.2	Configuring a Basic IPv6 Network .....	231
5.2	Configuring ICMP Control .....	231
5.3	Enabling and Configuring CLI Sessions .....	233
5.4	Enabling and Configuring SFTP Sessions .....	235
5.5	Enabling and Configuring WWW Interface Sessions .....	237
5.6	Enabling/Disabling Brute Force Attack Protection .....	239
5.7	Viewing the Status of IPv4 Routes .....	241
5.8	Viewing the Status of IPv6 Routes .....	242
5.9	Viewing the Memory Statistics .....	243

5.10	Managing NETCONF .....	244
5.10.1	Enabling and Configuring NETCONF Sessions .....	244
5.10.2	Viewing NETCONF Statistics .....	246
5.11	Managing SNMP .....	248
5.11.1	MIB Files and SNMP Traps .....	248
5.11.2	Enabling and Configuring SNMP Sessions .....	250
5.11.3	Viewing Statistics for SNMP .....	253
5.11.4	Discovering SNMP Engine IDs .....	253
5.11.5	Managing SNMP Communities .....	254
5.11.5.1	Viewing a List of SNMP Communities .....	255
5.11.5.2	Adding an SNMP Community .....	255
5.11.5.3	Deleting an SNMP Community .....	256
5.11.6	Managing SNMP Target Addresses .....	257
5.11.6.1	Viewing a List of SNMP Target Addresses .....	257
5.11.6.2	Adding an SNMP Target Address .....	257
5.11.6.3	Deleting an SNMP Target Address .....	260
5.11.7	Managing SNMP Users .....	261
5.11.7.1	Viewing a List of SNMP Users .....	261
5.11.7.2	Adding an SNMP User .....	262
5.11.7.3	Deleting an SNMP User .....	264
5.11.8	Managing SNMP Security Model Mapping .....	264
5.11.8.1	Viewing a List of SNMP Security Models .....	264
5.11.8.2	Adding an SNMP Security Model .....	265
5.11.8.3	Deleting an SNMP Security Model .....	266
5.11.9	Managing SNMP Group Access .....	267
5.11.9.1	Viewing a List of SNMP Groups .....	267
5.11.9.2	Adding an SNMP Group .....	268
5.11.9.3	Deleting an SNMP Group .....	270
5.12	Managing Time Synchronization Functions .....	270
5.12.1	Configuring the Time Synchronization Settings .....	271
5.12.2	Configuring the System Time and Date .....	272
5.12.3	Configuring the System Time Zone .....	273
5.12.4	Configuring the Local Time Settings .....	274
5.12.5	Configuring NTP Multicast Clients .....	275
5.12.6	Configuring NTP Broadcast Clients .....	275
5.12.7	Enabling/Disabling the NTP Service .....	276
5.12.8	Viewing the NTP Service Status .....	277
5.12.9	Viewing the Status of Reference Clocks .....	278
5.12.10	Monitoring Subscribers .....	279
5.12.11	Managing NTP Servers .....	280



5.12.11.1	Viewing a List of NTP Servers .....	280
5.12.11.2	Adding an NTP Server .....	280
5.12.11.3	Deleting an NTP Server .....	282
5.12.12	Managing NTP Broadcast/Multicast Addresses .....	283
5.12.12.1	Viewing a List of Broadcast/Multicast Addresses .....	283
5.12.12.2	Adding a Broadcast/Multicast Address .....	284
5.12.12.3	Deleting a Broadcast/Multicast Address .....	285
5.12.13	Managing Server Keys .....	286
5.12.13.1	Viewing a List of Server Keys .....	286
5.12.13.2	Adding a Server Key .....	287
5.12.13.3	Deleting a Server Key .....	288
5.12.14	Managing Server Restrictions .....	289
5.12.14.1	Viewing a List of Server Restrictions .....	289
5.12.14.2	Adding a Server Restriction .....	290
5.12.14.3	Deleting a Server Restriction .....	292
5.13	Managing the DHCP Relay Agent .....	292
5.13.1	Configuring the DHCP Relay Agent .....	293
5.13.2	Viewing a List of DHCP Client Ports .....	294
5.13.3	Adding DHCP Client Ports .....	294
5.13.4	Deleting a DHCP Client Port .....	295
5.14	Managing the DHCP Server .....	295
5.14.1	Configuring the DHCP Server .....	296
5.14.2	Enabling/Disabling the DHCP Server .....	296
5.14.3	Enabling/Disabling the DHCP Relay Support .....	297
5.14.4	Viewing a List of Active Leases .....	298
5.14.5	Managing DHCP Listen Interfaces .....	299
5.14.5.1	Viewing a List of DHCP Listen Interfaces .....	299
5.14.5.2	Adding a DHCP Listen Interface .....	299
5.14.5.3	Deleting a DHCP Listen Interface .....	300
5.14.6	Managing Shared Networks .....	301
5.14.6.1	Viewing a List of Shared Networks .....	301
5.14.6.2	Adding a Shared Network .....	301
5.14.6.3	Configuring Shared Network Options .....	302
5.14.6.4	Configuring a Shared Network Client .....	304
5.14.6.5	Customizing Shared Network Clients .....	307
5.14.6.6	Deleting a Shared Network .....	308
5.14.7	Managing Subnets .....	309
5.14.7.1	Viewing a List of Subnets .....	309
5.14.7.2	Adding a Subnet .....	310
5.14.7.3	Configuring Subnet Options .....	311

5.14.7.4	Configuring a Subnet Client .....	313
5.14.7.5	Deleting a Subnet .....	316
5.14.8	Managing Custom Client Options for Subnets .....	317
5.14.8.1	Viewing a List of Custom Client Options .....	317
5.14.8.2	Adding a Custom Client Option .....	317
5.14.8.3	Deleting a Custom Client Option .....	318
5.14.9	Managing Hosts .....	319
5.14.9.1	Viewing a List of Hosts .....	319
5.14.9.2	Adding a Host .....	320
5.14.9.3	Configuring Host Options .....	321
5.14.9.4	Configuring a Host Client .....	323
5.14.9.5	Deleting Hosts .....	326
5.14.10	Managing Custom Host Client Configurations .....	327
5.14.10.1	Viewing a List of Custom Host Client Configurations .....	327
5.14.10.2	Adding Custom Host Client Configurations .....	327
5.14.10.3	Deleting Custom Host Client Configurations .....	328
5.14.11	Managing Host Groups .....	329
5.14.11.1	Viewing a List of Host Groups .....	329
5.14.11.2	Adding a Host Group .....	330
5.14.11.3	Configuring Host Group Options .....	330
5.14.11.4	Configuring a Host Group Client .....	332
5.14.11.5	Deleting a Host Group .....	335
5.14.12	Managing Custom Host Group Client Configurations .....	336
5.14.12.1	Viewing a List of Custom Host Group Client Configurations .....	336
5.14.12.2	Adding Custom Host Group Client Configurations .....	336
5.14.12.3	Deleting Custom Host Group Client Configurations .....	337
5.14.13	Managing IP Pools .....	338
5.14.13.1	Viewing a List of IP Pools .....	338
5.14.13.2	Adding an IP Pool .....	339
5.14.13.3	Deleting an IP Pool .....	340
5.14.14	Managing IP Ranges for Subnets .....	341
5.14.14.1	Viewing a List of IP Ranges for Subnets .....	341
5.14.14.2	Adding an IP Range to a DHCP Subnet .....	342
5.14.14.3	Deleting an IP Range From a Subnet .....	343
5.14.15	Managing IP Ranges for IP Pools .....	343
5.14.15.1	Viewing a List of IP Ranges for IP Pools .....	344
5.14.15.2	Adding an IP Range to an IP Pool .....	344
5.14.15.3	Deleting an IP Range From an IP Pool .....	345
5.14.16	Managing Option 82 Classes for IP Pools .....	346
5.14.16.1	Viewing a List of Option 82 Classes for IP Pools .....	346

5.14.16.2	Adding an Option 82 Class to an IP Pool .....	346
5.14.16.3	Deleting an Option 82 Class From an IP Pool .....	348
5.15	Managing Port Mirroring .....	348
5.15.1	Configuring Port Mirroring .....	349
5.15.2	Managing Egress Source Ports .....	350
5.15.2.1	Viewing a List of Egress Source Ports .....	350
5.15.2.2	Adding an Egress Source Port .....	350
5.15.2.3	Deleting an Egress Source Port .....	351
5.15.3	Managing Ingress Source Ports .....	352
5.15.3.1	Viewing a List of Ingress Source Ports .....	352
5.15.3.2	Adding an Ingress Source Port .....	352
5.15.3.3	Deleting an Ingress Source Port .....	353
5.16	Managing Firewalls .....	354
5.16.1	Firewall Concepts .....	355
5.16.1.1	Stateless vs. Stateful Firewalls .....	355
5.16.1.2	Linux netfilter .....	355
5.16.1.3	Network Address Translation .....	356
5.16.1.4	Port Forwarding .....	356
5.16.1.5	Protecting Against a SYN Flood Attack .....	357
5.16.2	Viewing a List of Firewalls .....	357
5.16.3	Adding a Firewall .....	357
5.16.4	Deleting a Firewall .....	359
5.16.5	Working with Multiple Firewall Configurations .....	360
5.16.6	Configuring the Firewall for a VPN .....	360
5.16.7	Configuring the Firewall for a VPN in a DMZ .....	362
5.16.8	Managing Zones .....	362
5.16.8.1	Viewing a List of Zones .....	363
5.16.8.2	Adding a Zone .....	363
5.16.8.3	Deleting a Zone .....	365
5.16.9	Managing Interfaces .....	366
5.16.9.1	Viewing a List of Interfaces .....	366
5.16.9.2	Adding an Interface .....	366
5.16.9.3	Associating an Interface with a Zone .....	369
5.16.9.4	Configuring a Broadcast Address .....	370
5.16.9.5	Deleting an Interface .....	371
5.16.10	Managing Hosts .....	372
5.16.10.1	Viewing a List of Hosts .....	372
5.16.10.2	Adding a Host .....	373
5.16.10.3	Deleting a Host .....	375
5.16.11	Managing Policies .....	375

5.16.11.1	Viewing a List of Policies .....	376
5.16.11.2	Adding a Policy .....	377
5.16.11.3	Configuring the Source Zone .....	378
5.16.11.4	Configuring the Destination Zone .....	379
5.16.11.5	Deleting a Policy .....	380
5.16.12	Managing Network Address Translation Settings .....	380
5.16.12.1	Viewing a List of NAT Settings .....	381
5.16.12.2	Adding a NAT Setting .....	381
5.16.12.3	Deleting a NAT Setting .....	383
5.16.13	Managing Masquerade and SNAT Settings .....	384
5.16.13.1	Viewing a List of Masquerade and SNAT Settings .....	384
5.16.13.2	Adding Masquerade or SNAT Settings .....	384
5.16.13.3	Deleting a Masquerade or SNAT Setting .....	386
5.16.14	Managing Rules .....	387
5.16.14.1	Viewing a List of Rules .....	387
5.16.14.2	Adding a Rule .....	387
5.16.14.3	Configuring the Source Zone .....	391
5.16.14.4	Configuring the Destination Zone .....	391
5.16.14.5	Deleting Rules .....	392
5.16.15	Validating a Firewall Configuration .....	393
5.16.16	Enabling/Disabling a Firewall .....	394
5.17	Managing IS-IS .....	394
5.17.1	IS-IS Concepts .....	395
5.17.1.1	IS-IS Routers .....	395
5.17.1.2	Network Entity Title (NET) Addresses .....	396
5.17.1.3	Advantages and Disadvantages of Using IS-IS .....	396
5.17.2	Configuring IS-IS .....	396
5.17.3	Viewing the Status of Neighbors .....	398
5.17.4	Viewing the Status of the Link-State Database .....	399
5.17.5	Managing Area Tags .....	402
5.17.5.1	Viewing a List of Area Tags .....	402
5.17.5.2	Adding an Area Tag .....	403
5.17.5.3	Deleting an Area Tag .....	405
5.17.6	Managing Interfaces .....	406
5.17.6.1	Viewing a List of Interfaces .....	406
5.17.6.2	Configuring an Interface .....	407
5.17.7	Managing LSP Generation .....	410
5.17.7.1	Viewing a List of LSP Generation Intervals .....	410
5.17.7.2	Adding an LSP Generation Interval .....	410
5.17.7.3	Deleting an LSP Generation Interval .....	411

5.17.8	Managing SPF Calculations .....	412
5.17.8.1	Viewing a List of SPF Calculation Intervals .....	412
5.17.8.2	Adding an SPF Calculation Interval .....	413
5.17.8.3	Deleting an SPF Calculation Interval .....	414
5.17.9	Managing the Lifetime of LSPs .....	415
5.17.9.1	Viewing a List of LSP Lifetime Intervals .....	415
5.17.9.2	Adding an LSP Lifetime Interval .....	415
5.17.9.3	Deleting an LSP Lifetime Interval .....	417
5.17.10	Managing LSP Refresh Intervals .....	417
5.17.10.1	Viewing a List of LSP Refresh Intervals .....	418
5.17.10.2	Adding an LSP Refresh Interval .....	418
5.17.10.3	Deleting an LSP Refresh Interval .....	419
5.17.11	Managing Network Entity Titles (NETs) .....	420
5.17.11.1	Viewing a List of NETs .....	421
5.17.11.2	Adding a NET .....	421
5.17.11.3	Deleting a NET .....	422
5.17.12	Managing Redistribution Metrics .....	422
5.17.12.1	Viewing a List of Redistribution Metrics .....	423
5.17.12.2	Adding a Redistribution Metric .....	423
5.17.12.3	Deleting a Redistribution Metric .....	425
5.18	Managing BGP .....	425
5.18.1	Configuring BGP .....	426
5.18.2	Viewing the Status of Dynamic BGP Routes .....	428
5.18.3	Managing Route Maps .....	429
5.18.3.1	Viewing a List of Route Map Filters .....	430
5.18.3.2	Viewing a List of Route Map Filter Entries .....	430
5.18.3.3	Adding a Route Map Filter .....	431
5.18.3.4	Adding a Route Map Filter Entry .....	431
5.18.3.5	Deleting a Route Map Filter .....	433
5.18.3.6	Deleting a Route Map Filter Entry .....	433
5.18.3.7	Configuring Match Rules .....	434
5.18.3.8	Configuring a Set .....	436
5.18.4	Managing Prepended and Excluded Autonomous System Paths .....	438
5.18.4.1	Viewing a List of Prepended Autonomous System Path Filters .....	439
5.18.4.2	Viewing a List of Excluded Autonomous System Paths .....	439
5.18.4.3	Adding a Prepended Autonomous System Path Filter .....	439
5.18.4.4	Adding an Excluded Autonomous System Path filter .....	440
5.18.4.5	Deleting a Prepended Autonomous System Path Filter .....	441
5.18.4.6	Deleting an Excluded Autonomous System Path Filter .....	442
5.18.5	Managing Prefix Lists and Entries .....	443

5.18.5.1	Viewing a List of Prefix Lists .....	443
5.18.5.2	Viewing a List of Prefix Entries .....	443
5.18.5.3	Adding a Prefix List .....	444
5.18.5.4	Adding a Prefix Entry .....	445
5.18.5.5	Deleting a Prefix List .....	446
5.18.5.6	Deleting a Prefix Entry .....	447
5.18.6	Managing Autonomous System Paths and Entries .....	448
5.18.6.1	Viewing a List of Autonomous System Paths .....	448
5.18.6.2	Viewing a List of Autonomous System Path Entries .....	448
5.18.6.3	Adding an Autonomous System Path Filter .....	449
5.18.6.4	Adding an Autonomous System Path Filter Entry .....	450
5.18.6.5	Deleting an Autonomous System Path .....	451
5.18.6.6	Deleting an Autonomous System Path Filter Entry .....	452
5.18.7	Managing Neighbors .....	453
5.18.7.1	Viewing a List of Neighbors .....	453
5.18.7.2	Adding a Neighbor .....	453
5.18.7.3	Configuring the Distribution of Prefix Lists .....	456
5.18.7.4	Tracking Commands for BGP Neighbors .....	457
5.18.7.5	Deleting a Neighbor .....	458
5.18.8	Managing Networks .....	458
5.18.8.1	Viewing a List of Networks .....	459
5.18.8.2	Adding a Network .....	459
5.18.8.3	Tracking Commands for a BGP Network .....	460
5.18.8.4	Deleting a Network .....	461
5.18.9	Managing Aggregate Addresses .....	462
5.18.9.1	Viewing a List of Aggregate Addresses .....	462
5.18.9.2	Adding an Aggregate Address .....	463
5.18.9.3	Deleting an Aggregate Address .....	463
5.18.10	Managing Aggregate Address Options .....	464
5.18.10.1	Viewing a List of Aggregate Address Options .....	464
5.18.10.2	Adding an Aggregate Address Option .....	465
5.18.10.3	Deleting an Aggregate Address Option .....	465
5.18.11	Managing Redistribution Metrics .....	466
5.18.11.1	Viewing a List of Redistribution Metrics .....	466
5.18.11.2	Adding a Redistribution Metric .....	467
5.18.11.3	Deleting a Redistribution Metric .....	468
5.19	Managing RIP .....	468
5.19.1	Configuring RIP .....	469
5.19.2	Viewing the Status of Dynamic RIP Routes .....	471
5.19.3	Managing Prefix Lists and Entries .....	473

5.19.3.1	Viewing a List of Prefix Lists .....	473
5.19.3.2	Viewing a List of Prefix Entries .....	474
5.19.3.3	Adding a Prefix List .....	474
5.19.3.4	Adding a Prefix Entry .....	476
5.19.3.5	Deleting a Prefix List .....	477
5.19.3.6	Deleting a Prefix Entry .....	478
5.19.4	Managing Networks .....	479
5.19.4.1	Configuring a Network .....	479
5.19.4.2	Tracking Commands .....	479
5.19.5	Managing Network IP Address .....	480
5.19.5.1	Viewing a List of Network IP Addresses .....	481
5.19.5.2	Adding a Network IP Address .....	481
5.19.5.3	Deleting a Network IP Address .....	482
5.19.6	Managing Network Interfaces .....	482
5.19.6.1	Viewing a List of Network Interfaces .....	483
5.19.6.2	Adding a Network Interface .....	483
5.19.6.3	Deleting a Network Interface .....	484
5.19.7	Managing Neighbors .....	484
5.19.7.1	Viewing a List of Neighbors .....	484
5.19.7.2	Adding a Neighbor .....	485
5.19.7.3	Deleting a Neighbor .....	486
5.19.8	Managing the Prefix List Distribution .....	486
5.19.8.1	Viewing a List of Prefix List Distribution Paths .....	486
5.19.8.2	Adding a Prefix List Distribution Path .....	487
5.19.8.3	Deleting a Prefix List Distribution Path .....	488
5.19.9	Managing Key Chains and Keys .....	489
5.19.9.1	Viewing a List of Key Chains .....	489
5.19.9.2	Viewing a List of Keys .....	489
5.19.9.3	Adding a Key Chain .....	490
5.19.9.4	Adding a Key .....	490
5.19.9.5	Deleting a Key Chain .....	493
5.19.9.6	Deleting a Key .....	493
5.19.10	Managing Redistribution Metrics .....	494
5.19.10.1	Viewing a List of Redistribution Metrics .....	494
5.19.10.2	Adding a Redistribution Metric .....	495
5.19.10.3	Deleting a Redistribution Metric .....	496
5.19.11	Managing Routing Interfaces .....	497
5.19.11.1	Viewing a List of Routing Interfaces .....	497
5.19.11.2	Configuring a Routing Interface .....	497
5.20	Managing OSPF .....	499

5.20.1	OSPF Concepts .....	500
5.20.2	Configuring OSPF .....	500
5.20.3	Viewing the Status of Dynamic OSPF Routes .....	505
5.20.4	Managing Prefix Lists and Entries .....	505
5.20.4.1	Viewing a List of Prefix Lists .....	506
5.20.4.2	Viewing a List of Prefix Entries .....	506
5.20.4.3	Adding a Prefix List .....	507
5.20.4.4	Adding a Prefix Entry .....	508
5.20.4.5	Deleting a Prefix List .....	510
5.20.4.6	Deleting a Prefix Entry .....	511
5.20.5	Managing Areas .....	511
5.20.5.1	Viewing a List of Areas .....	512
5.20.5.2	Adding an Area .....	512
5.20.5.3	Deleting an Area .....	514
5.20.6	Managing Route Maps .....	515
5.20.6.1	Viewing a List of Route Map Filters .....	515
5.20.6.2	Viewing a List of Route Map Filter Entries .....	516
5.20.6.3	Adding a Route Map Filter .....	516
5.20.6.4	Adding a Route Map Filter Entry .....	517
5.20.6.5	Deleting a Route Map Filter .....	519
5.20.6.6	Deleting a Route Map Filter Entry .....	520
5.20.6.7	Configuring Match Rules .....	521
5.20.7	Managing Incoming Route Filters .....	522
5.20.7.1	Viewing List of Incoming Route Filters .....	523
5.20.7.2	Adding an Incoming Route Filter .....	523
5.20.7.3	Deleting an Incoming Route Filter .....	524
5.20.8	Managing Redistribution Metrics .....	525
5.20.8.1	Viewing a List of Redistribution Metrics .....	525
5.20.8.2	Adding a Redistribution Metric .....	525
5.20.8.3	Deleting a Redistribution Metric .....	527
5.20.9	Managing Routing Interfaces .....	528
5.20.9.1	Viewing a List of Routing Interfaces .....	528
5.20.9.2	Configuring a Routing Interface .....	528
5.20.10	Managing Message Digest Keys .....	531
5.20.10.1	Viewing a List of Message Digest Keys .....	532
5.20.10.2	Adding a Message Digest Key .....	532
5.20.10.3	Deleting a Message Digest Key .....	533
5.21	Managing Virtual Routing and Forwarding (VRF) .....	534
5.21.1	VRF Concepts .....	535
5.21.1.1	VRF and VRF-Lite .....	535



5.21.1.2 Advantages and Disadvantages of Using VRF .....	535
5.21.2 Viewing VRF Interface Statistics .....	536
5.21.3 Configuring VRF .....	537
5.21.4 Configuring a VRF Interface .....	538
5.21.5 Managing VRF Definitions .....	539
5.21.5.1 Viewing a List of VRF Definitions .....	539
5.21.5.2 Adding a VRF Definition .....	539
5.21.5.3 Deleting a VRF Definition .....	541
5.21.6 Managing Route Targets .....	542
5.21.6.1 Viewing a List of Route Targets .....	542
5.21.6.2 Adding a Route Target .....	542
5.21.6.3 Deleting a Route Target .....	543
5.21.7 Managing VRF Instances and OSPF .....	544
5.21.7.1 Viewing a List of VRF Instances .....	544
5.21.7.2 Adding a VRF Instance and Configuring OSPF .....	545
5.21.7.3 Deleting a VRF Instance .....	550
5.21.8 Managing IP/VPN Tunnels .....	550
5.21.8.1 Viewing a List of IP/VPN Tunnels .....	551
5.21.8.2 Adding an IP/VPN Tunnel .....	551
5.21.8.3 Deleting an IP/VPN Tunnels .....	552
5.21.9 Managing VPNv4 Neighbors .....	553
5.21.9.1 Viewing a List of Neighbors .....	553
5.21.9.2 Adding a Neighbor .....	553
5.21.9.3 Deleting a Neighbor .....	554
5.21.10 Managing IPv4 Address Families .....	555
5.21.10.1 Viewing a List of IPv4 Address Families .....	555
5.21.10.2 Adding an IPv4 Address Family .....	556
5.21.10.3 Deleting an IPv4 Address Family .....	556
5.21.11 Managing Redistribution for IPv4 Address Families .....	557
5.21.11.1 Viewing a List of Redistributions .....	557
5.21.11.2 Adding a Redistribution .....	558
5.21.11.3 Deleting a Redistribution .....	559
5.21.12 Managing Neighbors for IPv4 Address Families .....	560
5.21.12.1 Viewing a List of Neighbors .....	560
5.21.12.2 Adding a Neighbor .....	561
5.21.12.3 Configuring the Distribution of Prefix Lists .....	564
5.21.12.4 Tracking Commands .....	565
5.21.12.5 Deleting a Neighbor .....	566
5.21.13 Managing Static VRF Routes .....	567
5.21.13.1 Viewing a List of Static VRF Routes .....	567

5.21.13.2	Adding a Static VRF Route .....	568
5.21.13.3	Configuring a Black Hole Connection for a Static VRF Route .....	569
5.21.13.4	Deleting a Static VRF Route .....	570
5.21.14	Managing Gateways for Static VRF Routes .....	571
5.21.14.1	Viewing a List of Gateways for Static VRF Routes .....	571
5.21.14.2	Adding a Gateway for a Static VRF Route .....	571
5.21.14.3	Deleting a Gateway for a Static VRF Route .....	572
5.21.15	Managing Interfaces for Static VRF Routes .....	573
5.21.15.1	Viewing a List of Gateways for Static VRF Routes .....	573
5.21.15.2	Adding a Gateway for a Static VRF Route .....	574
5.21.15.3	Deleting a Gateway for a Static VRF Route .....	575
5.22	Managing Static Routing .....	575
5.22.1	Viewing a List of Static Routes .....	576
5.22.2	Adding an IPv4 Static Route .....	576
5.22.3	Adding an IPv6 Static Route .....	577
5.22.4	Deleting a Static Route .....	578
5.22.5	Configuring a Black Hole Connection for an IPv4 Static Route .....	579
5.22.6	Managing Gateways for Static Routes .....	580
5.22.6.1	Configuring Gateways for IPv6 Static Routes .....	580
5.22.6.2	Viewing a List of Gateways for IPv4 Static Routes .....	581
5.22.6.3	Adding a Gateway for an IPv4 Static Route .....	581
5.22.6.4	Deleting a Gateway for an IPv4 Static Route .....	582
5.22.7	Managing Interfaces for Static Routes .....	583
5.22.7.1	Configuring Interfaces for IPv6 Static Routes .....	583
5.22.7.2	Viewing a List of Interfaces for IPv4 Static Routes .....	584
5.22.7.3	Adding an Interface for an IPv4 Static Route .....	585
5.22.7.4	Deleting an Interface for an IPv4 Static Route .....	586
5.23	Managing Static Multicast Routing .....	586
5.23.1	Enabling/Disabling Static Multicast Routing .....	586
5.23.2	Managing Static Multicast Groups .....	587
5.23.2.1	Viewing a List of Static Multicast Groups .....	587
5.23.2.2	Adding a Static Multicast Group .....	588
5.23.2.3	Deleting a Static Multicast Group .....	590
5.23.3	Managing Out-Interfaces .....	590
5.23.3.1	Viewing a List of Out-Interfaces .....	590
5.23.3.2	Adding an Out-Interface .....	591
5.23.3.3	Deleting an Out-Interface .....	592
5.24	Managing Dynamic Multicast Routing .....	592
5.24.1	PIM-SM Concepts .....	593
5.24.2	Configuring PIM-SM .....	594

5.24.3	Viewing a List of PIM-SM Interfaces .....	595
5.24.4	Enabling/Disabling a PIM-SM Interface .....	595
5.24.5	Configuring a Static RP Address .....	596
5.24.6	Managing a Boot Strap Router .....	597
5.24.6.1	Configuring a BSR Candidate .....	597
5.24.6.2	Configuring a Group Prefix .....	598
5.24.6.3	Configuring an RP Candidate .....	599
5.24.7	Viewing the Status of PIM-SM .....	600
5.24.8	Viewing the Status of Dynamic Multicast Routing .....	602
5.25	Managing Multicast Filtering .....	602
5.25.1	Multicast Filtering Concepts .....	602
5.25.1.1	IGMP .....	602
5.25.1.2	GMRP (GARP Multicast Registration Protocol) .....	606
5.25.2	Enabling and Configuring GMRP .....	609
5.25.3	Managing IGMP Snooping .....	610
5.25.3.1	Configuring IGMP Snooping .....	610
5.25.3.2	Viewing a List of Router Ports .....	612
5.25.3.3	Adding a Router Port .....	612
5.25.3.4	Deleting a Router Port .....	613
5.25.4	Managing the Static Multicast Group Table .....	613
5.25.4.1	Viewing a List of Static Multicast Group Entries .....	614
5.25.4.2	Adding a Static Multicast Group Entry .....	614
5.25.4.3	Deleting a Static Multicast Group Entry .....	615
5.25.5	Managing Egress Ports for Multicast Groups .....	616
5.25.5.1	Viewing a List of Egress Ports .....	616
5.25.5.2	Adding an Egress Port .....	616
5.25.5.3	Deleting an Egress Port .....	617
5.25.6	Viewing a Summary of Multicast Groups .....	618
5.25.7	Viewing a List of IP Multicast Groups .....	619
5.26	Managing VRRP .....	619
5.26.1	VRRP Concepts .....	620
5.26.1.1	Static Routing vs. VRRP .....	620
5.26.1.2	VRRP Terminology .....	620
5.26.2	Viewing the Status of VRRP .....	623
5.26.3	Enabling/Disabling VRRP .....	623
5.26.4	Managing VRRP Trackers .....	624
5.26.4.1	Viewing a List of VRRP Trackers .....	625
5.26.4.2	Adding a VRRP Tracker .....	625
5.26.4.3	Deleting a VRRP Tracker .....	627
5.26.5	Managing VRRP Groups .....	627

5.26.5.1	Viewing a List of VRRP Groups .....	628
5.26.5.2	Adding a VRRP Group .....	628
5.26.5.3	Deleting a VRRP Group .....	629
5.26.6	Managing VRRP Instances .....	629
5.26.6.1	Viewing a List of VRRP Instances .....	629
5.26.6.2	Adding a VRRP Instance .....	630
5.26.6.3	Deleting a VRRP Instance .....	633
5.26.7	Managing VRRP Monitors .....	633
5.26.7.1	Viewing a List of VRRP Monitors .....	634
5.26.7.2	Adding a VRRP Monitor .....	634
5.26.7.3	Deleting a VRRP Monitor .....	635
5.26.8	Managing Track Scripts .....	636
5.26.8.1	Viewing a List of Track Scripts .....	636
5.26.8.2	Adding a Track Script .....	637
5.26.8.3	Deleting a Track Script .....	638
5.26.9	Managing Virtual IP Addresses .....	638
5.26.9.1	Viewing a List of Virtual IP Addresses .....	639
5.26.9.2	Adding a Virtual IP Address .....	639
5.26.9.3	Deleting a Virtual IP Address .....	640
5.27	Managing Link Failover Protection .....	640
5.27.1	Viewing the Link Failover Log .....	641
5.27.2	Viewing the Link Failover Status .....	641
5.27.3	Managing Link Failover Parameters .....	642
5.27.3.1	Viewing a List of Link Failover Parameters .....	643
5.27.3.2	Adding a Link Failover Parameter .....	643
5.27.3.3	Deleting a Link Failover Parameter .....	645
5.27.4	Managing Link Failover Backup Interfaces .....	646
5.27.4.1	Viewing a List of Link Failover Backup Interfaces .....	646
5.27.4.2	Adding a Link Failover Backup Interface .....	646
5.27.4.3	Deleting a Link Failover Backup Interface .....	648
5.27.5	Managing Link Failover Ping Targets .....	649
5.27.5.1	Viewing a List of Link Failover Ping Targets .....	649
5.27.5.2	Adding a Link Failover Ping Target .....	649
5.27.5.3	Deleting a Link Failover Ping target .....	650
5.27.6	Testing Link Failover .....	651
5.27.7	Canceling a Link Failover Test .....	652
5.28	Managing IPsec Tunnels .....	653
5.28.1	IPsec Tunneling Concepts .....	654
5.28.1.1	IPsec Modes .....	654
5.28.1.2	Supported Encryption Protocols .....	654

5.28.1.3	Public and Secret Key Cryptography .....	655
5.28.1.4	X509 Certificates .....	655
5.28.1.5	NAT Traversal .....	655
5.28.1.6	Remote IPsec Client Support .....	655
5.28.1.7	IPsec and Router Interfaces .....	656
5.28.2	Configuring IPsec Tunnels .....	656
5.28.3	Configuring Certificates and Keys .....	657
5.28.4	Viewing the IPsec Tunnel Status .....	658
5.28.5	Managing Pre-Shared Keys .....	659
5.28.5.1	Viewing a List of Pre-Shared Keys .....	659
5.28.5.2	Adding a Pre-Shared Key .....	659
5.28.5.3	Deleting a Pre-Shared Key .....	661
5.28.6	Managing Connections .....	661
5.28.6.1	Viewing a List of Connections .....	662
5.28.6.2	Adding a Connection .....	662
5.28.6.3	Configuring Dead Peer Detection .....	665
5.28.6.4	Deleting a Connection .....	666
5.28.7	Managing the Internet Key Exchange (IKE) Protocol .....	667
5.28.7.1	Viewing a List of IKE Algorithms .....	667
5.28.7.2	Adding an IKE Algorithm .....	668
5.28.7.3	Deleting an IKE Algorithm .....	669
5.28.8	Managing the Encapsulated Security Payload (ESP) Protocol .....	669
5.28.8.1	Configuring ESP Encryption .....	670
5.28.8.2	Viewing a List of ESP Algorithms .....	670
5.28.8.3	Adding ESP Algorithms .....	671
5.28.8.4	Deleting ESP Algorithms .....	672
5.28.9	Configuring the Connection Ends .....	672
5.28.10	Managing Private Subnets .....	676
5.28.10.1	Configuring Private Subnets for Connection Ends .....	676
5.28.10.2	Viewing a List of Addresses for Private Subnets .....	677
5.28.10.3	Adding an Address for a Private Subnet .....	677
5.28.10.4	Deleting an Address for a Private Subnet .....	678
5.29	Managing 6in4 and 4in6 Tunnels .....	678
5.29.1	Enabling/Disabling 6in4 or 4in6 Tunnels .....	679
5.29.2	Viewing a List of 6in4 or 4in6 Tunnels .....	679
5.29.3	Viewing the Status of 6in4/4in6 Tunnels .....	680
5.29.4	Adding a 6in4 or 4in6 Tunnel .....	680
5.29.5	Deleting a 6in4 or 4in6 Tunnel .....	681
5.30	Managing Layer 2 Tunnels .....	682
5.30.1	Viewing the Round Trip Time Statistics .....	683

5.30.2	Configuring L2TP Tunnels .....	684
5.30.3	Configuring L2TPv3 Tunnels .....	687
5.30.4	Configuring the Layer 2 Tunnel Daemon .....	693
5.30.5	Managing GOOSE Tunnels .....	694
5.30.5.1	Viewing the GOOSE Tunnel Statistics .....	695
5.30.5.2	Viewing a List of GOOSE Tunnels .....	696
5.30.5.3	Adding a GOOSE Tunnel .....	697
5.30.5.4	Deleting a GOOSE Tunnel .....	698
5.30.6	Managing Remote Daemons for GOOSE Tunnels .....	698
5.30.6.1	Viewing a List of Remote Daemons .....	699
5.30.6.2	Adding a Remote Daemon .....	699
5.30.6.3	Deleting a Remote Daemon .....	700
5.30.7	Managing Generic Tunnels .....	700
5.30.7.1	Viewing the Generic Tunnel Statistics .....	701
5.30.7.2	Viewing a List of Generic Tunnels .....	701
5.30.7.3	Adding a Generic Tunnel .....	702
5.30.7.4	Deleting a Generic Tunnel .....	703
5.30.8	Managing Remote Daemon IP Addresses for Generic Tunnels .....	704
5.30.8.1	Viewing a List of IP Addresses .....	704
5.30.8.2	Adding an IP Address .....	705
5.30.8.3	Deleting an IP Address .....	706
5.30.9	Managing Remote Daemon Egress Interfaces for Generic Tunnels .....	706
5.30.9.1	Viewing a List of Egress Interfaces .....	706
5.30.9.2	Adding an Egress Interface .....	707
5.30.9.3	Deleting an Egress Interface .....	708
5.30.10	Managing Ethernet Types for Generic Tunnels .....	708
5.30.10.1	Viewing a List of Ethernet Types .....	708
5.30.10.2	Adding an Ethernet Type .....	709
5.30.10.3	Deleting an Ethernet Type .....	710
5.31	Managing Generic Routing Encapsulation Tunnels .....	710
5.31.1	Viewing Statistics for GRE Tunnels .....	711
5.31.2	Viewing a List of GRE Tunnels .....	712
5.31.3	Adding a GRE Tunnel .....	712
5.31.4	Deleting a GRE Tunnel .....	715
5.32	Managing Layer 3 Switching .....	716
5.32.1	Layer 3 Switching Concepts .....	717
5.32.1.1	Layer 3 Switch Forwarding Table .....	717
5.32.1.2	Static Layer 3 Switching Rules .....	718
5.32.1.3	Dynamic Learning of Layer 3 Switching Rules .....	718
5.32.1.4	Layer 3 Switch ARP Table .....	719

5.32.1.5	Multicast Cross-VLAN Layer 2 Switching .....	719
5.32.1.6	Size of the Layer 3 Switch Forwarding Table .....	720
5.32.1.7	Interaction with the Firewall .....	720
5.32.2	Configuring Layer 3 Switching .....	720
5.32.3	Managing Static ARP Table Entries .....	722
5.32.3.1	Viewing a List of ARP Table Entries .....	722
5.32.3.2	Adding a Static ARP Table Entry .....	723
5.32.3.3	Deleting a Static ARP Table Entry .....	724
5.32.4	Viewing a Static and Dynamic ARP Table Summary .....	725
5.32.5	Viewing Routing Rules .....	726
5.32.6	Flushing Dynamic Hardware Routing Rules .....	727
5.33	Managing Classes of Service .....	728
5.33.1	Configuring Classes of Service .....	729
5.33.2	Managing Priority-to-CoS Mapping .....	729
5.33.2.1	Viewing a List of Priority-to-CoS Mapping Entries .....	730
5.33.2.2	Adding a Priority-to-CoS Mapping Entry .....	730
5.33.2.3	Deleting a Priority-to-CoS Mapping Entry .....	731
5.33.3	Managing DSCP-to-CoS Mapping .....	732
5.33.3.1	Viewing a List of DSCP-to-CoS Mapping Entries .....	732
5.33.3.2	Adding a DSCP-to-CoS Mapping Entry .....	733
5.33.3.3	Deleting a DSCP-to-CoS Mapping Entry .....	734
5.34	Managing MAC Addresses .....	735
5.34.1	Viewing a Dynamic List of MAC Addresses .....	735
5.34.2	Purging the Dynamic MAC Address List .....	736
5.34.3	Configuring MAC Address Learning Options .....	737
5.34.4	Managing Static MAC Addresses .....	738
5.34.4.1	Viewing a List of Static MAC Addresses .....	739
5.34.4.2	Adding a Static MAC Address .....	739
5.34.4.3	Deleting a Static MAC Address .....	741
5.35	Managing Spanning Tree Protocol .....	741
5.35.1	RSTP Operation .....	742
5.35.1.1	RSTP States and Roles .....	742
5.35.1.2	Edge Ports .....	744
5.35.1.3	Point-to-Point and Multipoint Links .....	744
5.35.1.4	Path and Port Costs .....	744
5.35.1.5	Bridge Diameter .....	745
5.35.1.6	eRSTP .....	745
5.35.1.7	Fast Root Failover .....	746
5.35.2	RSTP Applications .....	747
5.35.2.1	RSTP in Structured Wiring Configurations .....	747

5.35.2.2	RSTP in Ring Backbone Configurations .....	749
5.35.2.3	RSTP Port Redundancy .....	751
5.35.3	MSTP Operation .....	751
5.35.3.1	MSTP Regions and Interoperability .....	752
5.35.3.2	MSTP Bridge and Port Roles .....	753
5.35.3.3	Benefits of MSTP .....	754
5.35.3.4	Implementing MSTP on a Bridged Network .....	755
5.35.4	Configuring STP Globally .....	755
5.35.5	Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces .....	760
5.35.6	Managing Multiple Spanning Tree Instances Globally .....	763
5.35.6.1	Viewing Statistics for Multiple Spanning Tree Instances .....	763
5.35.6.2	Viewing a List of Multiple Spanning Tree Instances .....	765
5.35.6.3	Adding a Multiple Spanning Tree Instance .....	765
5.35.6.4	Deleting a Multiple Spanning Tree Instance .....	767
5.35.7	Managing Multiple Spanning Tree Instances Per-Port .....	767
5.35.7.1	Viewing Per-Port Multiple Spanning Tree Instance Statistics .....	768
5.35.7.2	Viewing a List of Per-Port Multiple Spanning Tree Instances .....	769
5.35.7.3	Adding a Port-Specific Multiple Spanning Tree Instance .....	769
5.35.7.4	Deleting a Port-Specific Multiple Spanning Tree Instances .....	771
5.35.8	Viewing the Status of RSTP .....	772
5.35.9	Viewing RSTP Per-Port Statistics .....	775
5.35.10	Clearing Spanning Tree Protocol Statistics .....	776
5.36	Managing VLANs .....	777
5.36.1	VLAN Concepts .....	777
5.36.1.1	Tagged vs. Untagged Frames .....	778
5.36.1.2	Native VLAN .....	778
5.36.1.3	Edge and Trunk Port Types .....	778
5.36.1.4	Ingress and Egress Rules .....	779
5.36.1.5	Forbidden Ports List .....	779
5.36.1.6	VLAN-Aware Mode of Operation .....	779
5.36.1.7	GARP VLAN Registration Protocol (GVRP) .....	780
5.36.1.8	PVLAN Edge .....	781
5.36.1.9	VLAN Advantages .....	781
5.36.2	Configuring the Internal VLAN Range .....	783
5.36.3	Managing VLANs for Switched Ethernet Ports .....	784
5.36.3.1	Viewing VLAN Assignments for Switched Ethernet Ports .....	785
5.36.3.2	Configuring VLANs for Switch Ethernet Ports .....	785
5.36.4	Managing Static VLANs .....	786
5.36.4.1	Viewing a List of Static VLANs .....	787
5.36.4.2	Adding a Static VLAN .....	787



5.36.4.3	Deleting a Static VLAN .....	789
5.36.5	Managing Forbidden Ports .....	789
5.36.5.1	Viewing a List of Forbidden Ports .....	789
5.36.5.2	Adding a Forbidden Port .....	790
5.36.5.3	Deleting a Forbidden Port .....	791
5.36.6	Managing VLANs for Virtual Switches .....	791
5.36.6.1	Viewing a List of Virtual Switch VLANs .....	791
5.36.6.2	Adding a Virtual Switch VLAN .....	792
5.36.6.3	Deleting a Virtual Switch VLAN .....	793
5.36.7	Managing VLANs for Routable-Only Ethernet Ports .....	794
5.36.7.1	Viewing a List of VLANs for Routable Ethernet Ports .....	794
5.36.7.2	Adding a VLAN to a Routable Ethernet Port .....	794
5.36.7.3	Deleting a VLAN for a Routable Ethernet Port .....	796
5.37	Managing Network Discovery and LLDP .....	796
5.37.1	Configuring LLDP .....	797
5.37.2	Viewing Global Statistics and Advertised System Information .....	799
5.37.3	Viewing Statistics for LLDP Neighbors .....	801
5.37.4	Viewing Statistics for LLDP Ports .....	803
5.38	Managing Traffic Control .....	805
5.38.1	Enabling and Configuring Traffic Control .....	805
5.38.2	Managing Traffic Control Interfaces .....	807
5.38.2.1	Viewing a List of Traffic Control Interfaces .....	807
5.38.2.2	Adding a Traffic Control Interface .....	808
5.38.2.3	Deleting a Traffic Control Interface .....	810
5.38.3	Managing Traffic Control Priorities .....	810
5.38.3.1	Viewing a List of Traffic Control Priorities .....	811
5.38.3.2	Adding a Traffic Control Priority .....	811
5.38.3.3	Deleting a Traffic Control Priority .....	813
5.38.4	Managing Traffic Control Classes .....	814
5.38.4.1	Viewing a List of Traffic Control Classes .....	815
5.38.4.2	Adding a Traffic Control Class .....	815
5.38.4.3	Deleting a Traffic Control Class .....	819
5.38.5	Managing Traffic Control Devices .....	820
5.38.5.1	Viewing a List of Traffic Control Devices .....	820
5.38.5.2	Adding a Traffic Control Device .....	821
5.38.5.3	Deleting a Traffic Control Device .....	823
5.38.6	Managing Traffic Control Rules .....	823
5.38.6.1	Viewing a List of Traffic Control Rules .....	824
5.38.6.2	Adding a Traffic Control Rule .....	824
5.38.6.3	Configuring QoS Marking .....	827

5.38.6.4	Deleting aTraffic Control Rule .....	831
5.38.7	Managing QoS Mapping for VLANs .....	832
5.38.7.1	Viewing a List of QoS Maps .....	832
5.38.7.2	Adding a QoS Map .....	833
5.38.7.3	Deleting a QoS Map .....	835
5.38.8	Managing Egress Markers for QoS Maps .....	835
5.38.8.1	Viewing a List of Egress Marks .....	836
5.38.8.2	Adding an Egress Mark .....	836
5.38.8.3	Deleting an Egress Mark .....	837
5.38.9	Viewing QoS Statistics .....	838
5.39	Managing IP Addresses for Routable Interfaces .....	839
5.39.1	Configuring Costing for Routable Interfaces .....	840
5.39.2	Viewing Statistics for Routable Interfaces .....	841
5.39.3	Managing IPv4 Addresses .....	844
5.39.3.1	Viewing a List of IPv4 Addresses .....	844
5.39.3.2	Adding an IPv4 Address .....	844
5.39.3.3	Deleting an IPv4 Address .....	846
5.39.4	Configuring IPv6 Neighbor Discovery .....	846
5.39.5	Managing IPv6 Network Prefixes .....	850
5.39.5.1	Adding an IPv6 Network Prefix .....	850
5.39.5.2	Deleting an IPv6 Network Prefix .....	852
5.39.6	Managing IPv6 Addresses .....	852
5.39.6.1	Viewing a List of IPv6 Addresses .....	852
5.39.6.2	Adding an IPv6 Address .....	853
5.39.6.3	Deleting an IPv6 Address .....	854
5.40	Managing MPLS .....	854
5.40.1	Viewing the Status of IP Binding .....	854
5.40.2	Viewing the Status of the Forwarding Table .....	855
5.40.3	Enabling/Disabling MPLS Routing .....	856
5.40.4	Managing the MPLS Interfaces .....	857
5.40.4.1	Viewing the Status of MPLS Interfaces .....	857
5.40.4.2	Viewing a List of MPLS Interfaces .....	857
5.40.4.3	Enabling/Disabling an MPLS Interface .....	858
5.40.5	Managing Static Label Binding .....	859
5.40.5.1	Viewing the Status of Static Label Binding .....	859
5.40.5.2	Viewing a List of Static Labels .....	859
5.40.5.3	Adding a Static Label .....	860
5.40.5.4	Deleting a Static Label .....	861
5.40.6	Managing Static Cross-Connects .....	862
5.40.6.1	Viewing the Status of Static Cross-Connects .....	862

5.40.6.2	Viewing a List of Static Cross-Connects .....	863
5.40.6.3	Adding a Static Cross-Connect .....	863
5.40.6.4	Deleting a Static Cross-Connect .....	865
5.40.7	Managing LDP .....	865
5.40.7.1	Viewing the Status of LDP Binding .....	866
5.40.7.2	Viewing the Status of the LDP Discovery Interfaces .....	867
5.40.7.3	Viewing the Status of the LDP Neighbor Local Node Information .....	868
5.40.7.4	Viewing the Status of the LDP Neighbor Connection Information .....	868
5.40.7.5	Viewing the Status of the LDP Neighbor Discovery Information .....	869
5.40.7.6	Configuring LDP .....	869
5.40.7.7	Configuring Neighbor Discovery .....	870
5.40.7.8	Viewing a List of LDP Interfaces .....	871
5.40.7.9	Enabling/Disabling an LDP Interface .....	872
 Chapter 6		
<b>Troubleshooting .....</b>		<b>873</b>
6.1	Feature Keys .....	873
6.2	Ethernet Ports .....	873
6.3	Multicast Filtering .....	874
6.4	Spanning Tree .....	875
6.5	VLANs .....	876



# Preface

This guide describes the Web-based user interface for RUGGEDCOM ROX II v2.9 running on the RUGGEDCOM RX5000/MX5000/MX5000RE. It contains instructions and guidelines on how to use the software, as well as some general theory.

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

## 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.*

## Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM RX5000 Installation Guide*
- *RUGGEDCOM RX5000 Data Sheet*

# System Requirements

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

- Must have one of the following Web browsers installed:
  - Microsoft Internet Explorer 8.0 or higher
  - Mozilla Firefox
  - Google Chrome
  - Iceweasel/IceCat (Linux Only)
- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM RX5000
- The ability to configure an IP address and netmask on the computer's Ethernet interface

## Accessing Documentation

The latest user documentation for RUGGEDCOM ROX II v2.9 is available online at [www.siemens.com/ruggedcom](http://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 [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom) or contact a Siemens sales representative.

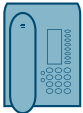
# Customer Support

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:



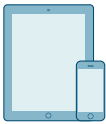
## Online

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®) v2.9 Web Interface User Guide for the RUGGEDCOM RX5000/MX5000/MX5000RE. This document details how to configure the RX5000 via the RUGGEDCOM ROX II Web interface. RUGGEDCOM ROX II also features a Command Line Interface (CLI), which is described in a separate Web Interface User Guide.

**IMPORTANT!**

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

The following sections provide more detail about RUGGEDCOM ROX II:

- [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 1.1

# Features and Benefits

Feature support in RUGGEDCOM ROX II is driven by feature keys that unlock feature levels. For more information about feature keys, refer to [Section 1.2, “Feature Keys”](#).

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

- **Cyber Security**

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

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

- **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. SNMP versions supported by RUGGEDCOM ROX II are v1, v2c and v3. SNMPv3 in particular 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 RUGGEDCOM ROX II NETCONF Reference Guide* available on [www.siemens.com/ruggedcom](http://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 make setup a breeze. RUGGEDCOM ROX II presents a common look and feel and standardized configuration process, allowing easy migration to other RUGGEDCOM managed products.

- **Command Line Interface (CLI)**

A command line interface used in conjunction with remote shell to automate data retrieval, configuration updates, and firmware upgrades. A powerful Telecom Standard style Command Line Interface (CLI) allows expert users the ability to selectively retrieve or manipulate any parameters the device has to offer.

- **Link Backup**

Link backup provides an easily configured means of raising a backup link upon the failure of a designated main link. The main and backup links can be Ethernet, Cellular, T1/E1, DDS or T3. The feature can back up to multiple remote locations, managing multiple main: backup link relationships. The feature can also back up a permanent high speed WAN link to a permanent low speed WAN link and can be used to migrate the default route from the main to the backup link.

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

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

- **BGP (Border Gateway Protocol)**

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

- **RIP (Routing Information Protocol)**

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

- **IS-IS (Intermediate System - Intermediate System)**

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

- **Brute Force Attack Prevention**

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

- **USB Mass Storage**

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

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

**IMPORTANT!**

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

**NOTE**

*Only one partition is supported on the USB Mass Storage drive.*

**NOTE**

*Only USB Mass Storage drives with one partition are supported.*

- **Hot Swapping Modules**

Power Modules (PM) and Line Modules (LM) can be safely replaced with modules of exactly the same type while the device is running, with minimal disruption to the network. The device only needs to be restarted after swapping a module with a different type, such as an Ethernet module with a serial module.

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

**NOTE**

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

**NOTE**

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

## 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.

Three feature keys are currently available: L2STD, L3STD and L3SEC. By default, each new RX5000/MX5000/MX5000RE is ordered with a base feature key, which is permanently installed on the device. Additional feature keys can be installed on the compact flash card or placed on a USB Mass Storage device, 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 (L2STD)	Layer 3 Standard Edition (L3STD)	Layer 3 Security Edition (L3SEC)
VLANs (802.1Q)	✓	✓	✓
QoS (802.1p)	✓	✓	✓
MSTP (802.1Q-2005) <sup>a</sup>	✓	✓	✓
RSTP	✓	✓	✓
eRSTP™	✓	✓	✓
SNTP	✓	✓	✓
L2TPv2 and L2TPv3	✓	✓	✓
Port Rate Limiting	✓	✓	✓
Broadcast Storm Filtering	✓	✓	✓
Port Mirroring	✓	✓	✓
SNMP v1/v2/v3	✓	✓	✓
RMON	✓	✓	✓
CLI	✓	✓	✓

Feature	Feature Key		
	Layer 2 Standard Edition (L2STD)	Layer 3 Standard Edition (L3STD)	Layer 3 Security Edition (L3SEC)
HTML User Interface	✓	✓	✓
MPLS	✗	✓	✓
DHCP	✗	✓	✓
VRRPv2 and VRRPv3	✗	✓	✓
PIM-SM	✗	✓	✓
Firewall	✗	✓	✓
OSPF	✗	✓	✓
BGP	✗	✓	✓
RIP v1/v2	✗	✓	✓
IS-IS	✗	✓	✓
Traffic Prioritization	✗	✓	✓
VPN	✗	✗	✓
IPSec	✗	✗	✓
Virtualization	✓	✓	✓

<sup>a</sup> Formerly 802.1s

For information about installing and viewing the contents of feature keys, refer to [Section 3.13, “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 such as *password1*, *123456789*, *abcdefgh*, etc. For more information about creating strong passwords, refer to the password requirements in [Section 4.10, “Managing Passwords and Passphrases”](#).
- 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 authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.
- 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.

#### Physical/Remote Access

- It is highly recommended to enable Brute Force Attack (BFA) protection to prevent a third-party from obtaining unauthorized access to the device. For more information, refer to [Section 5.6, “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.
- The default and auto-generated SSL certificates are self-signed. It is recommended to use an SSL certificate that is either signed by a trusted third-party Certificate Authority (CA) or by an organization's own CA. For more information, refer to [Generating SSH Keys and SSL Certificates for ROS and ROX Using Windows](http://w3.siemens.com/mcms/industrial-communication/Documents/AN22_Application-Note_EN.pdf) [http://w3.siemens.com/mcms/industrial-communication/Documents/AN22\_Application-Note\_EN.pdf].
- 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.
- 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.
- 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 5.11, “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 5.16, “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 Web Interface 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 3.9, “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 5.16, “Managing Firewalls”](#) and [Section 5.28, “Managing IPsec Tunnels”](#).
- 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 Telnet and RSTP, were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Prevent access to external, untrusted Web pages while accessing the device via a Web browser. This can assist in preventing potential security threats, such as session hijacking.
- Make sure the device is fully decommissioned before taking the device out of service. For more information, refer to [Section 3.7, “Decommissioning the Device”](#).
- Configure port security features on access ports to prevent a third-party from launching various attacks that can harm the network or device. For more information, refer to [Section 3.18.3, “Configuring Port Security”](#).

#### 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](http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx) [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] or the [ProductCERT Security Advisories website](http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm) [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. Use strong passwords with this feature. For more information about creating strong passwords, refer to the password requirements in [Section 4.10, “Managing Passwords and Passphrases”](#).



**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

Services	Port Number	Port Open	Port Default	Access Authorized
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

## 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 read/write/execute 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	No	No	
/admin/rox-imaging	R/U	No	No	
/admin/authentication	R/U	No	No	
/admin/authentication/password-complexity	R/U	R	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	

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
/admin/webui	R/U	R/U	No	
/admin/scheduler	C/R/U	No	No	
/admin/contact	R/U	R/U	No	
/admin/hostname	R/U	R/U	No	
/admin/location	R/U	R/U	No	
/admin/session-limits	R/U	R/U	No	
/admin/session-security	R/U	R/U	No	
/admin/sftp	R/U	R/U	No	
/admin/time (status)	R	R	No	
/admin/switch-config (status)	R/U	R	No	
/admin/system	R/U	R/U	No	
/admin/sytem-name	R/U	R/U	No	
/admin/timezone	R/U	C/R/U	No	
/admin/clear-all-alarms (action)	E	C/R/U	No	
/admin/backup-files (action)	E/R/U	No	No	
/admin/delete-all-ssh-known-hosts (action)	E	E	No	
/admin/delete-logs (action)	E	No	No	
/admin/delete-ssh-known-host (action)	E	E	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	E	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	R/U	R	
/chassis/line-module-list	R/U	R	R	
/chassis/line-modules/line-module	R/U	R/U	R	
/interfaces	R	C/R/U	R	
/interface	C/R/U	R/U	R	
/routing	C/R/U	C/R/U	R	

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

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
wizard	E	No	No	

## Section 1.6

## Removable Memory

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

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

**IMPORTANT!**

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

**NOTE**

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

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



# 2

## Using RUGGEDCOM ROX II

This chapter describes how to use the RUGGEDCOM ROX II interface. It describes the following tasks:

- [Section 2.1, “Connecting to RUGGEDCOM ROX II”](#)
- [Section 2.2, “Default User Names and Passwords”](#)
- [Section 2.3, “Logging In”](#)
- [Section 2.4, “Logging Out”](#)
- [Section 2.5, “Navigating the Interface”](#)
- [Section 2.6, “Using Network Utilities”](#)
- [Section 2.7, “Using the Command Line Interface”](#)

### Section 2.1

## Connecting to RUGGEDCOM ROX II

The following describes the various methods for connecting the device:

- [Section 2.1.1, “Connecting Directly”](#)
- [Section 2.1.2, “Connecting Through the Network”](#)

### Section 2.1.1

## Connecting Directly

RUGGEDCOM ROX II can be accessed through a direct serial or Ethernet connection.

### » Using the RS-232 Serial Console Port

To establish a serial connection to the device, refer to the *RUGGEDCOM ROX II v2.9 CLI User Guide*.

### » Using an Ethernet Port

To establish a direct Ethernet connection to the device, do the following:

1. Connect a serial terminal or a computer running terminal emulation software to either the MGMT (Management) port or any other RJ-45 Ethernet port on the device.

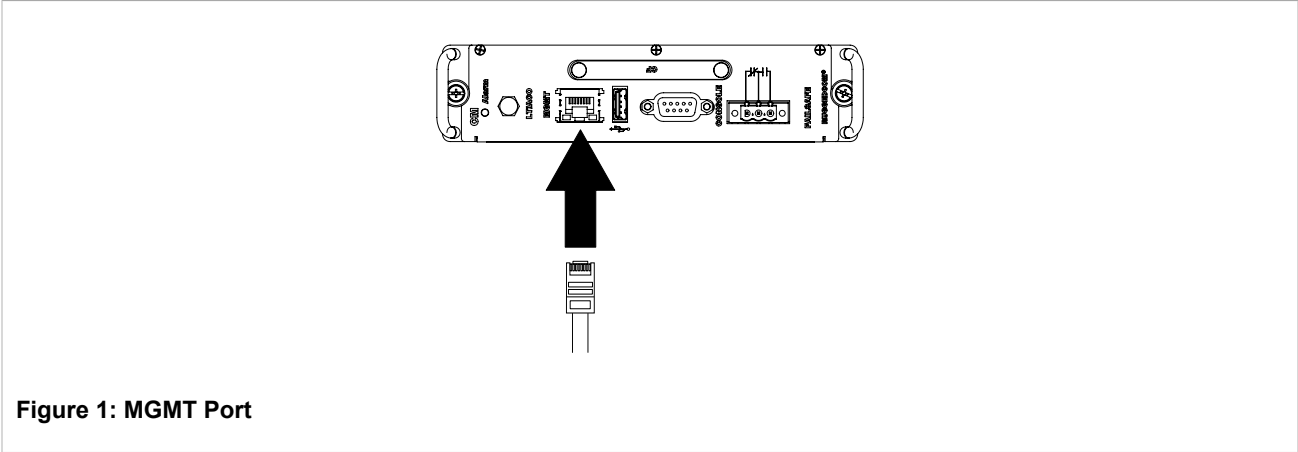


Figure 1: MGMT Port

2. Configure the IP address range and subnet for the serial terminal or computer's Ethernet port. The range is typically the IP address for the device's IP interface plus one, ending at \*.\*\*.254.  
By default, the RUGGEDCOM RX5000 has a different IP address and subnet configured for two types of IP interfaces, both of which are mapped to one or more physical ports:

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

For example, if the serial terminal or computer is connected to the device's MGMT port, configure the serial terminal or computer's Ethernet port with an IP address in the range of 192.168.1.3 to 192.168.1.254. Connect to the device using the IP address 192.168.1.2, the address of the MGMT interface.

3. Launch the SSH client on the computer and connect to `admin@{ipaddress}`, where `{ipaddress}` is the IP address for the MGMT port. The login prompt appears:  

```
Using username "admin".
admin@192.168.0.2's password:
```
4. Log in to RUGGEDCOM ROX II. For more information about logging in to RUGGEDCOM ROX II, refer to [Section 2.3, "Logging In"](#).

Section 2.1.2

# Connecting Through the Network

To connect to RUGGEDCOM ROX II through the network, do the following:

1. On the workstation being used to connect to the device, configure the Ethernet port to use an IP address falling within the subnet of the device.  
By default, the RUGGEDCOM RX5000 has a different IP address and subnet configured for two types of IP interfaces, both of which are mapped to one or more physical ports:

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



For example, if the device is connected via the MGMT port, configure the computer's Ethernet port with an IP address in the range of 192.168.1.3 to 192.168.1.254. Connect to the device using the IP address 192.168.1.2, the address of the MGMT interface.

2. Open a Web browser. For a list of recommended Web browsers, refer to [the section called "System Requirements"](#).

**IMPORTANT!**

*Upon connecting to the device, some Web browsers may report that the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.*

3. In the address bar, type the IP address for the device. For example, to access the device using its factory default IP address, type `https://192.168.0.2` and press **Enter**. Once the connection is established, the login screen for the Web interface appears.

For more information about logging in to RUGGEDCOM ROX II, refer to [Section 2.3, "Logging In"](#).

## Section 2.2

## 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 4.10, "Managing Passwords and Passphrases"](#).*

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

## Section 2.3

## Logging In

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

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



**Figure 2: RUGGEDCOM ROX II Log In Form**

1. Username Box   2. Password Box   3. Submit Button



**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 4.9.2, “Adding a User”](#).*

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



**NOTE**

*If a unique password/passphrase has not been configured, use the factory default password. For more information, refer to [Section 2.2, “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 5.6, “Enabling/Disabling Brute Force Attack Protection”](#).*

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

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

Section 2.4

## Logging Out

To log out of the device, click the Logout link in the toolbar.



**Figure 3: Logout**

1. Logout Link

## Section 2.5

# Navigating the Interface

The following sections describe features of the Web interface:

- [Section 2.5.1, “Menus”](#)
- [Section 2.5.2, “Modes”](#)
- [Section 2.5.3, “Edit Toolbar”](#)
- [Section 2.5.4, “Using the Navigation Menu”](#)
- [Section 2.5.5, “Icons”](#)
- [Section 2.5.6, “Common Controls”](#)

## Section 2.5.1

# Menus

The toolbar at the top of the RUGGEDCOM ROX II interface allows access to two separate menus: **Configure Running** and **Tools**.



**Figure 4: Toolbar**

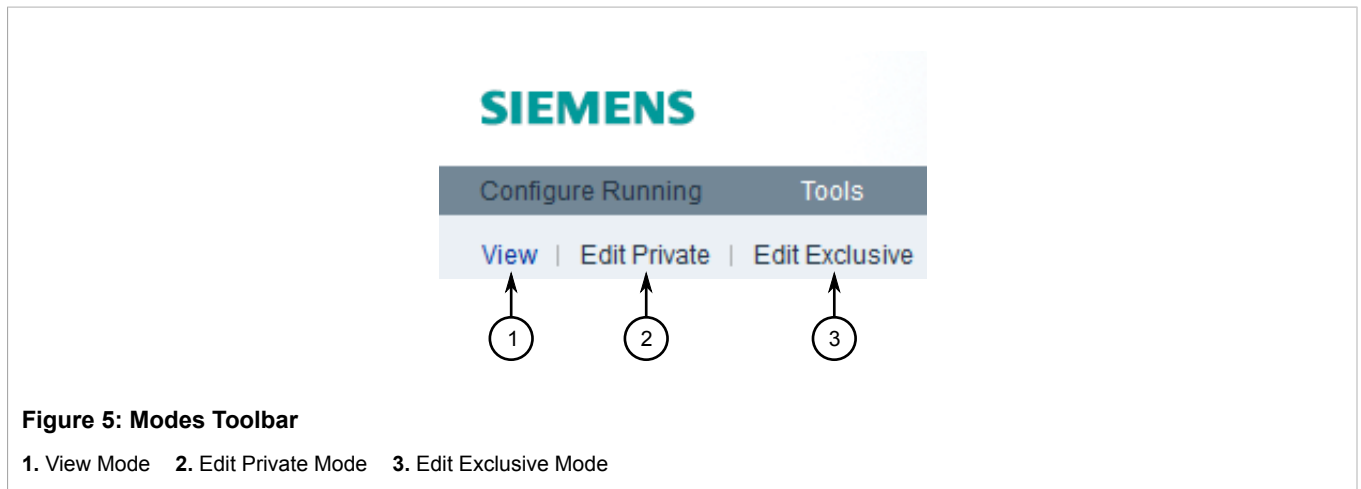
1. Configure Running Menu    2. Tools Menu

- **Configure Running**  
Click the **Configure Running** link to access the main RUGGEDCOM ROX II interface.
- **Tools**  
Click the **Tools** link to access various tools, such as a built-in CLI, system/network logs, network utilities and administrative controls.

## Section 2.5.2

# Modes

There are three modes available in RUGGEDCOM ROX II. The modes can be selected from the toolbar below the tabs on the **Configure Running** page.



### IMPORTANT!

Switching from either of the edit modes to **View** mode does not close the current configuration session. A configuration session can only be closed by pressing **Exit Transaction** on the edit toolbar.

## >> View Mode

In **View** mode, users can view parameter settings, logs, graphs, and the status of each connected device. Changes to RUGGEDCOM ROX II are not permitted.

## >> Edit Private Mode

**Edit Private** mode 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.

## >> Edit Exclusive Mode

**Edit Exclusive** mode is similar to **Edit Private** mode, except all other users are blocked from committing their changes until the user using **Edit Exclusive** mode exits. Only one Operator or Admin user can use **Edit Exclusive** mode at a time per device.

In **Edit Exclusive** mode, a dialog box will appear whenever a user attempts to commit configuration changes asking for 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.

To cancel a commit before the time elapses and discard the changes, click **Abort Commit**.

To permanently commit the changes, click **Commit** before the time elapses.



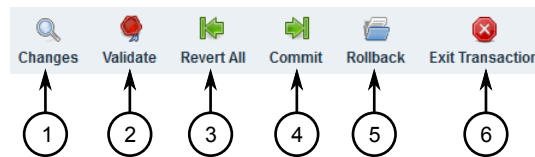
### IMPORTANT!

*Always log out of **Edit Exclusive** 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 2.5.3







## Edit Toolbar

The edit toolbar appears in the **Edit Private** and **Edit Exclusive** modes. The controls on the toolbar allow users to list, validate, revert, commit and abort changes made during the editing session.



**Figure 6: Edit Toolbar**

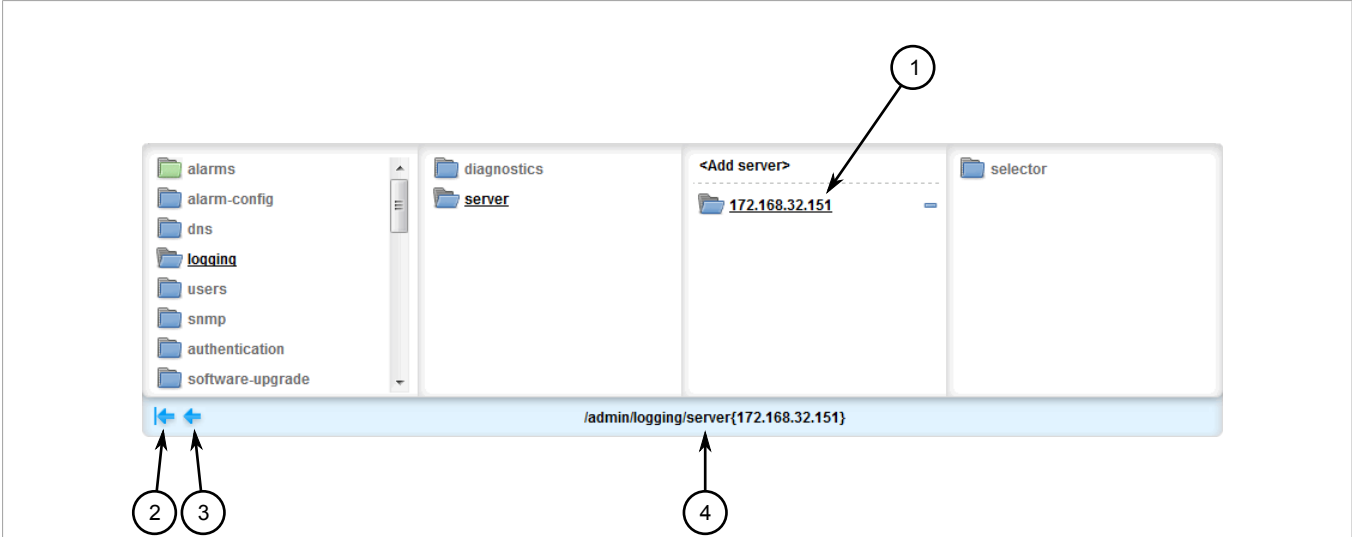
1. Changes Button   2. Validate Button   3. Revert All Button   4. Commit Button   5. Rollback Button   6. Exit Transaction Button

Control	Description
 <b>Changes</b>	Present a summary of all pending changes.
 <b>Validate</b>	Automatically check the validity of pending changes.
 <b>Revert All</b>	Abort all pending changes.
 <b>Commit</b>	Commit all pending changes.
 <b>Rollback</b>	Present a list of change sets made to date, with an option to revert a selected set of changes.
 <b>Exit Transaction</b>	Exit from configuration editing mode. All pending changes will be discarded.

#### Section 2.5.4

## Using the Navigation Menu

The navigation menu consists of four columns, each listing the contents of the node selected in the adjacent column to the left. The path to the selected node is displayed at the bottom of the navigation menu (e.g. /admin/authentication).






**Figure 7: Navigation Menu**

1. Selected Node    2. Home Button    3. Previous Button    4. Path to Current Node

Tables or configuration forms specific to the selected node appear below the navigation menu.

As the user navigates beyond four levels within the RUGGEDCOM ROX II data structure, the columns shift left. To shift the columns right, click the **Previous** arrow. To return to the top-level of the menu, click the **Home** arrow.

The following icons appear in the navigation menu:

	Folder icons represent nodes under which forms or additional nodes are located. Click on a node to open the next menu level and display any associated tables or forms.
	A blue folder icon represents a configuration node, whereas a green folder icon represents a status node that provides up-to-date information about the device and the network.
	The gear icon represents an action node. Click on an action node to perform a specific task or function. Parameters may need to be configured.

Section 2.5.5

# Icons

Icons appear in the title bar of each table or form in RUGGEDCOM ROX II to indicate the information type.

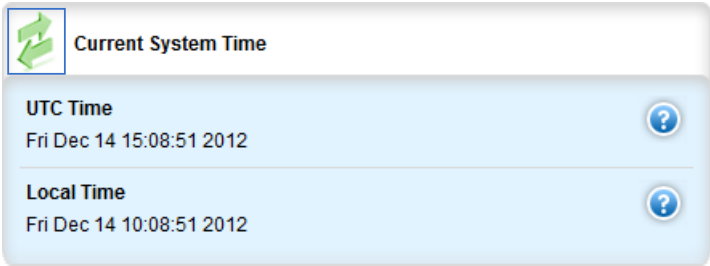








Figure 8: Icon In a Form


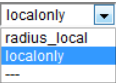
The following icons appear in RUGGEDCOM ROX II:


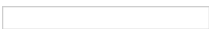



Icon	Information Type
	Key setting
	Global setting
	Operational data
	Configuration data
	Input data
	Action

Section 2.5.6

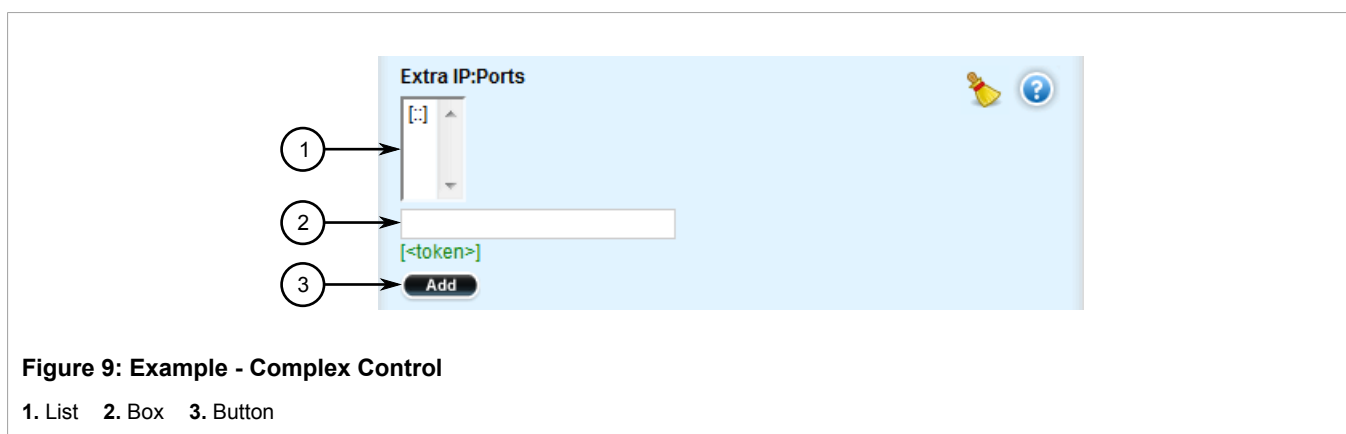
Common Controls

The following are common controls that can be found in the RUGGEDCOM ROX II Web interface.

	<b>Check Box</b> Click a check box to select or enable an option. Clear the check box to de-select or disable the option.
	<b>List</b> Select a value from a list.

	<b>Button</b> Click the button to perform an action. The action to be performed (e.g. add, perform, cancel, etc.) is written on the button itself.
	<b>Box</b> Type parameter values in text boxes.
	<b>Paper and Pencil</b> The paper and pencil icon represents a configurable parameter value. Click this icon to convert it to a box and change the current value.
	<b>Help</b> Click the Help icon to display a description of the parameter and its usage.
	<b>Brush</b> Click the Brush icon to clear the current parameter value.

Some controls are used in combination for complex parameter configurations. For example, the following parameter combines a list, box and button, allowing users to enter multiple values. Users enter a single value in the box and then click the **Add** button to add the value to the list.



## Section 2.6

# Using Network Utilities

The following sections describe how to use the built-in RUGGEDCOM ROX II network utilities:

- [Section 2.6.1, “Pinging a Host”](#)
- [Section 2.6.2, “Dumping Raw Data to a Terminal or File”](#)
- [Section 2.6.3, “Tracing the Route to a Remote Host”](#)
- [Section 2.6.4, “Pinging an IPv4 Address Using MPLS Protocols”](#)
- [Section 2.6.5, “Tracing the Route of an IPv4 Address Using MPLS Protocols”](#)

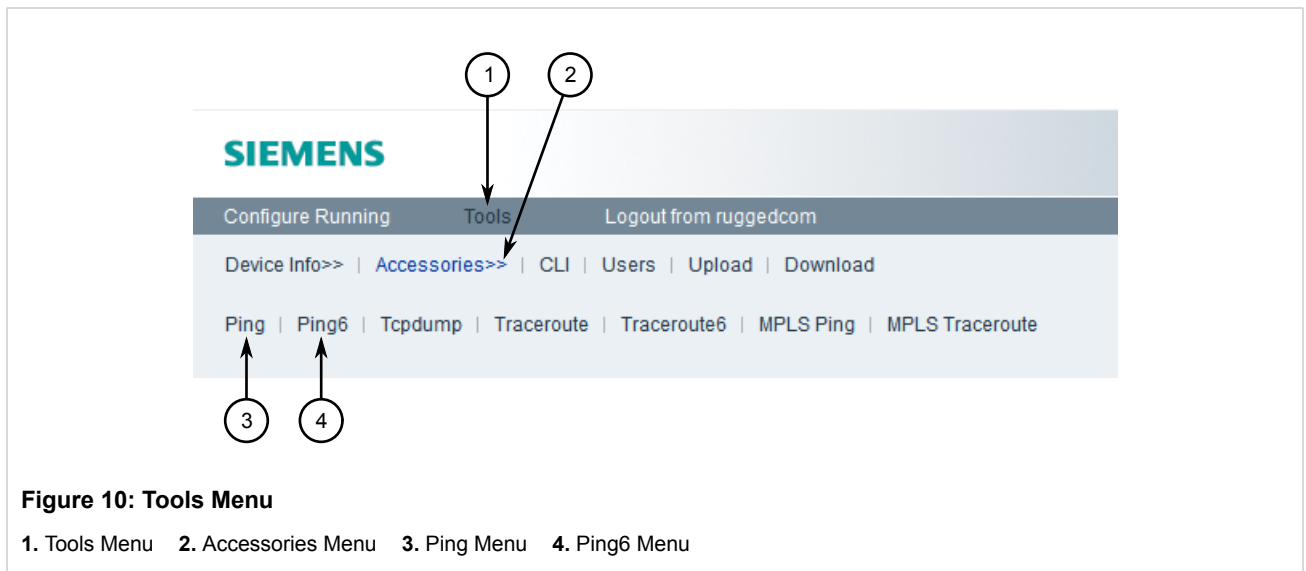
## Section 2.6.1

# Pinging a Host

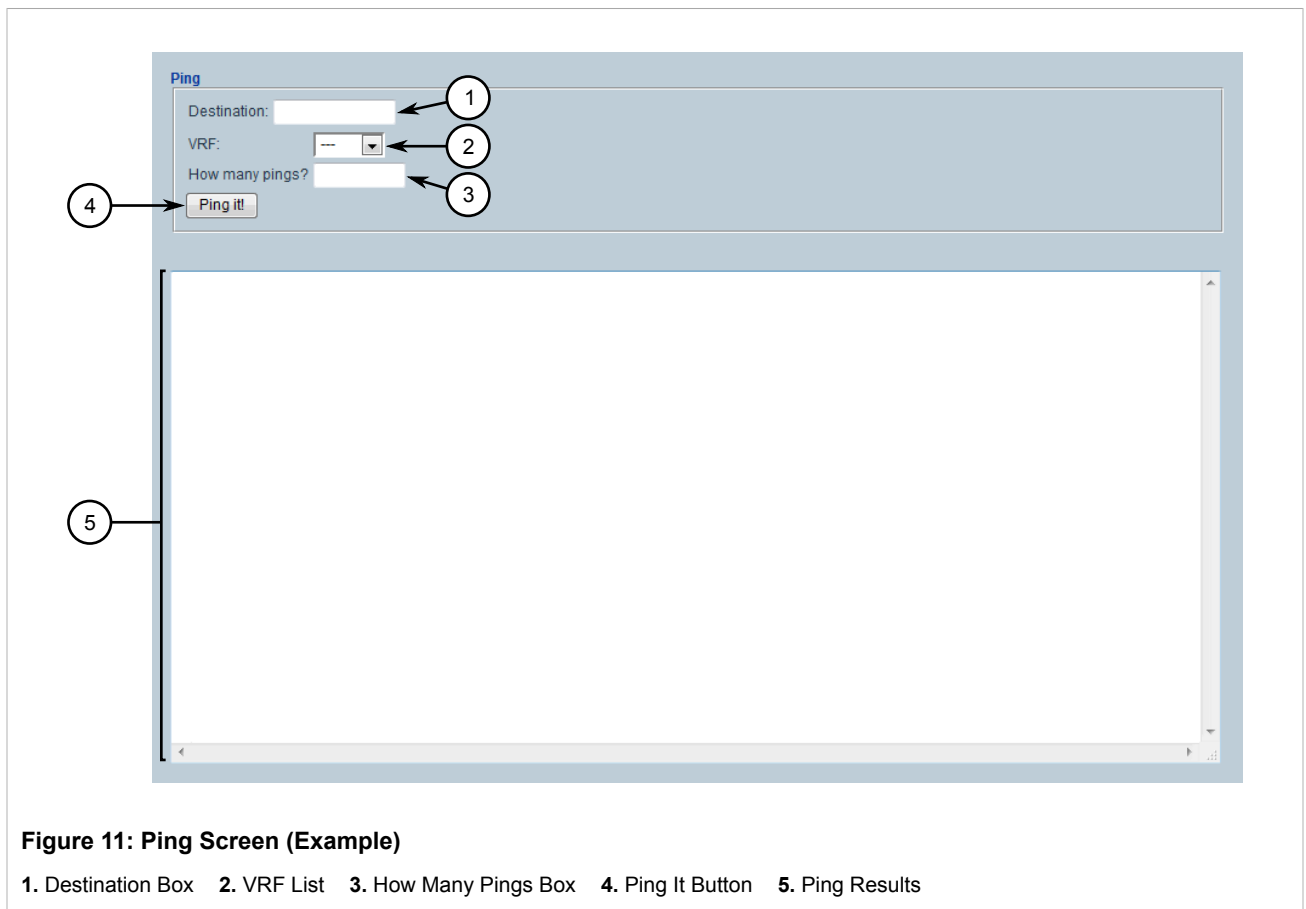
To ping a host, do the following:



1. Select the **Tools** menu and click **Accessories**.



2. Depending on the host's IP address, click **Ping** if the host has an IPv4 address, or **Ping6** if the host has an IPv6 address. The **Ping** screen appears.



3. Configure the following parameters as required:

Parameter	Description
Destination	The IP address of the host.
VRF	The target VRF. Only required when pinging VRF routes.
How Many Pings	The number of ping attempts.

4. Click **Ping It**. The results of the ping action are displayed below.

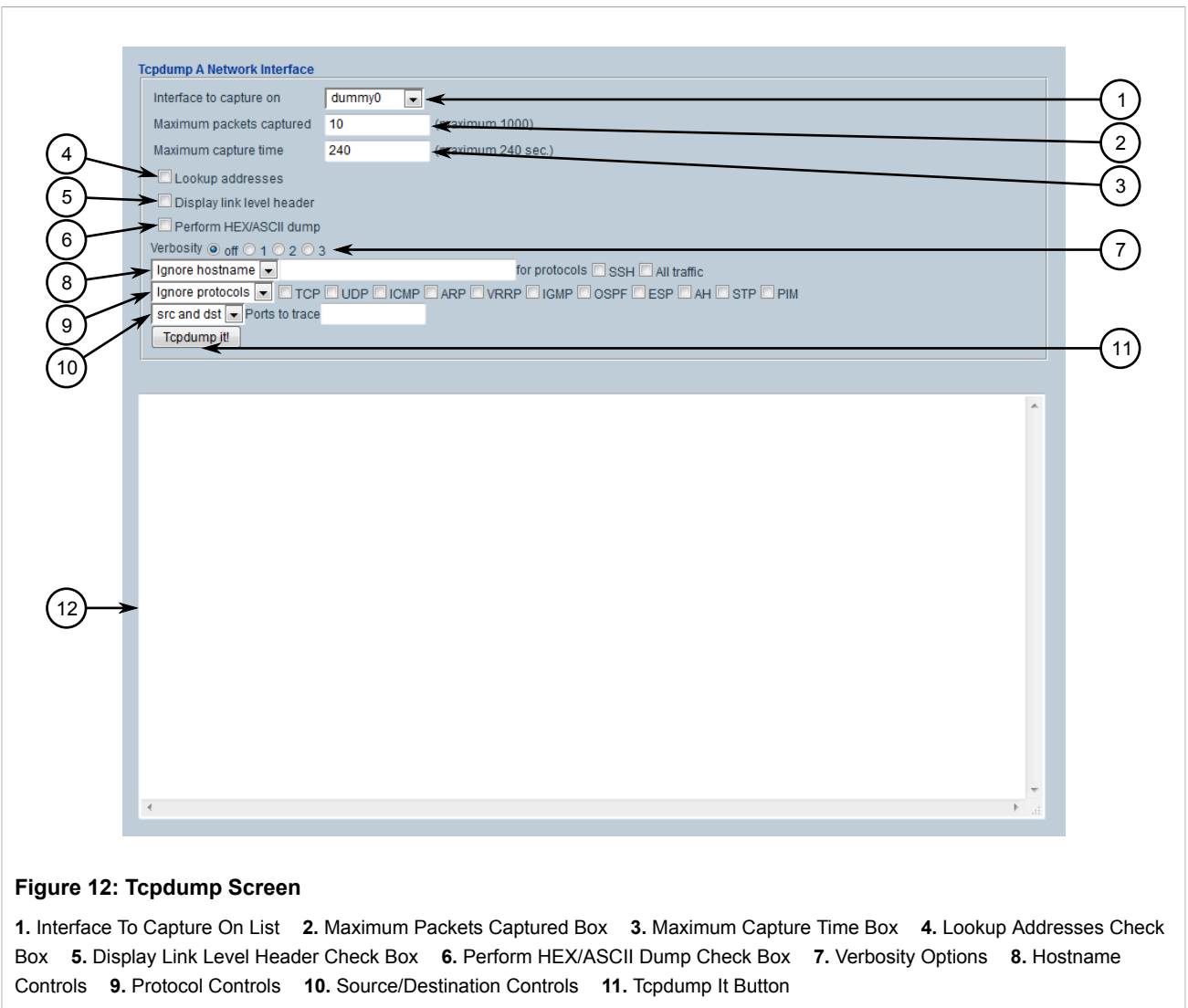
#### Section 2.6.2

## Dumping Raw Data to a Terminal or File

Tcpdump is a packet analyzer for TCP/IP and other packets. It can be used to dump raw data to a terminal or file.

To dump raw data to a terminal or file, do the following:

1. Select the **Tools** menu and click **Accessories**.
2. Click **Tcpdump**. The **Tcpdump** screen appears.



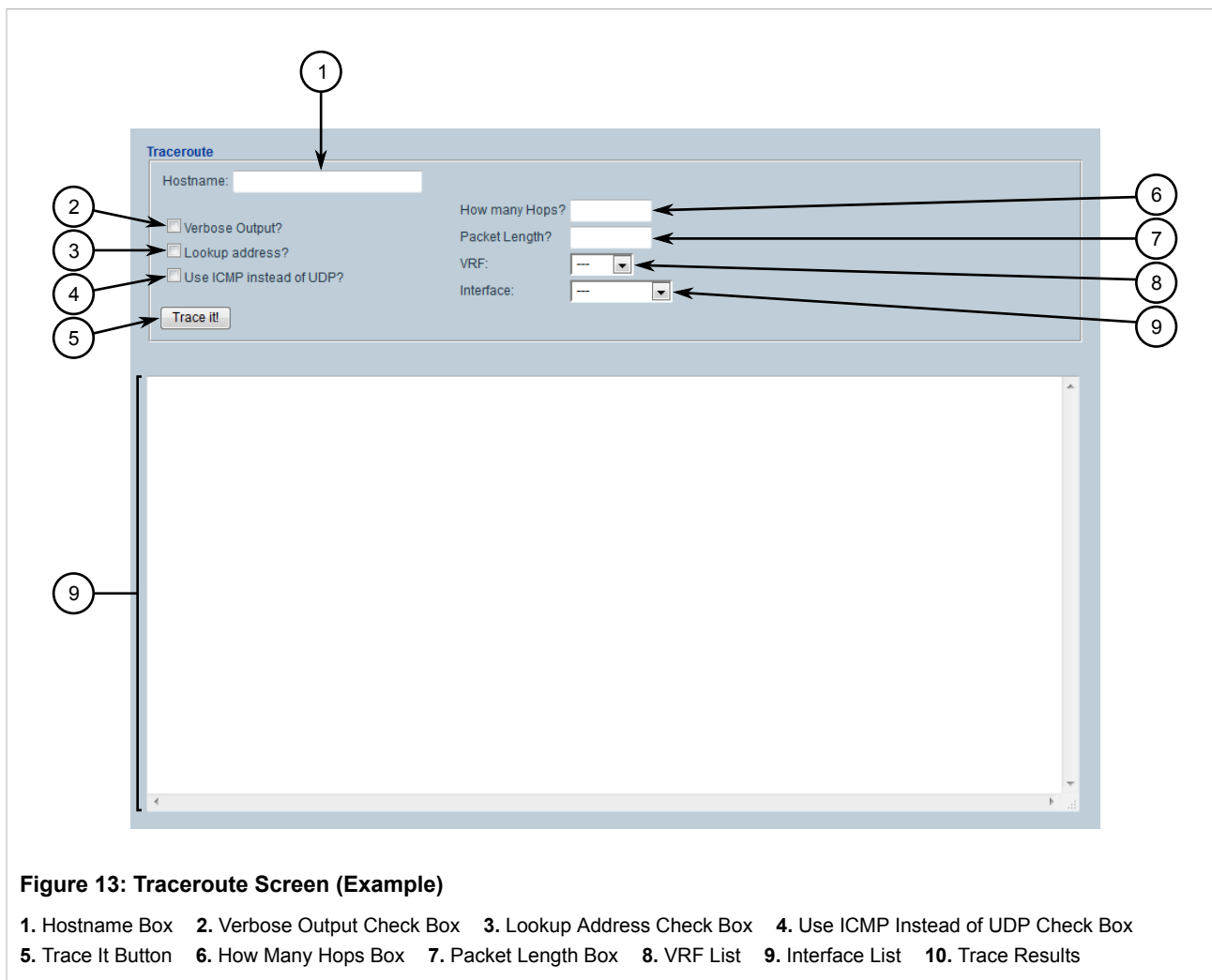
3. Under **Interface To Capture On**, select the interface to capture data from.
4. Under **Maximum Packets Captured**, set the maximum number of packets to capture.
5. Under **Maximum Capture Time**, set the maximum time to capture packets.
6. If necessary, select **Lookup Addresses** to display the source IP for each packet.
7. If necessary, select **Display Link Level Header** to display the link level header information for each packet.
8. If necessary, select **Perform HEX/ASCII Dump** to convert the data to hexadecimal or ASCII characters.
9. Set the verbosity level to control how much information is dumped.
10. If a specific host name should be ignored, define the name of the host.
11. If a specific protocol(s) should be ignored, define the protocol type(s).
12. If packets are to be captured on a particular port, define the port.
13. Click **Tcpdump It!** to start the dump.

### Section 2.6.3

## Tracing the Route to a Remote Host

To trace the route between the device and a remote host, do the following:

1. Select the **Tools** menu and click **Accessories**.
2. Depending on the host's IP address, click **Traceroute** if the host has an IPv4 address, or **Traceroute6** if the host has an IPv6 address. The **Traceroute** screen appears.



3. Configure the following parameters as required:

Parameter	Description
Hostname	The name or IP address of the host.
Verbose Output	When selected, trace results provide more detail.
Lookup Address	When selected, the source IP address is displayed in the trace results.
Use ICMP Instead of UDP	When selected, ICMP is used in place of UDP.
How Many Hops	The maximum number of hops to the remote host.

Parameter	Description
Packet Length	The maximum length of each packet.
VRF	The target VRF. Only required when pinging VRF routes.
Interface	The interface connected to the remote host.

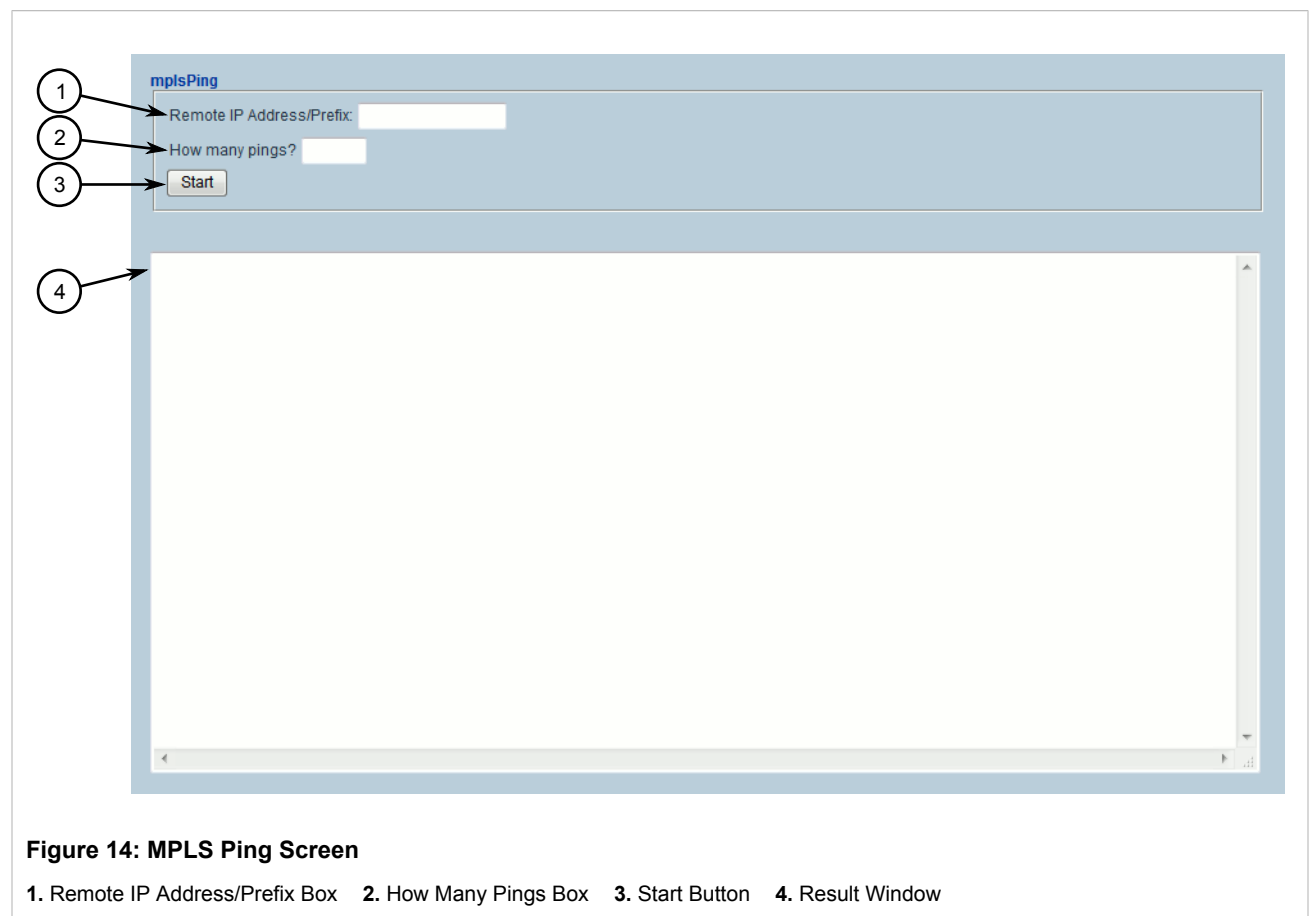
- Click **Trace It** to start the trace. The results of the ping action are displayed below.

#### Section 2.6.4

## Pinging an IPv4 Address Using MPLS Protocols

To ping an IPv4 address using the MPLS protocols, do the following:

- Select the **Tools** menu and click **Accessories**.
- Click **MPLS Ping**. The **MPLS Ping** screen appears.



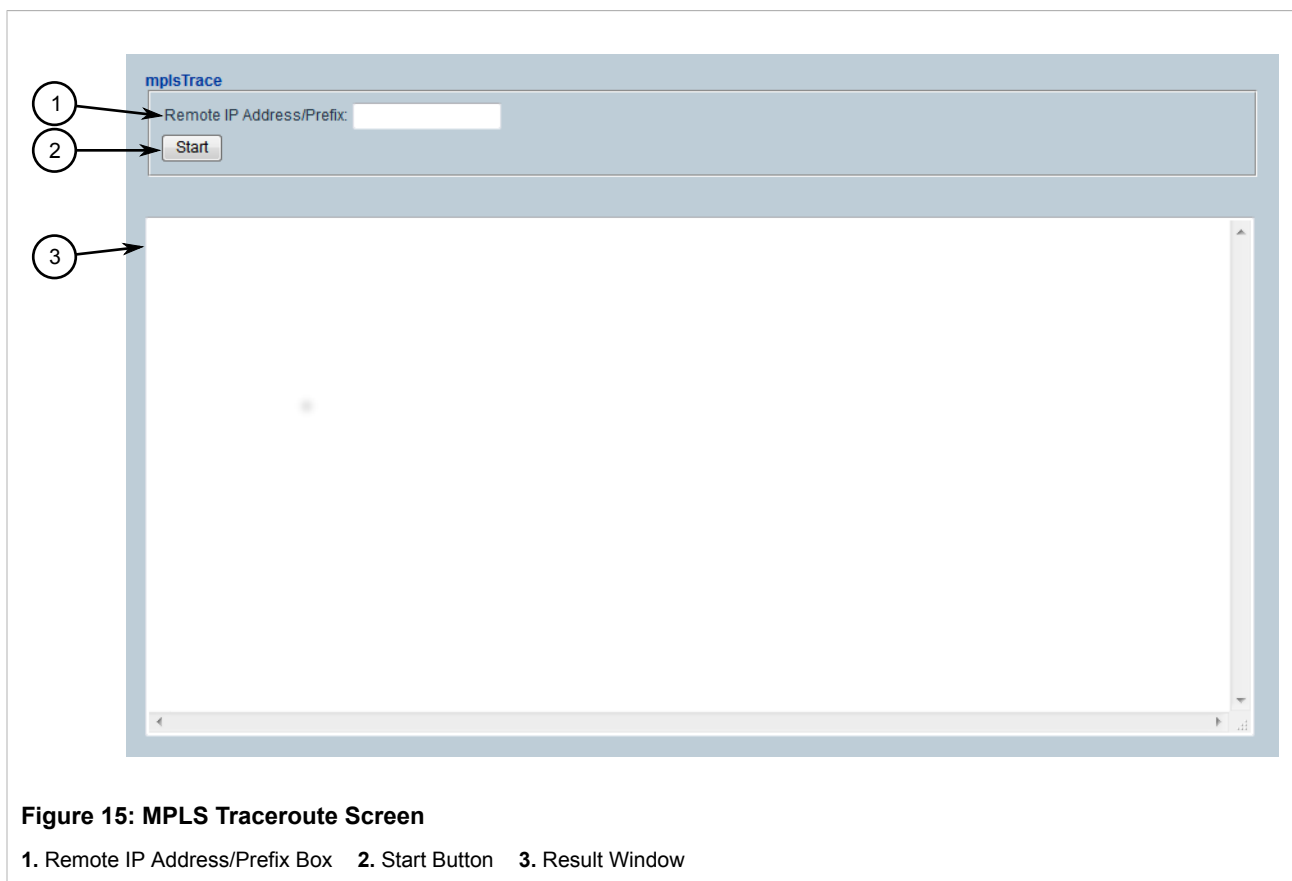
- Type the IPv4 address in the **Remote IP Address/Prefix** box.
- Type the number of pings in the **How Many Pings** box and click **Start**. The results of the ping action are displayed in the **Result Window**.

### Section 2.6.5

## Tracing the Route of an IPv4 Address Using MPLS Protocols

To trace the route of an IPv4 address using MPLS protocols, do the following:

1. Select the **Tools** menu and click **Accessories**.
2. Click **MPLS Traceroute**. The **MPLS Traceroute** screen appears.



**Figure 15: MPLS Traceroute Screen**

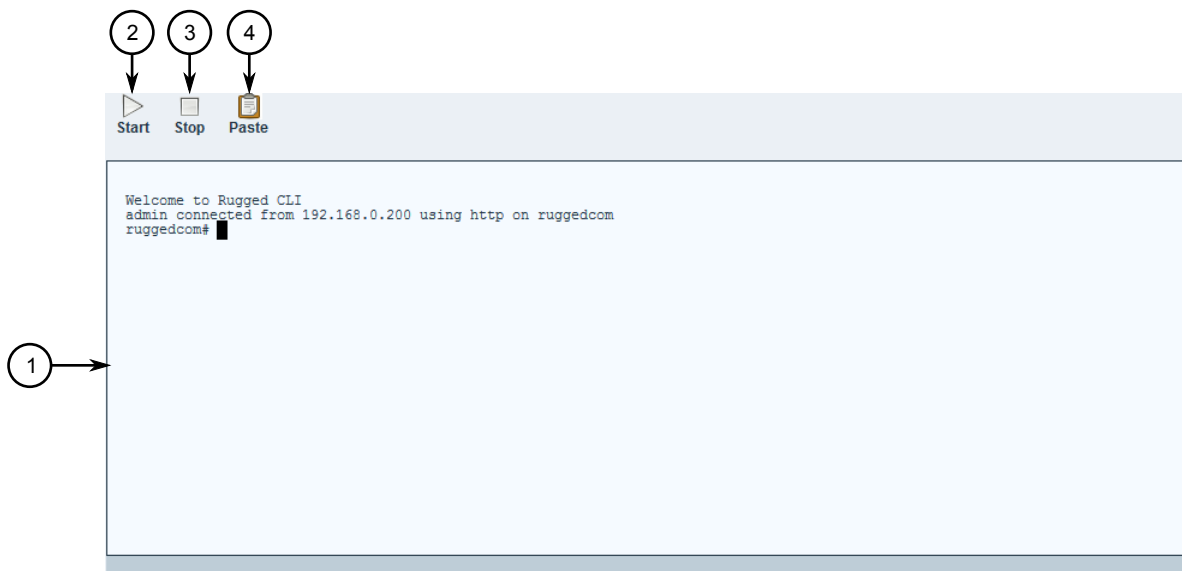
1. Remote IP Address/Prefix Box    2. Start Button    3. Result Window

3. Type the IPv4 address in the **Remote IP Address/Prefix** box and click **Start**. The results of the trace are displayed in the **Result Window**.

### Section 2.7

## Using the Command Line Interface

The Web interface includes a built-in Command Line Interface (CLI). To access the Command Line Interface (CLI) from within the Web interface, select the **Tools** menu and click **CLI**. The **CLI** screen appears.



**Figure 16: CLI Screen**

1. CLI Window   2. Start Button   3. Stop Button   4. Paste Button

For more information about how to use the Command Line Interface, refer to the *RUGGEDCOM ROX II v2.9 CLI User Guide*.





# 3 Device Management

This chapter describes how to configure and manage the device and its components, such as module interfaces, logs and files. It describes the following tasks:



## NOTE

*For information about how to configure the device to work with a network, refer to [Chapter 5, Setup and Configuration](#).*

- [Section 3.1, “Determining the Product Version”](#)
- [Section 3.2, “Viewing Chassis Information and Status”](#)
- [Section 3.3, “Viewing the Parts List”](#)
- [Section 3.4, “Shutting Down the Device”](#)
- [Section 3.5, “Rebooting the Device”](#)
- [Section 3.6, “Restoring Factory Defaults”](#)
- [Section 3.7, “Decommissioning the Device”](#)
- [Section 3.8, “Managing Files”](#)
- [Section 3.9, “Managing Logs”](#)
- [Section 3.10, “Managing the Software Configuration”](#)
- [Section 3.11, “Upgrading/Downgrading the RUGGEDCOM ROX II Software”](#)
- [Section 3.12, “Managing RUGGEDCOM ROX II Applications”](#)
- [Section 3.13, “Managing Feature Keys”](#)
- [Section 3.14, “Managing the Fan Controller”](#)
- [Section 3.15, “Managing Fixed Modules”](#)
- [Section 3.16, “Managing Line Modules”](#)
- [Section 3.17, “Managing Event Trackers”](#)
- [Section 3.18, “Managing Switched Ethernet Ports”](#)
- [Section 3.19, “Managing Routable Ethernet Ports”](#)
- [Section 3.22, “Managing Ethernet Trunk Interfaces”](#)
- [Section 3.23, “Managing Virtual Switches”](#)
- [Section 3.24, “Managing a Domain Name System \(DNS\)”](#)

## Section 3.1

# Determining the Product Version

During troubleshooting or when ordering new devices, Siemens Canada Ltd. personnel may request specific information about the device, such as the model, order code or serial number.

To display general information about the product, navigate to **chassis**. The **Chassis Status** form appears.



The image shows a screenshot of the 'Chassis Status' form in the RuggedCom web interface. The form has a title bar with a green double-arrow icon and the text 'Chassis Status'. Below the title bar, there are four rows of information, each with a blue circular help icon (a question mark) to its right. The rows are: 'Chassis Model' with the value 'RX1501'; 'Software-license' with the value 'Layer 3 Standard Edition'; 'Order-code' with the value 'RX1501-L3-MNT-HI-L3SE-CG01-XX-S01-XX-XX-XX'; and 'ROX Software Release' with the value 'ROX 2.4.0-QA2.1 (2012-10-04 17:44)'.

Parameter	Value
Chassis Model	RX1501
Software-license	Layer 3 Standard Edition
Order-code	RX1501-L3-MNT-HI-L3SE-CG01-XX-S01-XX-XX-XX
ROX Software Release	ROX 2.4.0-QA2.1 (2012-10-04 17:44)

**Figure 17: Chassis Status Form**

This form provides the following information:

Parameter	Description
Chassis Model	<b>Synopsis:</b> A string The RuggedCom device model name.
Software License	<b>Synopsis:</b> A string The current software capability.
MLFB	<b>Synopsis:</b> A string 1 to 256 characters long <b>Prerequisite:</b> /ruggedcom:ruggedcom-internal/ ruggedcom:chassis-type/ruggedcom:family = 'RX1400' MLFB(Machine-Readable Product Designation) or order code
ROX Software Release	<b>Synopsis:</b> A string The release of ROX running on the chassis.
System Serial Number	<b>Synopsis:</b> A string 1 to 32 characters long The system serial number on the chassis label.
BootLoader	<b>Synopsis:</b> A string The version of the ROX bootloader software on the installed module. <b>Prerequisite:</b> /ruggedcom:ruggedcom-internal/ ruggedcom:chassis-type/ruggedcom:family = 'RX1400'

### Section 3.2

## Viewing Chassis Information and Status

The following sections describe how to view the routing status for various routing protocols and related statistics:

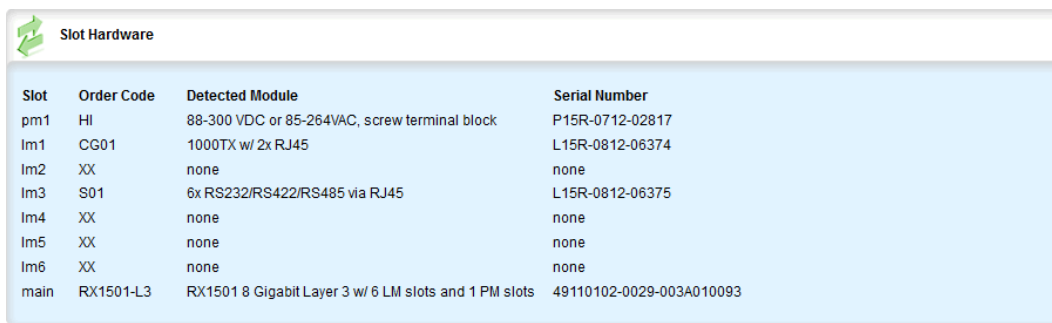
- [Section 3.2.1, “Viewing the Slot Hardware”](#)

- [Section 3.2.2, “Viewing Module Information”](#)
- [Section 3.2.3, “Viewing Flash Card Storage Utilization”](#)
- [Section 3.2.4, “Viewing CPU/RAM Utilization”](#)
- [Section 3.2.5, “Viewing the Slot Status”](#)
- [Section 3.2.6, “Viewing the Slot Sensor Status”](#)
- [Section 3.2.7, “Viewing the Power Controller Status”](#)

## Section 3.2.1

## Viewing the Slot Hardware

To view a list of the hardware installed in each slot, navigate to **chassis » hardware**. The **Slot Hardware** table appears.



Slot	Order Code	Detected Module	Serial Number
pm1	HI	88-300 VDC or 85-264VAC, screw terminal block	P15R-0712-02817
lm1	CG01	1000TX w/ 2x RJ45	L15R-0812-06374
lm2	XX	none	none
lm3	S01	6x RS232/RS422/RS485 via RJ45	L15R-0812-06375
lm4	XX	none	none
lm5	XX	none	none
lm6	XX	none	none
main	RX1501-L3	RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots	49110102-0029-003A010093

Figure 18: Slot Hardware Table

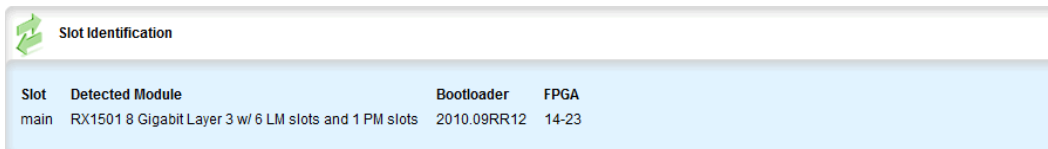
This table provides the following information:

Parameter	Description
slot	<b>Synopsis:</b> { --, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, cm, em, trnk } The slot name, as marked on the silkscreen across the top of the chassis.
Order Code	<b>Synopsis:</b> A string 1 to 25 characters long The order code of the chassis as derived from the current hardware configuration.
Detected Module	<b>Synopsis:</b> A string 1 to 60 characters long The installed module's type specifier.
Serial Number	<b>Synopsis:</b> A string 1 to 64 characters long The installed module's unique serial number.

## Section 3.2.2

## Viewing Module Information

To view information about the modules installed in the device, navigate to **chassis » info**. The **Slot Identification** table appears.

The image shows a screenshot of a web interface titled "Slot Identification". It contains a table with four columns: Slot, Detected Module, Bootloader, and FPGA. The data row shows "main" for Slot, "RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots" for Detected Module, "2010.09RR12" for Bootloader, and "14-23" for FPGA.

Slot	Detected Module	Bootloader	FPGA
main	RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots	2010.09RR12	14-23

**Figure 19: Slot Identification Table**

This table provides the following information:

Parameter	Description
slot	<b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celpport, cm, em, trnk } The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	<b>Synopsis:</b> A string 1 to 60 characters long The installed module's type specifier.
Bootloader	<b>Synopsis:</b> A string The version of the ROX bootloader software on the installed module.
FPGA	<b>Synopsis:</b> A string The version of the ROX FPGA firmware (if any) running on the installed module.

### Section 3.2.3

## Viewing Flash Card Storage Utilization

To view the Flash card storage utilization statistics for the Flash card installed in the device, navigate to **chassis » storage**. The **Flash** form appears.

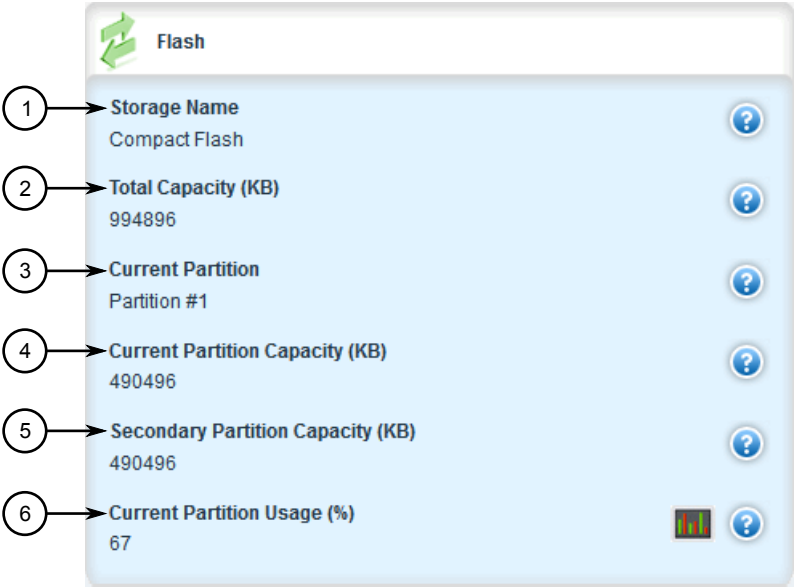


Figure 20: Flash Form

1. Storage Name    2. Total Capacity (KB)    3. Current Partition    4. Current Partition Capacity (KB)    5. Secondary Partition Capacity (KB)    6. Current Partition Usage (%)


This table provides the following information:

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

Section 3.2.4

# Viewing CPU/RAM Utilization

To view the CPU/RAM utilization statistics for each module installed in the device, navigate to **chassis » cpu**. The **Slot CPU/RAM Utilization** table appears.



Slot	Detected-module	CPU load(%)	RAM Avail(%)	RAM Low(%)
main	RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots	26	56	56

**Figure 21: Slot CPU/RAM Utilization Table**


This table provides the following information:

Parameter	Description
slot	<b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, cm, em, trnk } The slot name, as marked on the silkscreen across the top of the chassis.
detected-module	<b>Synopsis:</b> A string 1 to 60 characters long The installed module's type specifier.
CPU load(%)	<b>Synopsis:</b> An integer between 0 and 100 The CPU load, in percent, on the installed module.
RAM Avail(%)	<b>Synopsis:</b> An integer between 0 and 100 The proportion of memory (RAM) currently unused, in percent, on the installed module.
RAM Low(%)	<b>Synopsis:</b> An integer between 0 and 100 The lowest proportion of unused memory (RAM), in percent, recorded for the installed module since start-up.

### Section 3.2.5

## Viewing the Slot Status

To view the overall status of each slot, navigate to **chassis » status**. The **Slot Status** table appears.



Slot	Detected Module	State	Status	Uptime	Boot Date	Boot Time
pm1	88-300 VDC or 85-264VAC, screw terminal block	operating	Normal	2D 1hr 53min 41sec	2012-10-24Z	06:44:32Z
lm1	1000TX w/ 2x RJ45	operating	Normal	0D 0hr 0min 0sec	2012-10-24Z	06:42:28Z
lm2	none	empty	----	0D 0hr 0min 0sec	2012-10-24Z	06:42:28Z
lm3	6x RS232/RS422/RS485 via RJ45	operating	Normal	0D 0hr 0min 0sec	2012-10-24Z	06:42:28Z
lm4	none	empty	----	0D 0hr 0min 0sec	2012-10-24Z	06:42:28Z
lm5	none	empty	----	0D 0hr 0min 0sec	2012-10-24Z	06:42:28Z
lm6	none	empty	----	0D 0hr 0min 0sec	2012-10-24Z	06:42:28Z
main	RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots	operating	Normal	2D 1hr 53min 45sec	2012-10-24Z	06:44:32Z

**Figure 22: Slot Status Table**

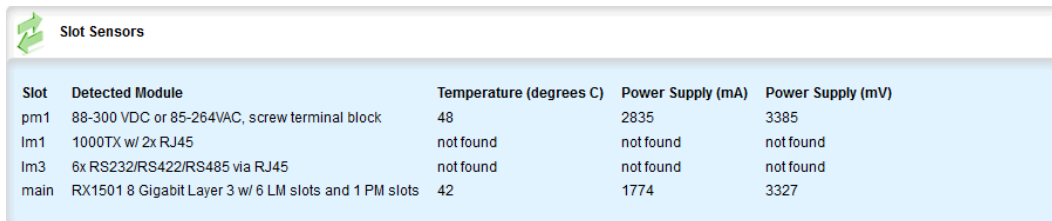
This table provides the following information:

Parameter	Description
slot	<b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celpport, cm, em, trnk } The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	<b>Synopsis:</b> A string 1 to 60 characters long The installed module's type specifier.
State	<b>Synopsis:</b> { unknown, empty, disabled, resetting, operating, failed, disconnected } The current state of the installed module.
Status	<b>Synopsis:</b> A string The runtime status of the installed module.
Uptime	<b>Synopsis:</b> A string The total time elapsed since the start-up of the installed module.
Boot Date	<b>Synopsis:</b> A string The date on which the installed module was started up.
Boot Time	<b>Synopsis:</b> A string The time at which the installed module was started up.

## Section 3.2.6

## Viewing the Slot Sensor Status

To view information about the slot sensors, navigate to **chassis » sensors**. The **Slot Sensors** table appears..



Slot	Detected Module	Temperature (degrees C)	Power Supply (mA)	Power Supply (mV)
pm1	88-300 VDC or 85-264VAC, screw terminal block	48	2835	3385
lm1	1000TX w/ 2x RJ45	not found	not found	not found
lm3	6x RS232/RS422/RS485 via RJ45	not found	not found	not found
main	RX1501 8 Gigabit Layer 3 w/ 6 LM slots and 1 PM slots	42	1774	3327

**Figure 23: Slot Sensors Table**

This table provides the following information:

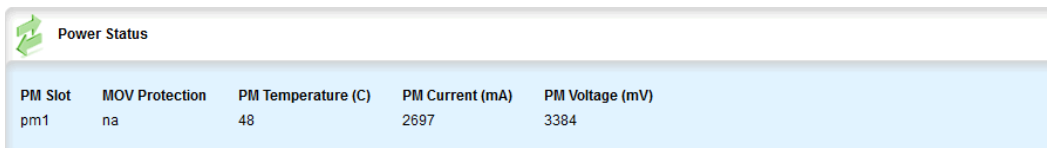
Parameter	Description
slot	<b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celpport, cm, em, trnk } The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	<b>Synopsis:</b> A string 1 to 60 characters long The installed module's type specifier.
Temperature (degrees C)	<b>Synopsis:</b> An integer between 55 and 125 The temperature, in degrees C, of the installed module. If multiple temperature sensors are present on the board, the maximum reading is reported.
Power Supply (mA)	<b>Synopsis:</b> An integer between 0 and 15000

Parameter	Description
	The power supply current, in mA, being drawn by the installed module.
Power Supply (mV)	<b>Synopsis:</b> An integer between 0 and 15000 <b>Prerequisite:</b> /ruggedcom:ruggedcom-internal/ruggedcom:chassis-type/ruggedcom:family != 'RX1400' The power supply voltage, in mV, seen by the installed module.

## Section 3.2.7

## Viewing the Power Controller Status

To view the status of the power controller, navigate to **chassis » power-controller**. The **Power Status** table appears.



Power Status				
PM Slot	MOV Protection	PM Temperature (C)	PM Current (mA)	PM Voltage (mV)
pm1	na	48	2697	3384

Figure 24: Power Status Table

This table provides the following information:

Parameter	Description
PM Slot	<b>Synopsis:</b> { pm1, pm2 } The name of the power module slot as labeled on the chassis.
MOV Protection	<b>Synopsis:</b> { na, working, damaged } The state of the MOV protection circuit.
PM Temperature (C)	<b>Synopsis:</b> An integer between 55 and 125 The temperature (Celsius) inside the power module.
PM Current (mA)	<b>Synopsis:</b> An integer between 0 and 15000 The current (mA) sourced by the power module.
PM Voltage (mV)	<b>Synopsis:</b> An integer between 0 and 15000 The voltage (mV) sourced by the power module.

## Section 3.3

## Viewing the Parts List

To view a list of parts installed in the device, navigate to **chassis » part-list**. The **Module Database** table appears.





Model	Orderfield	Partnumber	Partname
RX1000	24	12-10-0012	24VDC (9-36VDC) Power Supply
RX1000	48	12-10-0004	48VDC (36-59VDC) Power Supply
RX1000	CM01	12-01-0099-001	RX1000 Control Module
RX1000	D01	13-01-0007	DSL card
RX1000	D02	13-01-0008	DDS Card
RX1000	DS3	13-01-0012	1x T3/E3
RX1000	FX01	12-11-0007	2x 100Fx MM ST
RX1000	FX02	12-11-0009	2x 100Fx MM SC
RX1000	FX03	12-11-0008	2x 100Fx MM MTRJ
RX1000	FX04	12-11-0006	2x 100Fx SM ST 20km
RX1000	FX05	12-11-0005	2x 100Fx SM SC 20km
RX1000	FX06	12-11-0004	2x 100Fx SM LC 20km
RX1000	FX07	12-11-0031	2x 100Fx SM SC 50km
RX1000	FX08	12-11-0032	2x 100Fx SM LC 50km
RX1000	FX09	12-11-0033	2x 100Fx SM SC 90km
RX1000	FX10	12-11-0034	2x 100Fx SM LC 90km

Figure 25: Module Database Table

#### Section 3.4

## Shutting Down the Device

To shut down the device, do the following:



### 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

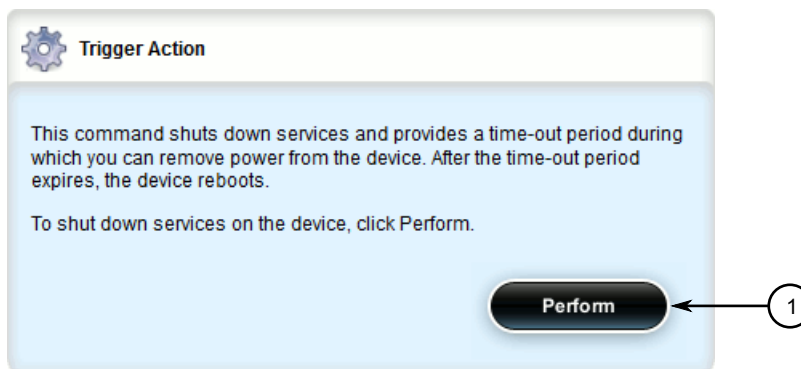
*The device never enters a permanent shutdown state. When instructed to shutdown, the device shuts down and provides a time-out period during which power can be disconnected from the device. The default time-out period is 300 seconds (five minutes). At the end of the time-out period, the device reboots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



### NOTE

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

1. Navigate to **admin** and click **shutdown** in the menu. The **Trigger Action** form appears.



**Figure 26: Trigger Action Form**

1. Perform Button

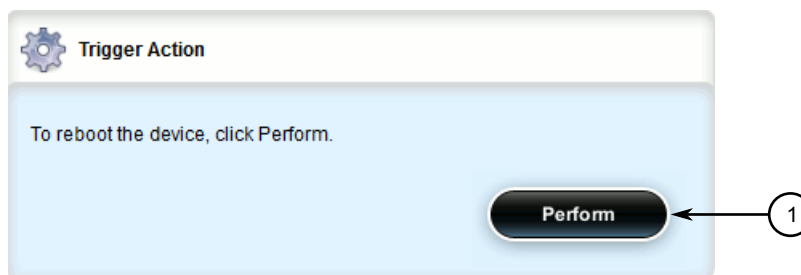
2. Click **Perform**.

### Section 3.5

## Rebooting the Device

To reboot the device, do the following:

1. Navigate to **admin** and click **reboot** in the menu. The **Trigger Action** form appears.



**Figure 27: Trigger Action Form**

1. Perform Button

2. Click **Perform**.

### Section 3.6

## Restoring Factory Defaults

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

1. Navigate to **admin** and click **restore-factory-defaults** in the menu. The **Restore Factory Defaults** and **Trigger Action** forms appear.

**Figure 28: Restore Factory Defaults Form**

1. Delete Logs Check Box    2. Default Both Partitions Check Box    3. Delete Saved Configurations Check Box    4. Shutdown Check Box

**Figure 29: Trigger Action Form**

1. Perform Button

- On the **Restore Factory Defaults** form, configure the following parameter(s) as required:

Parameter	Description
delete-logs	<b>Synopsis:</b> true or false <b>Default:</b> false Delete system logs as well as restoring default settings.
default-both-partitions	<b>Synopsis:</b> true or false <b>Default:</b> false Perform the operation on both partitions.
delete-saved-configurations	<b>Synopsis:</b> true or false <b>Default:</b> false Delete saved configuration files (works with default-both-partitions option).
shutdown	<b>Synopsis:</b> true or false <b>Default:</b> false

Parameter	Description
	Shutdown rather than reboot after restoring factory defaults.

3. On the **Trigger Action** form, click **Perform**.

## Section 3.7

## Decommissioning the Device

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

To decommission the device, do the following:

1. Obtain a copy of the RUGGEDCOM ROX II firmware currently installed on the device. For more information, contact Siemens Customer Support.
2. Log in to maintenance mode. For more information, refer to the *RUGGEDCOM ROX II v2.9 CLI User Guide*.
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 2.3, “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 3.11.5.2, “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 3.4, “Shutting Down the Device”](#).

## Section 3.8

## Managing Files

The following sections describe how to manage important files on the device:

**NOTE**

*Only feature keys and configuration files can be installed or backed up.*

- [Section 3.8.1, “Uploading Files”](#)
- [Section 3.8.2, “Downloading Files”](#)
- [Section 3.8.3, “Installing Files”](#)
- [Section 3.8.4, “Backing Up Files”](#)

### Section 3.8.1

## Uploading Files

The following file types can be uploaded to the device:

- configuration files
- feature keys

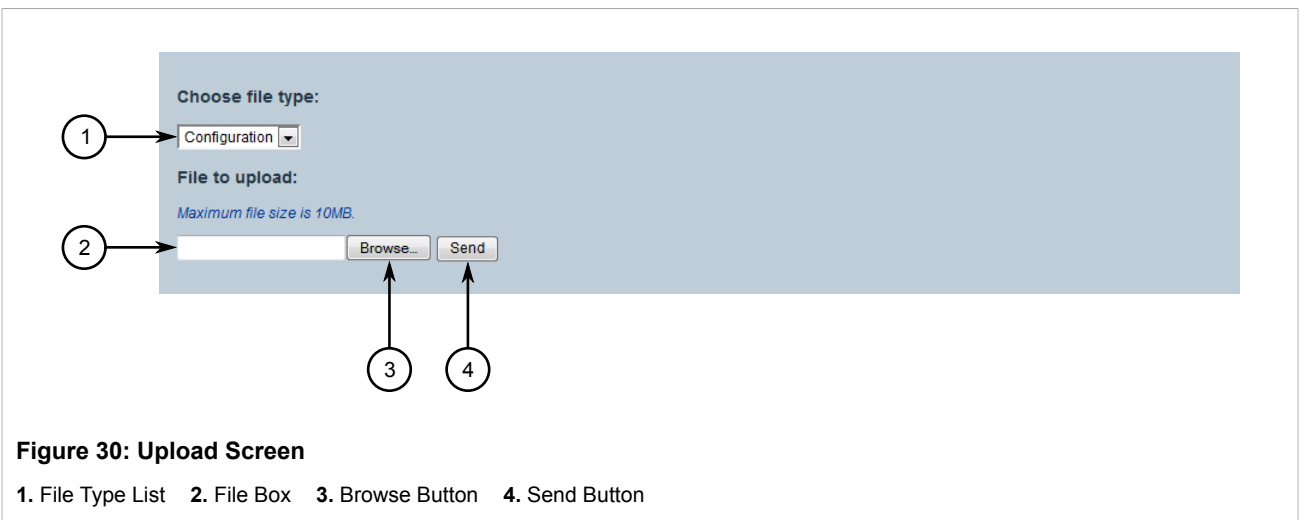
To upload a file to the device, do the following:



### 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. Select the **Tools** menu and click **Upload**. The **Upload** screen appears.



2. Under **Choose file type**, select the type of file that will be uploaded to the device.
3. Under **File to upload**, either type the path and filename in the box or click **Browse** and select the file.
4. Click **Send** to start the upload.

### Section 3.8.2

## Downloading Files

The following file types can be downloaded from the device:

- configuration files
- feature keys
- logs
- rollbacks

To download a file from the device, do the following:

1. Select the **Tools** menu and click **Download**. The **Download** screen appears.



**Figure 31: Download Screen**

1. File Type List    2. Available Files

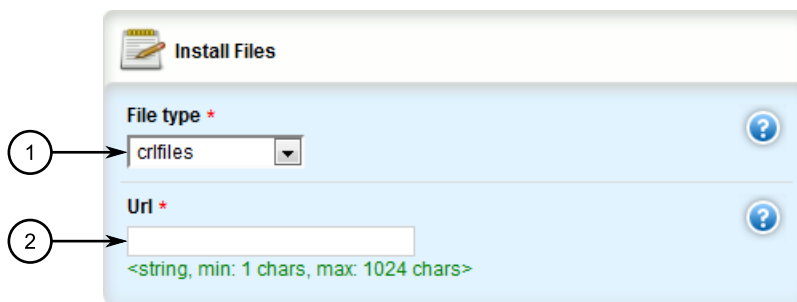
2. Under **Choose file type**, select the type of file to download from the device. Files of that type, if available, are automatically listed.
3. Click the filename. Depending on the browser, a save dialog box appears.
4. Open the file or save it to an appropriate location.

### Section 3.8.3

## Installing Files

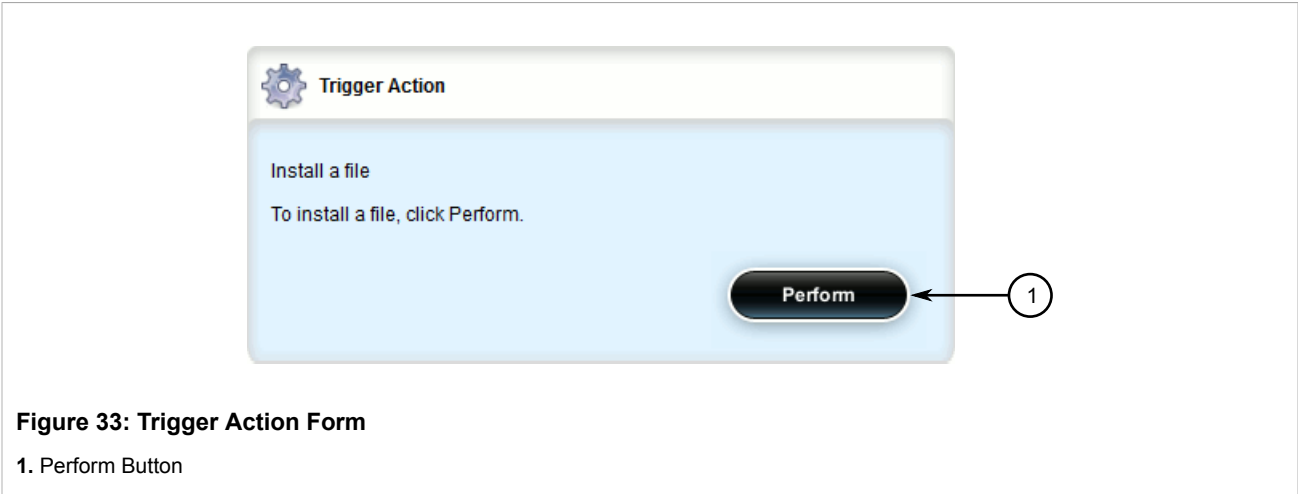
To install a file on the device, such as a configuration file or feature key, do the following:

1. If the source of the file is a USB Mass Storage drive, insert the drive in the USB port on the device. For more information, refer to the *RUGGEDCOM RX5000/MX5000/MX5000RE Installation Guide*.
2. Navigate to **admin** and click **install-files** in the menu. The **Install Files** and **Trigger Action** forms appear.



**Figure 32: Install Files Form**

1. File Type List    2. URL Box



**Figure 33: Trigger Action Form**  
1. Perform Button

3. On the **Install Files** form, configure the following parameters:

Parameter	Description
file-type	<b>Synopsis:</b> { config, featurekey, vmfile } The file types to be copied.
url	<b>Synopsis:</b> 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/microSDHC drive (if applicable), the URL format is "usb://<usb-device-name>/path-to-file-on-system" or "sd://sd-1//path-to-file-on-system". Run "show chassis" to determine the name of the USB device. Note that only one single partition is supported for either data medium. For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If "port" is not specified, the default port for the protocol is used.

4. On the **Trigger Action** form, click **Perform**.

Section 3.8.4

## Backing Up Files

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

1. If the file's destination is a USB Mass Storage drive, insert the drive in the USB port on the device. For more information, refer to the *RUGGEDCOM RX5000/MX5000/MX5000RE Installation Guide*.
2. Navigate to **admin** and click **backup-files** in the menu. The **Backup Files** and **Trigger Action** forms appear.

The screenshot shows the 'Backup Files' form with the following fields and callouts:

- 1** points to the 'File type \*' dropdown menu, which currently shows 'rollbacks'.
- 2** points to the 'File \*' text input box, which has a placeholder text '<string, min: 1 chars, max: 255 chars>'.
- 3** points to the 'Timestamp' section, which includes a checkbox labeled 'Enabled'.
- 4** points to the 'Url \*' text input box, which has a placeholder text '<string, min: 1 chars, max: 1024 chars>'.

**Figure 34: Backup Files Form**

1. File Type List   2. File Box   3. Timestamp Check Box   4. URL Box

The screenshot shows the 'Trigger Action' form with the following elements:

- A gear icon and the title 'Trigger Action'.
- The text 'Backup a file'.
- The instruction 'To back up a file, click Perform.'
- A 'Perform' button, which is pointed to by callout **1**.

**Figure 35: Trigger Action**

1. Perform Button

3. On the **Backup Files** form, configure the following parameters:

Parameter	Description
file-type	<b>Synopsis:</b> { config, featurekey, logfiles, rollbacks, licenses } The file types to copy.
file	<b>Synopsis:</b> A string 1 to 255 characters long The file names to copy.
timestamp	<b>Synopsis:</b> true or false <b>Default:</b> false If enabled, a time stamp will be appended to the file name. This option is not applicable to file names that contain '*'.
url	<b>Synopsis:</b> A string 1 to 1024 characters long




Parameter	Description
	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/microSDHC drive (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 using a path only, close it with '/'. If "port" is not specified, the default port for the protocol is used.

- On the **Trigger Action** form, click **Perform**.

## Section 3.9

## Managing Logs

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

<b>Security Event Logs</b>	<p>Information related to the following security events are logged by RUGGEDCOM ROX II:</p> <div> <b>NOTE</b> <i>Passwords can be retried up to 3 times before the login attempt is considered a security event.</i></div> <ul style="list-style-type: none"><li>Successful and unsuccessful login attempts</li><li>Local and remote (RADIUS) authentication</li><li>Security-sensitive commands (whether successful or unsuccessful)</li><li>An optionally configurable SNMP Authentication Failure Trap (disabled by default) in accordance with SNMPv2-MIB</li></ul> <p>All security event logs are recorded in <code>var/log/auth.log</code> and can be viewed in the Authlog Viewer. For more information about viewing logs, refer to <a href="#">Section 3.9.1, "Viewing Logs"</a>.</p>
<b>Syslogs</b>	<p>Syslog allows users to configure local and remote syslog connections to record important, non-security event information. The remote Syslog protocol, defined in <a href="http://tools.ietf.org/html/rfc3164">RFC 3164</a> [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.</p> <p>All log files are organized in the log directory (<code>/var/log</code>) according to the facility and priority at which they have been logged. Remote Syslog sends the requested logs to the remote server(s) at whichever facility and priority they were initially logged, after filtering the logs based on the selectors configured for the server.</p> <p>The following log files are setup with the following default selectors:</p> <ul style="list-style-type: none"><li><code>syslog</code> catches all logs except <code>daemon.debug</code>, <code>auth</code> or <code>authpriv</code> logs</li><li><code>daemon.log</code> catches all <i>err</i> level (and above) logs written to the <code>daemon</code> facility</li><li><code>messages</code> catches all <i>info</i>, <i>notice</i> and <i>warn</i> level logs for all facilities except <code>auth</code>, <code>authpriv</code>, <code>cron</code>, <code>daemon</code>, <code>mail</code> and <code>news</code></li></ul> <p>A selector setup using the following facilities at level <i>info</i> and up is recommended:</p> <ul style="list-style-type: none"><li><code>daemon</code></li><li><code>user</code></li><li><code>kern</code></li><li><code>syslog</code></li></ul>
<b>Diagnostic Logs</b>	Diagnostic logs record system information for the purposes of troubleshooting.

The following sections describe how to view, configure and manage logs:

- [Section 3.9.1, “Viewing Logs”](#)
- [Section 3.9.2, “Deleting Logs”](#)
- [Section 3.9.3, “Configuring a Source IP Address for Remote Syslog Messages”](#)
- [Section 3.9.4, “Managing Diagnostic Logs”](#)
- [Section 3.9.5, “Configuring Secure Remote Syslog”](#)
- [Section 3.9.6, “Managing Remote Syslog Servers”](#)
- [Section 3.9.7, “Managing Remote Server Selectors”](#)

## Section 3.9.1

## Viewing Logs

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

**NOTE**

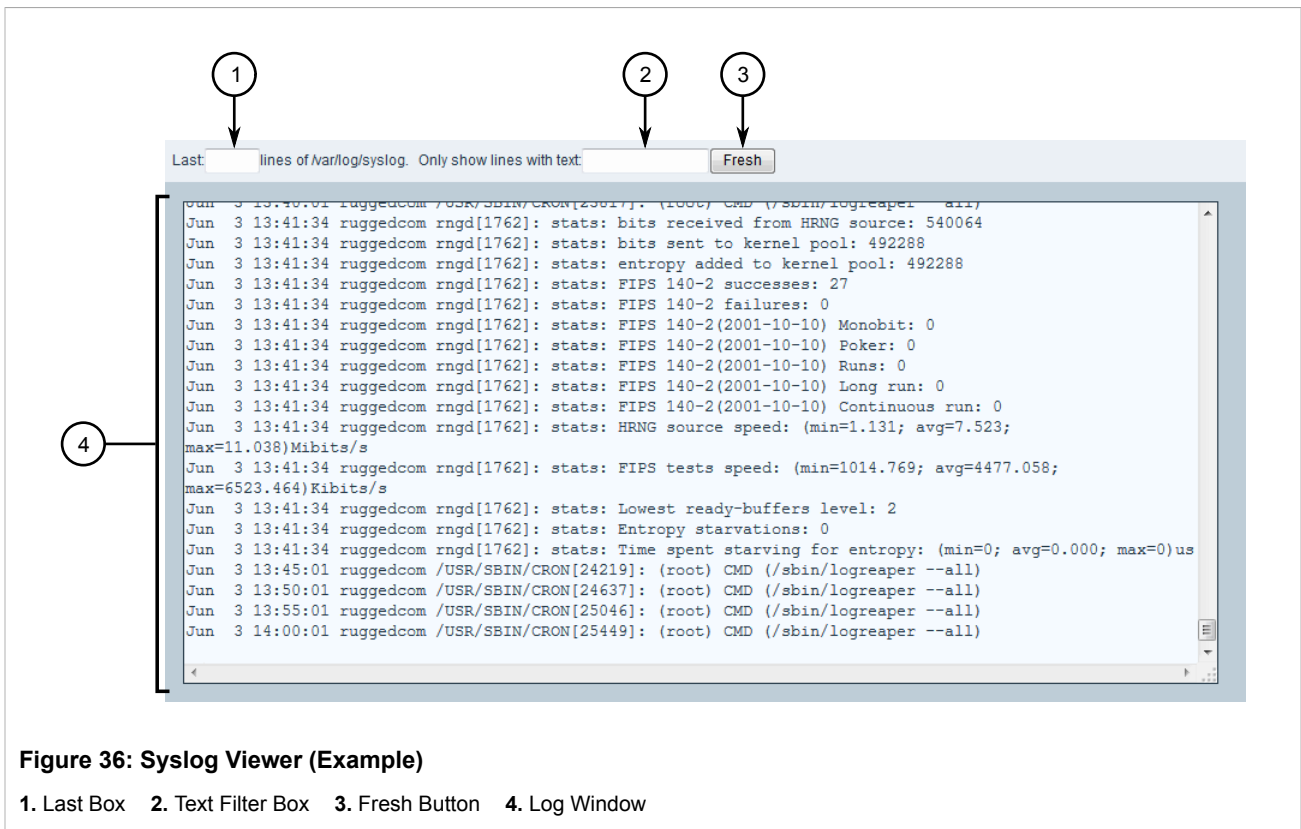
For information about downloading log files from the device, refer to [Section 3.8.4, “Backing Up Files”](#).

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

1. Select the **Tools** menu and click **Device Info**. The toolbar at the top of the **Tools** menu features the following links:

<b>Messages Viewer</b>	Displays all events from <code>/var/log/messages</code>
<b>Syslog Viewer</b>	Displays syslog events from <code>/var/log/syslog</code>
<b>Authlog Viewer</b>	Displays authentication events from <code>/var/log/auth.log</code>
<b>Layer2log Viewer</b>	Displays Layer 2 events from <code>/var/log/layer2</code>
<b>Kernlog Viewer</b>	Displays kernel events from <code>/var/log/kern.log</code>

2. Click the link for the log viewer. The selected log appears.



**Figure 36: Syslog Viewer (Example)**

1. Last Box   2. Text Filter Box   3. Fresh Button   4. Log Window

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

- Enter a number in the **Last** box to control the number of lines displayed
- Enter a number, word or phrase in the **Text Filter** box to show only lines that contain the specified text

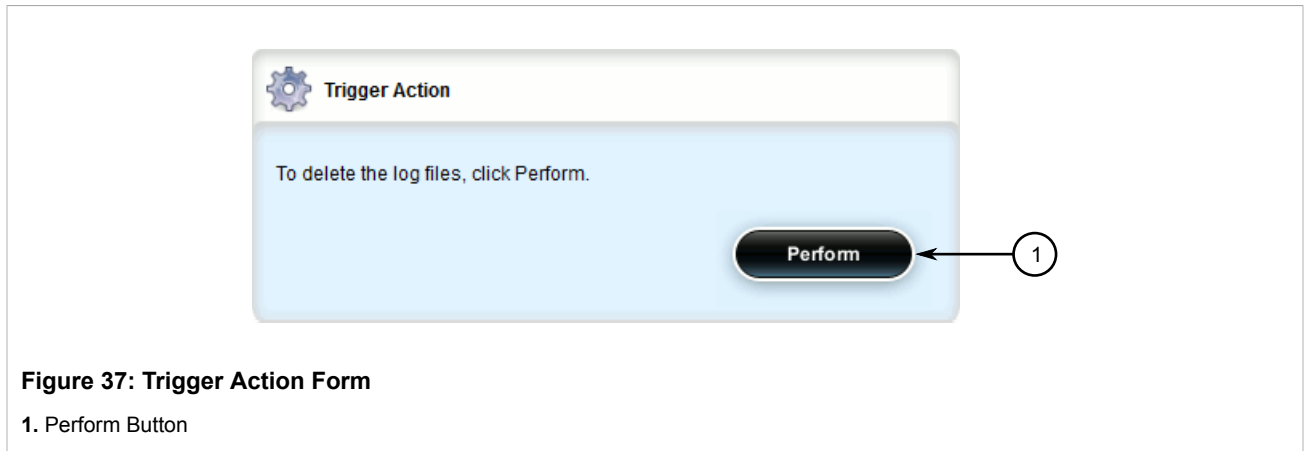
Click **Fresh** to filter the content of the log.

### Section 3.9.2

## Deleting Logs

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

1. Navigate to **admin** and click **delete-logs** in the menu. The **Trigger Action** form appears.



2. Click **Perform**.

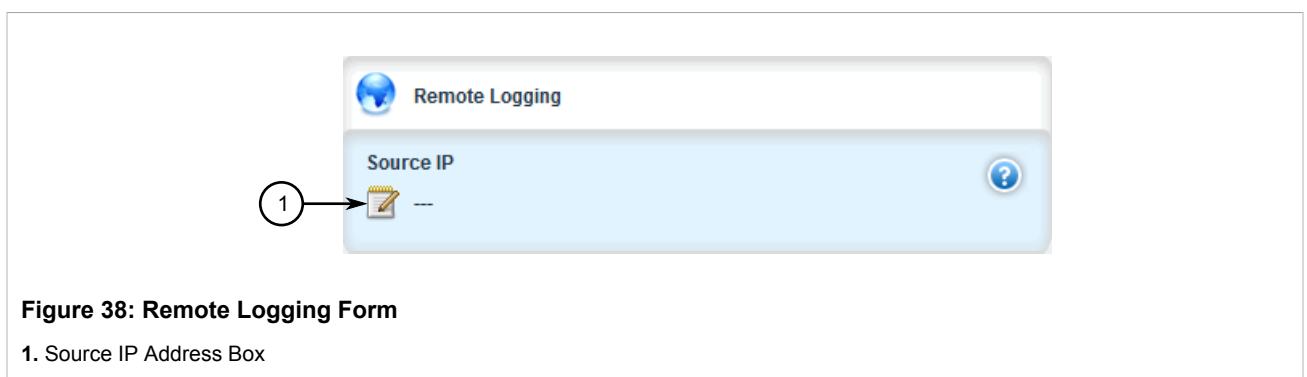
### Section 3.9.3

## 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. Change the mode to **Edit Public** or **Edit Exclusive**.
2. Make sure an IP address is first defined for the desired interface. For more information, refer to either [Section 5.39.3.2, “Adding an IPv4 Address”](#) or [Section 5.39.6.2, “Adding an IPv6 Address”](#).
3. Navigate to **admin » logging**. The **Remote Logging** form appears.



4. In the **Source IP Address** box, type the alternative source IP address.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

## Section 3.9.4

## Managing Diagnostic Logs

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

Log	Filename
Developer's Log	/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.*

The following sections describe how to configure and manage diagnostic logs:

- [Section 3.9.4.1, “Enabling/Disabling the Developer's Log”](#)
- [Section 3.9.4.2, “Enabling/Disabling the SNMP Log”](#)
- [Section 3.9.4.3, “Enabling/Disabling the NETCONF Summary Log”](#)
- [Section 3.9.4.4, “Enabling/Disabling the NETCONF Trace Log”](#)
- [Section 3.9.4.5, “Enabling/Disabling the XPATH Trace Log”](#)
- [Section 3.9.4.6, “Enabling/Disabling the WebUI Trace Log”](#)

## Section 3.9.4.1

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » logging » diagnostics**. The **Developer's Log** form appears.

**Figure 39: Developer's Log Form**

1. Enabled Check Box    2. Log-Level List

- Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/Disables developer logging to the confd-dev.log.
log-level	<b>Synopsis:</b> { error, info, trace } <b>Default:</b> info Sets the verbosity level for developer logging.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 3.9.4.2

### Enabling/Disabling the SNMP Log

The SNMP log records all SNMP related events.

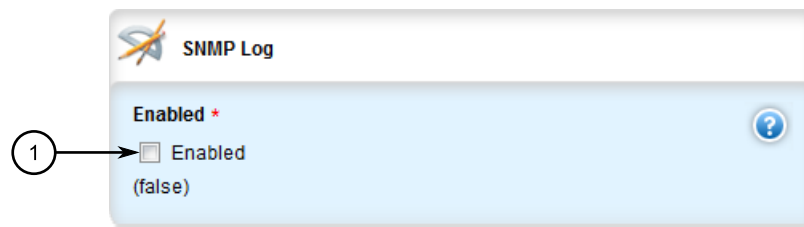


#### CAUTION!

*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:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » logging » diagnostics**. The **SNMP Log** form appears.



**Figure 40: SNMP Log Form**

1. Enabled Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/Disables SNMP logging to the snmp-trace.log.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.9.4.3

### Enabling/Disabling the NETCONF Summary Log

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

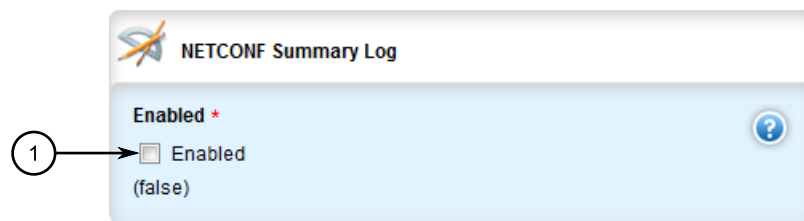


#### **CAUTION!**

*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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » logging » diagnostics**. The **NETCONF Summary Log** form appears.



**Figure 41: NETCONF Summary Log Form**

1. Enabled Check Box

- Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/Disables NETCONF logging to the netconf.log.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 3.9.4.4

### Enabling/Disabling the NETCONF Trace Log

The NETCONF trace log details all NETCONF protocol transactions, including successful and failed transactions.

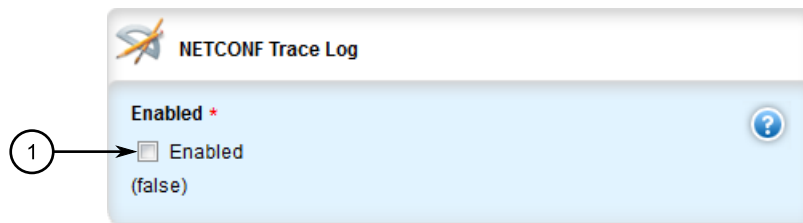


#### CAUTION!

*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:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » logging » diagnostics**. The **NETCONF Trace Log** form appears.



**Figure 42: NETCONF Trace Log Form**

1. Enabled Check Box

- Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/disables NETCONF Trace logging to netconf-trace.log.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.



### Section 3.9.4.5

## Enabling/Disabling the XPATH Trace Log

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

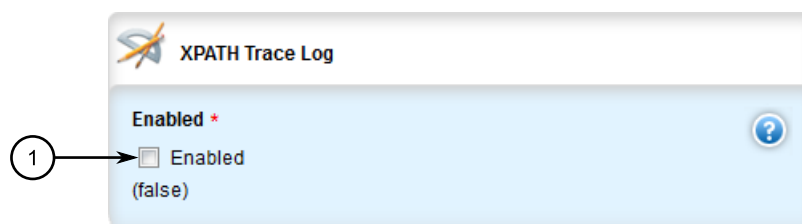


### CAUTION!

*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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » logging » diagnostics**. The **XPATH Trace Log** form appears.



**Figure 43: XPATH Trace Log Form**

1. Enabled Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/disables XPATH Trace logging to the xpath-trace.log.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 3.9.4.6

## Enabling/Disabling the WebUI Trace Log

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



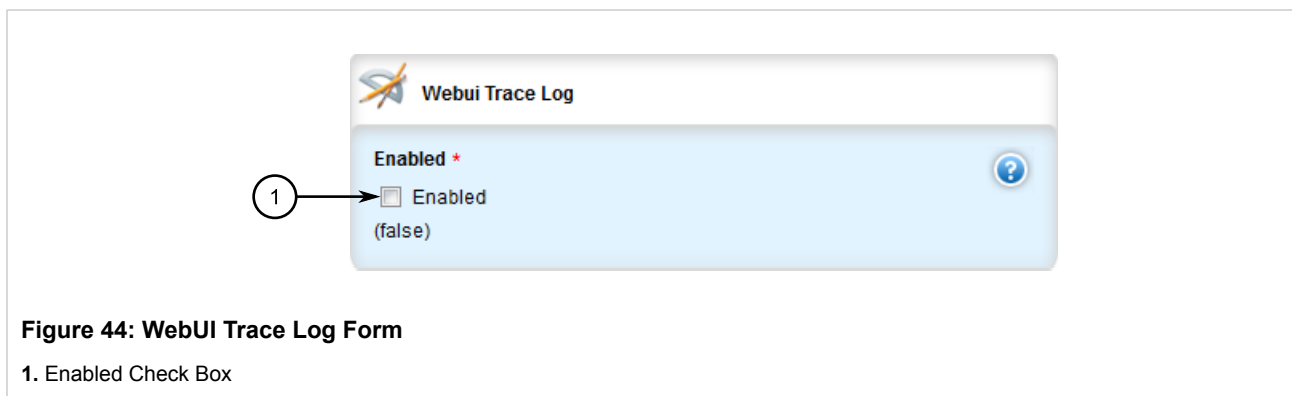
### CAUTION!

*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. Change the mode to **Edit Private** or **Edit Exclusive**.

- Navigate to **admin » logging » diagnostics**. The **WebUI Trace Log** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/disables WebUI Trace logging to the webui-trace.log.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 3.9.5

## 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 be signed by the same CA.*

The following sections describe how to enable and configure secure remote syslog:

- [Section 3.9.5.1, “Enabling/Disabling Secure Remote Syslog”](#)
- [Section 3.9.5.2, “Viewing a List of Permitted Peers”](#)
- [Section 3.9.5.3, “Adding a Permitted Peer”](#)
- [Section 3.9.5.4, “Deleting a Permitted Peer”](#)

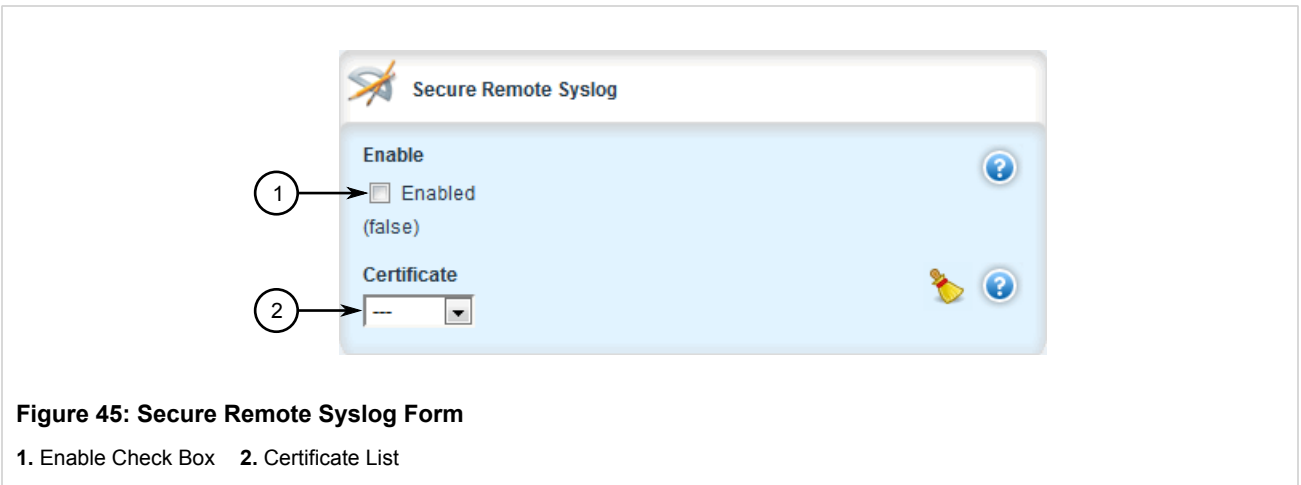
#### Section 3.9.5.1

### Enabling/Disabling Secure Remote Syslog

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

- Change the mode to **Edit Public** or **Edit Exclusive**.

2. Navigate to **admin » logging » secure-remote-syslog**. The **Secure Remote Syslog** form appears.



#### NOTE

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

3. Click **Enable** to enable secure remote syslog, or clear the check box to disable secure remote syslog.



#### IMPORTANT!

All certificates must meet the following requirements:

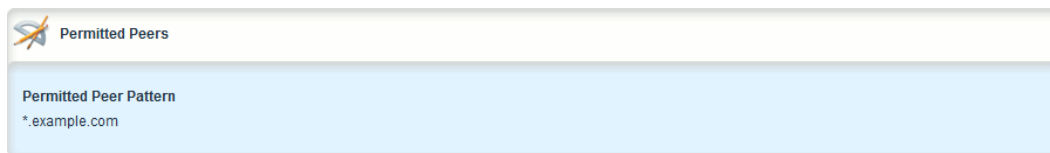
- X.509 v3 digital certificate format
- PEM format
- RSA key pair, 512 to 2048 bits in length

4. If secure remote syslog is enabled, specify a certificate to use for authentication with remote syslog server. If the desired certificate is not listed, add it. For more information, refer to [Section 4.7.4.3, “Adding a Certificate”](#).
5. [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 3.9.5.3, “Adding a Permitted Peer”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 3.9.5.2

### Viewing a List of Permitted Peers

To view a list of permitted peers, navigate to **admin » logging » secure-remote-syslog » permitted-peer**. If permitted peers have been configured, the **Permitted Peers** table appears.



**Figure 46: Permitted Peers Table**

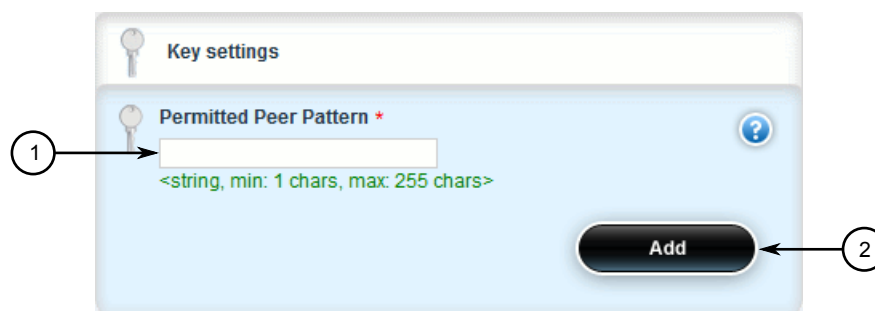
If no permitted peers have been configured, add peers as needed. For more information, refer to [Section 3.9.5.3, “Adding a Permitted Peer”](#).

### Section 3.9.5.3

## Adding a Permitted Peer

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » logging » secure-remote-syslog » permitted-peer** and click **<Add permitted-peer>**. The **Key Settings** form appears.



**Figure 47: Key Settings Form**

1. Permitted Peer Pattern Box    2. Add Button

3. Configure the following parameter(s) as required:

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

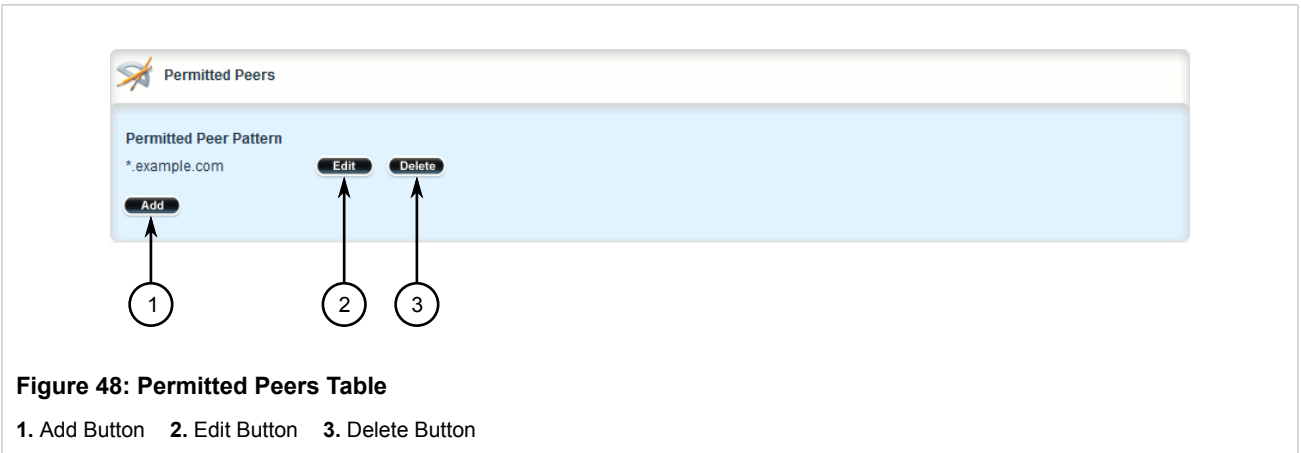
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.9.5.4

### Deleting a Permitted Peer

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » logging » secure-remote-syslog » permitted-peer**. The **Permitted Peers** table appears.



3. Click **Delete** next to the chosen peer.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.9.6

### 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

The following sections describe how to configure and manage remote Syslog servers:

- [Section 3.9.6.1, “Viewing a List of Remote Servers”](#)
- [Section 3.9.6.2, “Adding a Remote Server”](#)
- [Section 3.9.6.3, “Deleting a Remote Server”](#)

#### Section 3.9.6.1

### Viewing a List of Remote Servers

To view a list of remote servers, navigate to **admin » logging » server**. If remote servers have been configured, the **Remote Server** table appears.

Remote Server	
Server IP Address	Enabled
172.30.144.254	enabled

**Figure 49: Remote Server Table**

If no remote servers have been configured, add servers as needed. For more information, refer to [Section 3.9.6.2, “Adding a Remote Server”](#).

### Section 3.9.6.2

## Adding a Remote Server

To add a remote server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » logging » server** and click **<Add server>**. The **Key Settings** form appears.

**Figure 50: Key Settings Form**

1. Server IP Address Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Server IP Address	<b>Synopsis:</b> A string The IPv4 or IPv6 address of a logging server. Up to 8 logging servers can be added.

4. Click **Add**. The **Remote Server** form appears.

**Figure 51: Remote Server Form**

1. Enabled Check Box   2. Transport Protocol List   3. Monitor Interface List   4. Port Box

5. Configure the following parameter(s) as required:

Parameter	Description
Enable	<b>Synopsis:</b> typeless Enables/disables the feed to the remote logging server.
Transport Protocol	<b>Synopsis:</b> { udp, tcp } <b>Default:</b> udp TCP or UDP.
Monitor Interface	The interface to monitor. If the IP address is changed on the interface, the logging daemon will restart.
Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 514 Port number.

6. Configure one or more selectors for the server. For more information, refer to [Section 3.9.7.2, “Adding a Remote Server Selector”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

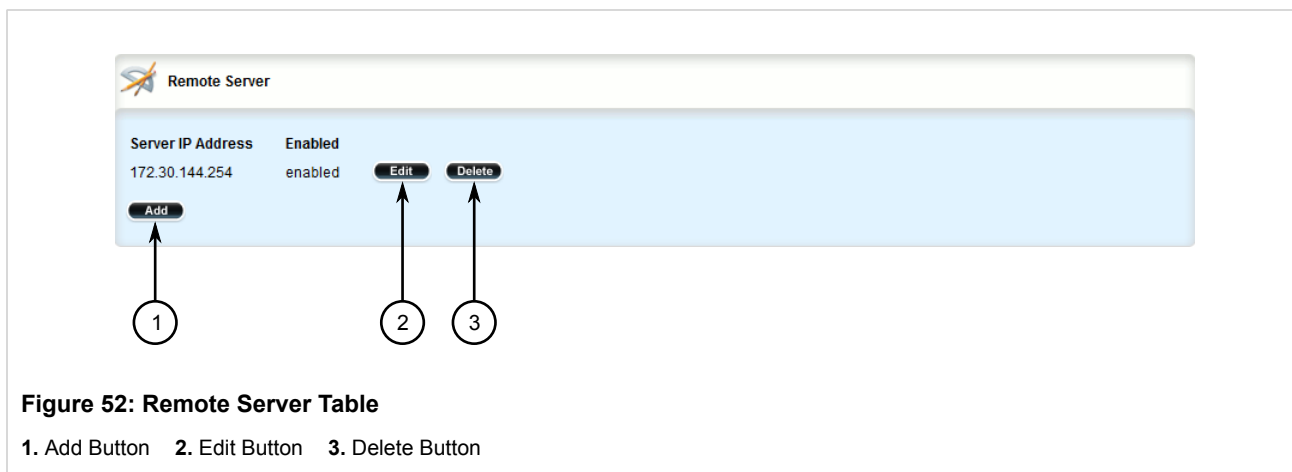
### Section 3.9.6.3

## Deleting a Remote Server

To delete a remote server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **admin » logging » server**. The **Remote Server** table appears.



3. Click **Delete** next to the chosen remote server.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.9.7

## Managing Remote Server Selectors

Remote server selectors filter the information sent to specific servers.

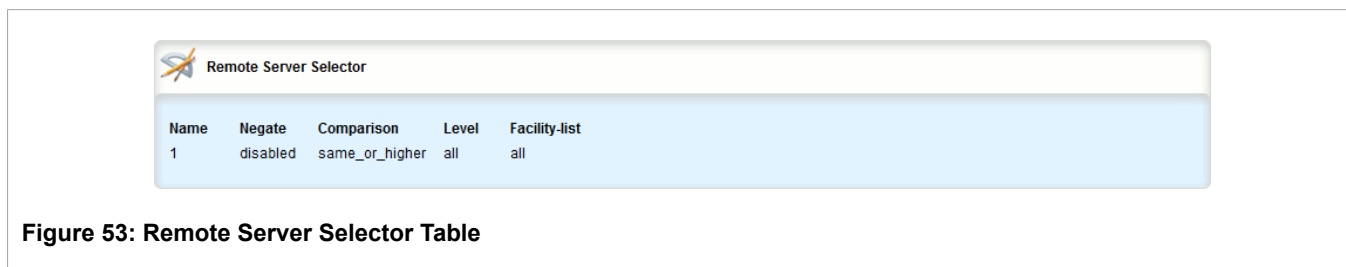
The following sections describe how to configure and manage remote server selectors:

- [Section 3.9.7.1, “Viewing a List of Remote Server Selectors”](#)
- [Section 3.9.7.2, “Adding a Remote Server Selector”](#)
- [Section 3.9.7.3, “Deleting a Remote Server Selector”](#)

#### Section 3.9.7.1

### Viewing a List of Remote Server Selectors

To view a list of remote server selectors, navigate to **admin » logging » server » {address} » selector**, where **{address}** is the IP address of the remote server. If remote server selectors have been configured, the **Remote Server Selector** table appears.





If no remote server selectors have been configured, add selectors as needed. For more information, refer to [Section 3.9.7.2, “Adding a Remote Server Selector”](#).

Section 3.9.7.2

Adding a Remote Server Selector

To add a remote server selector, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to **admin » logging » server » {address} » selector**, where {address} is the IP address of the remote server.
- 3. Click **<Add selector>**. The **Key Settings** form appears.

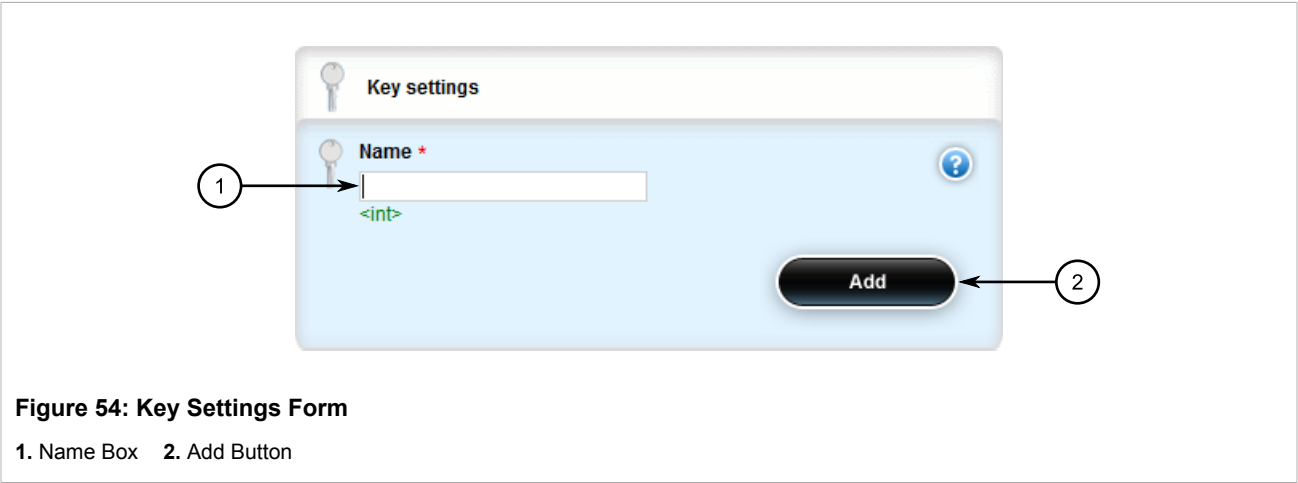


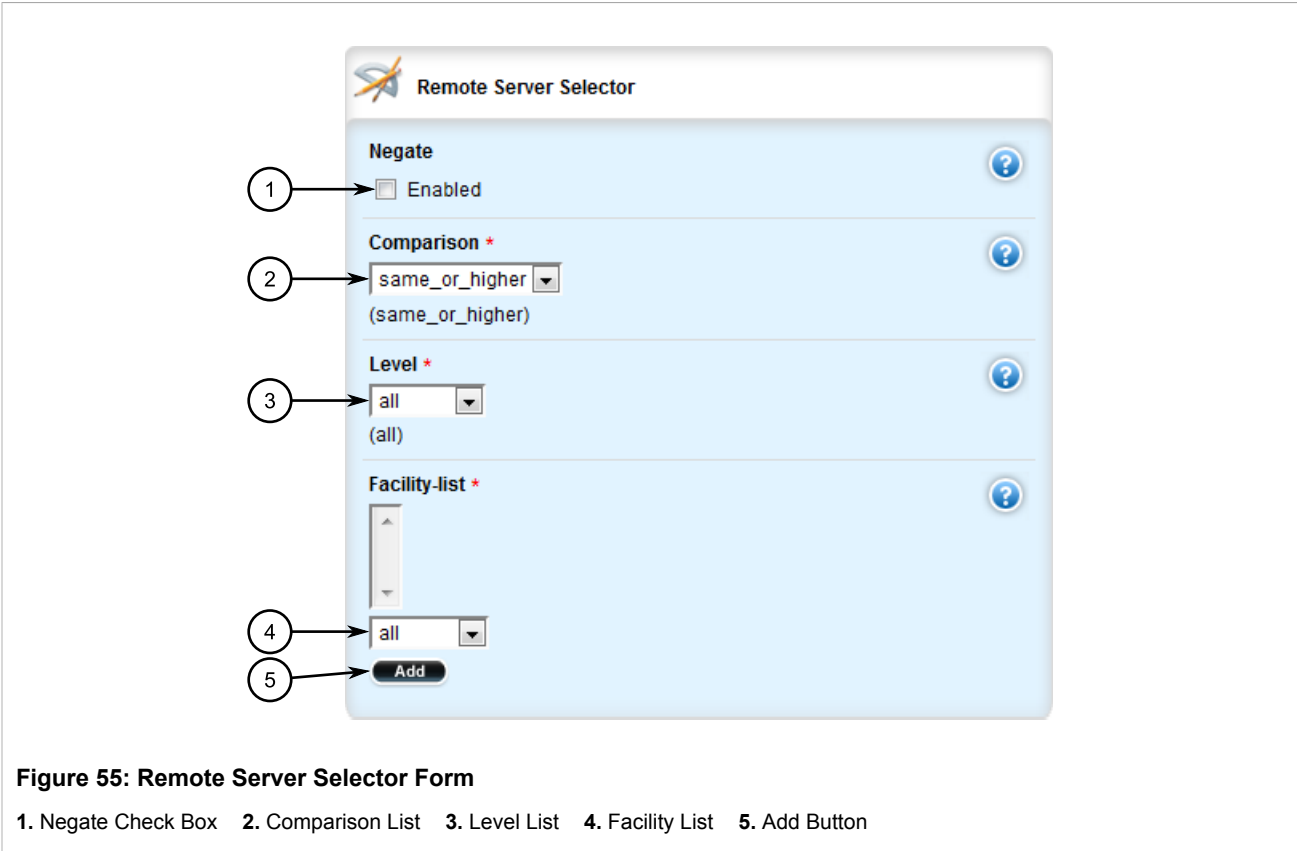
Figure 54: Key Settings Form

1. Name Box    2. Add Button

- 4. Configure the following parameter(s) as required:

Parameter	Description
Name	The log selector identifier. Enter an integer greater than 0; up to 8 selectors can be added. The log selector determines which subsystem messages are included in the log.

- 5. Click **Add**. The **Remote Server Selector** form appears.



**Figure 55: Remote Server Selector Form**

1. Negate Check Box    2. Comparison List    3. Level List    4. Facility List    5. Add Button

6. Configure the following parameter(s) as required:

Parameter	Description
Negate	<p><b>Synopsis:</b> typeless</p> <p>Excludes messages defined in the <code>&lt;emphasis&gt;Remote Server Selector&lt;/emphasis&gt;</code> fields from the log. Selecting this option acts as a logical NOT for the selector definition. For example: Selecting <code>&lt;emphasis role="bold"&gt;same&lt;/emphasis&gt;</code>, <code>&lt;emphasis role="bold"&gt;debug&lt;/emphasis&gt;</code>, and <code>&lt;emphasis role="bold"&gt;mail&lt;/emphasis&gt;</code> in the <code>&lt;emphasis&gt;Comparison&lt;/emphasis&gt;</code>, <code>&lt;emphasis&gt;Level&lt;/emphasis&gt;</code>, and <code>&lt;emphasis&gt;Facility-list&lt;/emphasis&gt;</code> fields includes debug messages from the mail subsystem in the log. Selecting <code>&lt;emphasis role="bold"&gt;Negate&lt;/emphasis&gt;</code> <code>&lt;emphasis&gt;excludes&lt;/emphasis&gt;</code> debug messages from the mail subsystem from the log.</p>
Comparison	<p><b>Synopsis:</b> { same_or_higher, same }</p> <p><b>Default:</b> same_or_higher</p> <p>The message severity levels to include in the log:</p> <ul style="list-style-type: none"><li><code>&lt;itemizedlist&gt;&lt;listitem&gt;&lt;emphasis role="bold"&gt;same:&lt;/emphasis&gt; includes only messages of the severity level selected in the <code>&lt;emphasis&gt;Level&lt;/emphasis&gt;</code> field.&lt;/listitem&gt;</code></li><li><code>&lt;listitem&gt;&lt;emphasis role="bold"&gt;same_or_higher:&lt;/emphasis&gt; includes messages of the severity level selected in the <code>&lt;emphasis&gt;Level&lt;/emphasis&gt;</code> field, and all messages of higher severity.&lt;/listitem&gt;&lt;/itemizedlist&gt;</code></li></ul> <p>For example: <code>&lt;itemizedlist&gt;&lt;listitem&gt;Selecting <code>&lt;emphasis role="bold"&gt;debug&lt;/emphasis&gt;</code> in the <code>&lt;emphasis&gt;Level&lt;/emphasis&gt;</code> field and <code>&lt;emphasis role="bold"&gt;same&lt;/emphasis&gt;</code> in the</code></p>

Parameter	Description
	<p>&lt;emphasis&gt;Comparison&lt;/emphasis&gt; field includes only debug messages in the log.&lt;/listitem&gt; &lt;listitem&gt;Selecting &lt;emphasis role="bold"&gt;debug&lt;/emphasis&gt; in the &lt;emphasis&gt;Level&lt;/emphasis&gt; field and &lt;emphasis role="bold"&gt;same_or_higher&lt;/emphasis&gt; in the &lt;emphasis&gt;Comparison&lt;/emphasis&gt; field includes debug and all higher severity messages in the log.&lt;/listitem&gt;&lt;/itemizedlist&gt;</p>
Level	<p><b>Synopsis:</b> { emerg, alert, crit, err, warning, notice, info, debug, none, all }</p> <p><b>Default:</b> all</p> <p>The base message severity level to include in the log. &lt;emphasis role="bold"&gt;all&lt;/emphasis&gt; includes all messages. &lt;emphasis role="bold"&gt;none&lt;/emphasis&gt; excludes all messages. Other levels are listed in order of increasing severity.</p>
Facility List	<p><b>Synopsis:</b> { auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, security, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7, all }</p> <p>The subsystems generating log messages. Messages from the selected subusystems are included in the log. At least one subsystem must be selected; up to 8 subsystems can be selected.</p>

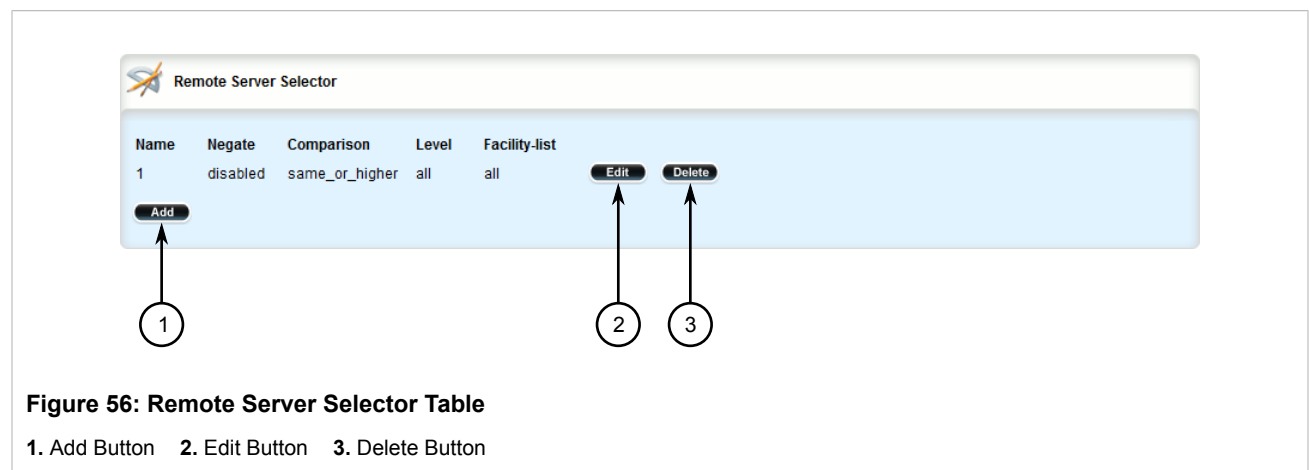
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 3.9.7.3

## Deleting a Remote Server Selector

To delete a remote server selector, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » logging » server » {address} » selector**, where {address} is the IP address of the remote server. The **Remote Server Selector** table appears.



- Click **Delete** next to the chosen remote server selector.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 3.10

## Managing the Software Configuration

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

The following sections describe how to save and load the RUGGEDCOM ROX II software configuration:

- [Section 3.10.1, “Saving the Configuration”](#)
- [Section 3.10.2, “Loading a Configuration”](#)

### Section 3.10.1

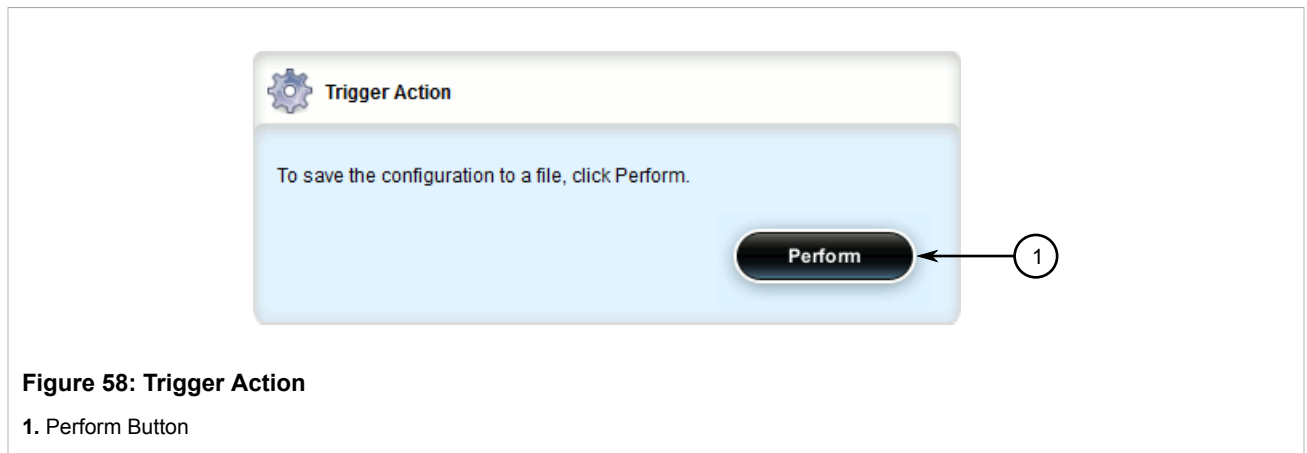
## Saving the Configuration

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

1. Navigate to **admin** and click **full-configuration-save** in the menu. The **Full Configuration Save** and **Trigger Action** forms appear.

**Figure 57: Full Configuration Save Form**

1. Format List    2. Filename Box



- On the **Full Configuration Save** form, configure the following parameters:

Parameter	Description
format	<b>Synopsis:</b> { cli } Save full configuration to a file.
file-name	<b>Synopsis:</b> A string 1 to 255 characters long

- On the **Trigger Action** form, click **Perform**.
- [Optional] Backup the configuration file to a USB mass storage drive. For more information, refer to [Section 3.8.4, “Backing Up Files”](#).

### Section 3.10.2

## 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.*

- [Optional] Install the configuration file on the device. For more information, refer to [Section 3.8.3, “Installing Files”](#).
- Navigate to **admin** and click **full-configuration-load** in the menu. The **Load Full Configuration** and **Trigger Action** forms appear.

**Figure 59: Load Full Configuration**

1. Format List 2. Filename Box

**Figure 60: Trigger Action**

1. Perform Button

- On the **Load Full Configuration** form, configure the following parameters:

Parameter	Description
format	<b>Synopsis:</b> { cli } Load a full configuration from a file
file-name	<b>Synopsis:</b> A string 1 to 255 characters long

- On the **Trigger Action** form, click **Perform**.

### Section 3.11

## Upgrading/Downgrading the RUGGEDCOM ROX II Software

The following sections describe how to upgrade and downgrade the RUGGEDCOM ROX II software:

- [Section 3.11.1, “Configuring the Upgrade Source”](#)
- [Section 3.11.2, “Setting Up an Upgrade Server”](#)

- [Section 3.11.3, “Upgrading the RUGGEDCOM ROX II Software”](#)
- [Section 3.11.4, “Stopping/Declining a Software Upgrade”](#)
- [Section 3.11.5, “Downgrading the RUGGEDCOM ROX II Software”](#)

## Section 3.11.1

## Configuring the Upgrade Source

Firmware for upgrading or downgrading RUGGEDCOM ROX II can be uploaded from either an upgrade server or a portable USB Mass Storage drive. For information about setting up an upgrade server, refer to [Section 3.11.2, “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 4.7.1.3, “Adding a CA Certificate and CRL”](#).

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » software-upgrade**. The **Upgrade Settings** form appears.

**Figure 61: Upgrade Settings Form**

1. Upgrade Server URL Box    2. Target ROX Version Box    3. Server CA Box

3. Configure the following parameter(s) as required:

Parameter	Description
Upgrade Server URL	<b>Synopsis:</b> A string  The URL for the upgrade server or file system. Supported URIs are HTTP, HTTPS and FTP. To upgrade from a USB flash drive or microSD/microSDHC drive (if applicable), the URL format is "usb://<usb-device-name>/path-to-repository" or "sd://sd-1//path-to-repository". Run "show chassis" to determine the name of the USB device. Note that only one single partition is supported for either data medium.
Target ROX Version	<b>Synopsis:</b> A string

Parameter	Description
	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.

- Click **Exit Transaction** or continue making changes.

## Section 3.11.2

## 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 host must also be able to download new software releases from [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom).
- The server must have sufficient disk space for at least two full software releases. Each full software release is approximately 75 Mbits, 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/`, which can be accessed via the CLI. For more information about viewing the contents of a file via the CLI, refer to the *RUGGEDCOM RUGGEDCOM ROX II v2.9 CLI User Guide*.

**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.*

The following sections describe how to configure an upgrade server:

- [Section 3.11.2.1, "Configuring the Upgrade Server"](#)
- [Section 3.11.2.2, "Adding Software Releases to the Upgrade Server"](#)

## Section 3.11.2.1

### 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, 2.9.1.*

File Type	File	Required MIME Type
RUGGEDCOM ROX II Image Archive	imager2.x.y.tar.bz2	application/x-bzip2
RUGGEDCOM ROX II Upgrade Archive	rr2/dists/rr2.x.y/Release (extracted from rr2.x.y.zip)	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 3.11.2.2

## Adding Software Releases to the Upgrade Server

Software releases are obtained from [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom) as compressed ZIP files.

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

1. Download the appropriate RUGGEDCOM ROX II software release from [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom) 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.*

2. 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. "rrX"). Subsequence releases will also be extracted to this folder.

Section 3.11.3

## 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 USB Mass Storage 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 3.11.4, "Stopping/Declining a Software Upgrade"](#).*



### NOTE

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

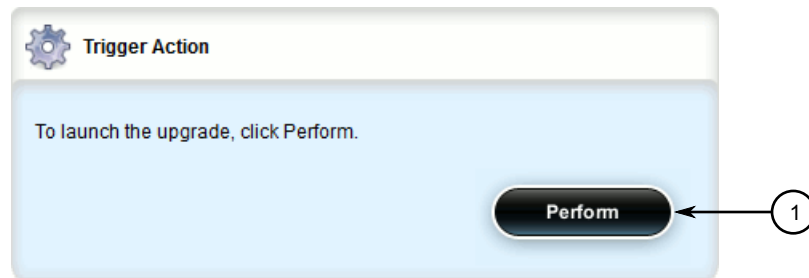


### NOTE

*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 USB Mass Storage drive, insert the drive in the USB port on the device. For more information, refer to the *RUGGEDCOM RX5000/MX5000/MX5000RE Installation Guide*.
2. Make sure the source of the software upgrade has been configured. For more information, refer to [Section 3.11.1, "Configuring the Upgrade Source"](#).
3. Change the mode to **Edit Private** or **Edit Exclusive**.
4. Navigate to **admin » software-upgrade** and click **launch-upgrade** in the menu. The **Trigger Action** form appears.



**Figure 62: Trigger Action Form**

1. Perform Button

5. Click **Perform**. The upgrade process begins.

To monitor the real-time progress of the software upgrade, navigate to **admin » software-upgrade** and view the **Upgrade Monitoring** form.

**Figure 63: Upgrade Monitoring Form**

1. Software Partition   2. Current Version   3. Upgrade Phase   4. Status Message   5. Phase 1: Filesystem Sync   6. Phase 2: Package Download   7. Phase 3: Package Installation   8. Last Attempt   9. Last Result

This form contains the following parameters:

Parameter	Description
software-partition	<p><b>Synopsis:</b> A string 1 to 31 characters long</p> <p>The current active partition number. The unit has two software partitions: #1 and #2. Upgrades are always performed to the other partition.</p>
Current Version	<p><b>Synopsis:</b> A string 1 to 31 characters long</p> <p>The current operating software version.</p>
Upgrade Phase	<p><b>Synopsis:</b> { Inactive, Estimating upgrade size, Copying filesystem, Downloading packages, Installing packages, Unknown state, Completed successfully, Failed, Uninstalling packages }</p> <p>The current phase or state of the upgrade. It is one of 'Estimating upgrade size', 'Copying filesystem', 'Downloading packages', 'Installing packages', 'Unknown state', 'Completed successfully', or 'Failed'. These phrases will not vary and any may be used programmatically for ascertaining state.</p>
status-message	<p><b>Synopsis:</b> A string</p> <p>Additional details on the status of the upgrade.</p>
Phase 1: Filesystem Sync (% complete)	<p><b>Synopsis:</b> An integer between 0 and 100</p> <p>Phase 1 of the upgrade involves synchronizing the filesystem with the partition you are upgrading to.</p> <p>This reflects the estimated percentage complete.</p>
Phase 2: Package Download (% complete)	<p><b>Synopsis:</b> An integer between 0 and 100</p> <p>Phase 2 of the upgrade downloads all packages that require an update. This reflects the estimated percentage complete.</p>
Phase 3: Package Installation (% complete)	<p><b>Synopsis:</b> An integer between 0 and 100</p> <p>Phase 3 of the upgrade installs all packages that require an update. This reflects the estimated percentage complete.</p>
Last Attempt	<p><b>Synopsis:</b> A string 1 to 64 characters long</p> <p>The date and time of the completion of the last upgrade attempt.</p>
Last Result	<p><b>Synopsis:</b> { Upgrade Successful, Upgrade Failed, Unknown, Reboot Pending, Not Applicable, Declined, Interrupted }</p> <p>Indicates whether or not the last upgrade was completed successfully</p>

- If the software upgrade is successful, reboot the device or decline the software upgrade. For more information about rebooting the device, refer to [Section 3.5, "Rebooting the Device"](#).

#### Section 3.11.4

## Stopping/Declining a Software Upgrade

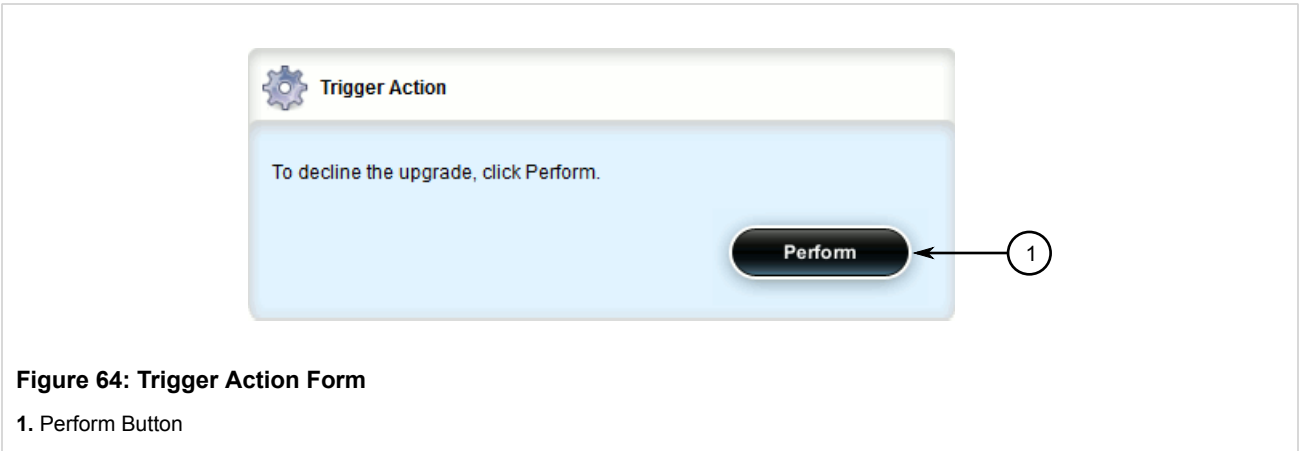
To stop/decline a recent software upgrade and revert back to the previously installed version, do the following:



### 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 3.11.5.1, "Rolling Back a Software Upgrade"](#).*

1. Navigate to **admin » software-upgrade** and click **decline-upgrade** in the menu. The **Trigger Action** form appears.



2. Click **Perform**.

#### Section 3.11.5

## Downgrading the RUGGEDCOM ROX II Software

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

The following sections describe the various methods for downgrading the RUGGEDCOM ROX II software:

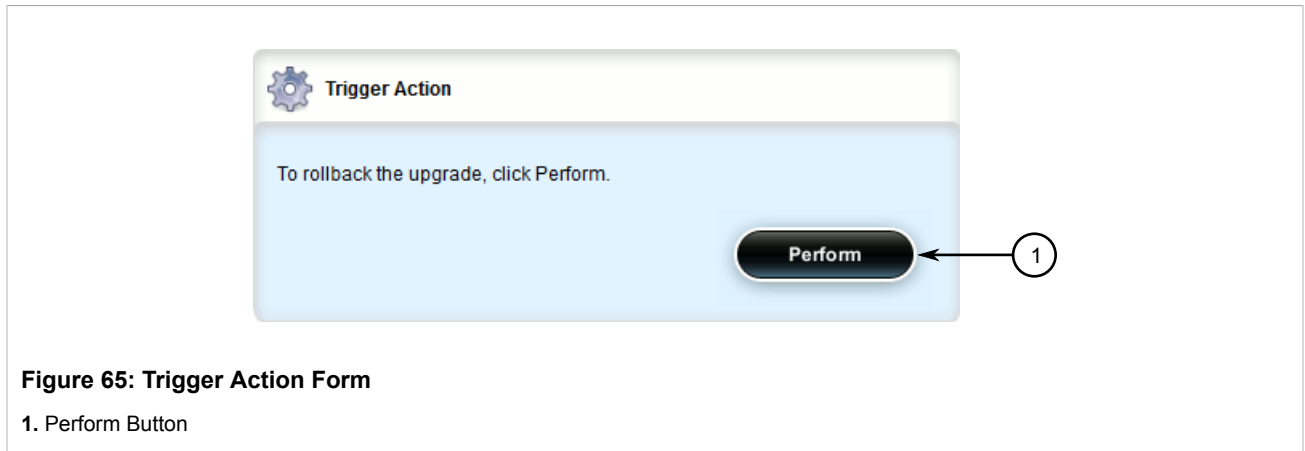
- [Section 3.11.5.1, “Rolling Back a Software Upgrade”](#)
- [Section 3.11.5.2, “Downgrading Using ROXflash”](#)

#### Section 3.11.5.1

### 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. Navigate to **admin » software-upgrade** and click **rollback-reboot** in the menu. The **Trigger Action** form appears.



- Click **Perform**. The device is automatically rebooted. Once the reboot is complete, the previously inactive partition containing the older software version is changed to an active state.

#### Section 3.11.5.2

### 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 3.11.3, "Upgrading the RUGGEDCOM ROX II Software"](#).*



#### IMPORTANT!

*When a USB Mass Storage drive is used, do not remove the drive during the file transfer.*

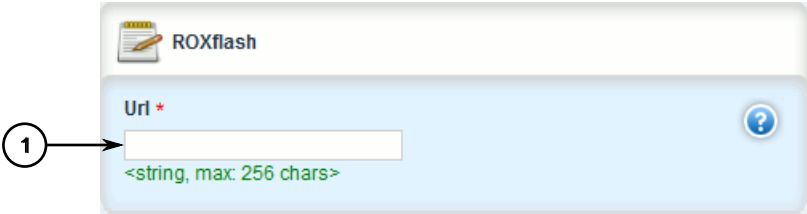


#### NOTE

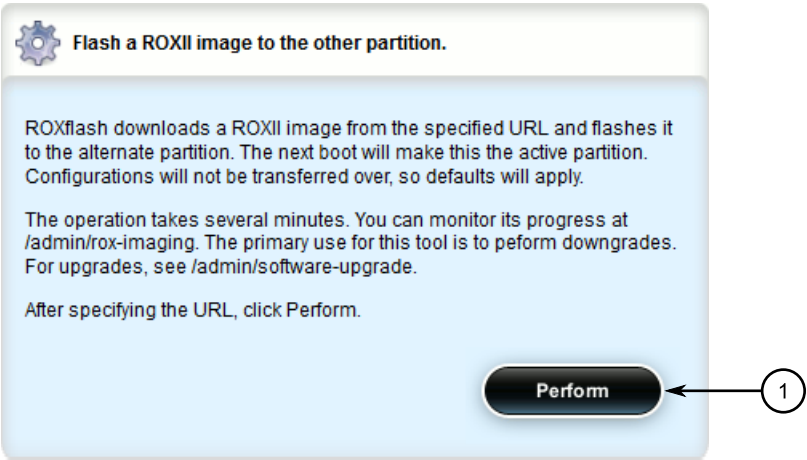
*If a major system failure is detected upon rebooting with the newly downgraded partition, the device will automatically roll back to the previously active partition.*

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

- If the source of the software is a USB Mass Storage drive, insert the drive in the USB port on the device. For more information, refer to the *RUGGEDCOM RX5000/MX5000/MX5000RE Installation Guide*.
- Navigate to **admin » rox-imaging** and click **roxflash** in the menu. The **ROXflash** and **Flash a ROXII image to the other partition** forms appear.

The screenshot shows a web form titled "ROXflash" with a yellow header bar containing a pencil icon. Below the header is a light blue box. Inside this box, the label "Url \*" is followed by a text input field. A circled number "1" with an arrow points to the input field. Below the input field, the text "<string, max: 256 chars>" is displayed in green. A blue question mark icon is located to the right of the input field.

**Figure 66: ROXflash Form**  
1. URL Box

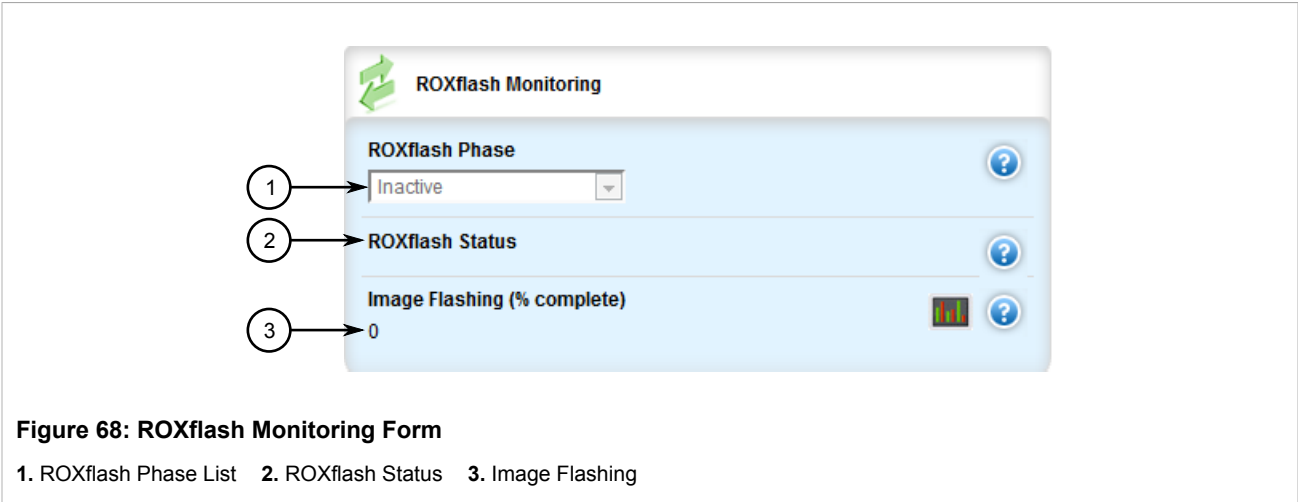
The screenshot shows a web form titled "Flash a ROXII image to the other partition." with a gear icon in the header. The form has a light blue background. It contains several paragraphs of text explaining the process: "ROXflash downloads a ROXII image from the specified URL and flashes it to the alternate partition. The next boot will make this the active partition. Configurations will not be transferred over, so defaults will apply." followed by "The operation takes several minutes. You can monitor its progress at /admin/rox-imaging. The primary use for this tool is to perform downgrades. For upgrades, see /admin/software-upgrade." and "After specifying the URL, click Perform." At the bottom right, there is a dark grey button labeled "Perform". A circled number "1" with an arrow points to the "Perform" button.

**Figure 67: Flash a ROXII image to the other partition Form**  
1. Perform Button

3. On the **ROXflash** form, configure the following parameters:

Parameter	Description
url	<b>Synopsis:</b> A string 1 to 256 characters long The URL of the ROX II image to download. Supported URIs are HTTP, HTTPS, FTP, USB and SD. To flash from a USB flash drive or microSD/microSDHC drive (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 the server does not require authentication, omit "user:password". When using the default port for the protocol, omit ":port".

4. Click **Perform**. ROXflash begins to flash the software image to the inactive partition.  
To monitor the real-time progress of the flashing process, navigate to **admin » rox-imaging** and view the **ROXflash Monitoring** form.



This form contains the following parameters:

Parameter	Description
ROXflash Phase	<b>Synopsis:</b> { Inactive, Downloading image, Imaging partition, Unknown state, Completed successfully, Failed } The current phase or state of the ROXflash operation. It is always one of the following: Inactive, Imaging partition, Unknown state, Completed successfully, or Failed. These phrases do not vary, and may be used programatically for ascertaining state.
ROXflash Status	<b>Synopsis:</b> A string 1 to 1024 characters long Detailed messages about ROXflash progress or errors.
Image Flashing (% complete)	<b>Synopsis:</b> An integer between 0 and 100 Indicates the imaging progress and the percentage that is complete.

5. If the software is successfully downgraded, reboot the device. For more information about rebooting the device, refer to [Section 3.5, “Rebooting the Device”](#).

Section 3.12

# Managing RUGGEDCOM ROX II Applications

RUGGEDCOM ROX II applications are special add-ons that extend the functionality of ROX, such as enhanced support for other ROX products (e.g. RUGGEDCOM CROSSBOW, RUGGEDCOM ELAN, etc.). 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 3.11.2, “Setting Up an Upgrade Server”](#).

The following sections describe how to manage ROX applications on the device:

- [Section 3.12.1, “Viewing a List of Installed Applications”](#)

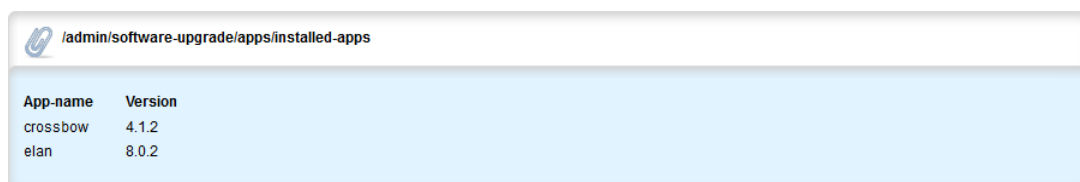


- [Section 3.12.2, “Installing an Application”](#)
- [Section 3.12.3, “Upgrading an Application”](#)
- [Section 3.12.4, “Uninstalling an Application”](#)
- [Section 3.12.5, “Managing Application Repositories”](#)

## Section 3.12.1

## Viewing a List of Installed Applications

To view a list of RUGGEDCOM ROX II applications installed on the device, navigate to **admin » software-upgrade » apps » installed-apps**. If applications have been installed, the **Installed Apps** table appears.



App-name	Version
crossbow	4.1.2
elan	8.0.2

Figure 69: Installed Apps Table

If no applications have been installed, install applications as needed. For more information, refer to [Section 3.12.2, “Installing an Application”](#).

## Section 3.12.2

## Installing an Application

To install an application, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure a repository for the application has been configured before installing the application. For more information, refer to [Section 3.12.5.3, “Adding a Repository”](#).
3. Navigate to **admin » software-upgrade » apps** and click **install-app** in the menu. The **Install App** and **Trigger Action** forms appear.

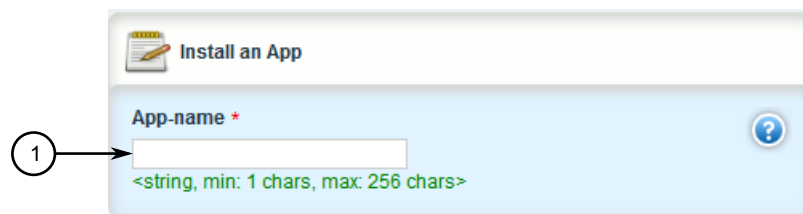
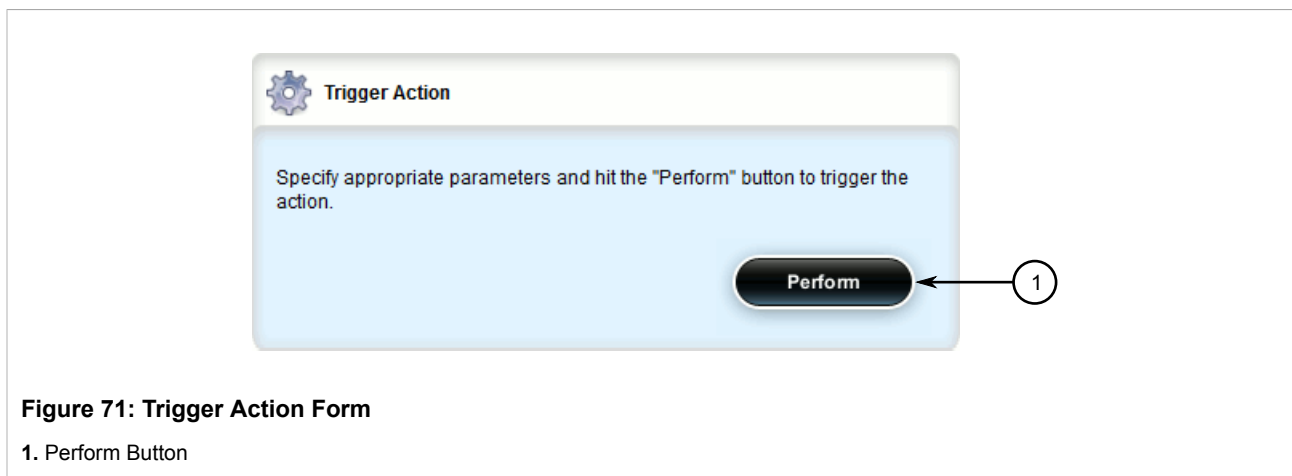


Figure 70: Install App Form

1. App Name Box



- On the **Install Apps** form, configure the following parameters:

Parameter	Description
app-name	<p><b>Synopsis:</b> A string 1 to 256 characters long</p> <p>The name of the app to install as it appears in the repository configuration. To install more than one app, use a comma-separated list.</p>

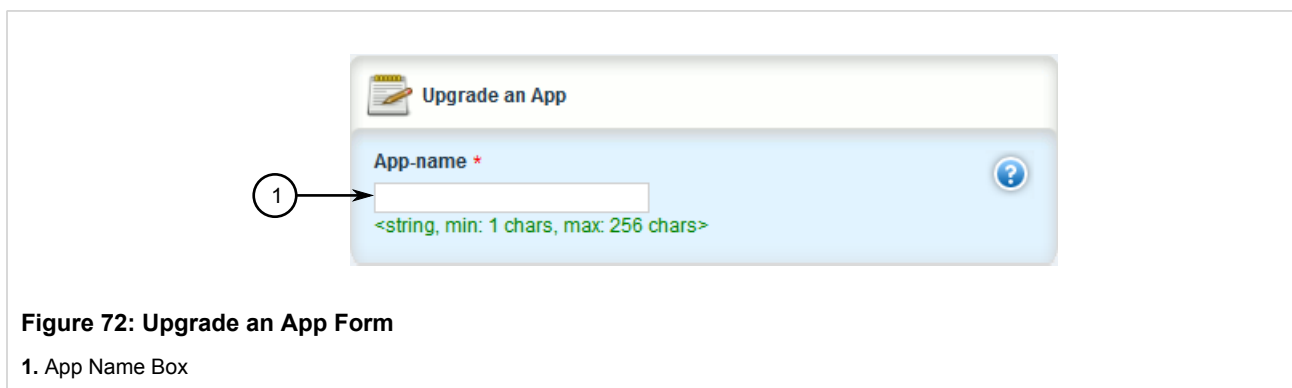
- On the **Trigger Action** form, click **Perform**.

### Section 3.12.3

## Upgrading an Application

To upgrade an application, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » software-upgrade » apps** and click **upgrade-app** in the menu. The **Upgrade an App** and **Trigger Action** forms appear.



**Figure 73: Trigger Action Form**

1. Perform Button

- On the **Upgrade Apps** form, configure the following parameters:

Parameter	Description
app-name	<b>Synopsis:</b> A string 1 to 256 characters long The name of the app to upgrade as it appears in the repository configuration. To upgrade more than one app, use a comma-separated list.

- On the **Trigger Action** form, click **Perform**.

#### Section 3.12.4

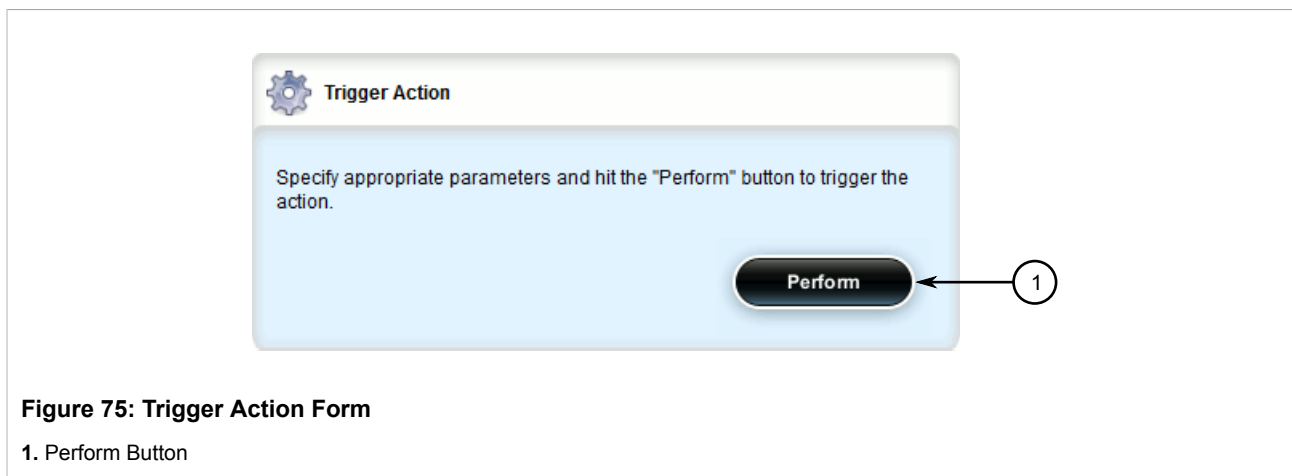
## Uninstalling an Application

To uninstall an application, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » software-upgrade » apps** and click **uninstall-app** in the menu. The **Uninstall Apps** and **Trigger Action** forms appear.

**Figure 74: Uninstall Apps Form**

1. App Name Box



- On the **Uninstall Apps** form, configure the following parameters:

Parameter	Description
app-name	<p><b>Synopsis:</b> A string 1 to 256 characters long</p> <p>The name of the app to uninstall as it appears in the repository configuration. To uninstall more than one app, use a comma-separated list.</p>

- On the **Trigger Action** form, click **Perform**.

#### Section 3.12.5

## 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.



### NOTE

*Multiple applications can be installed or upgraded at the same time. Therefore, multiple repositories may be configured.*

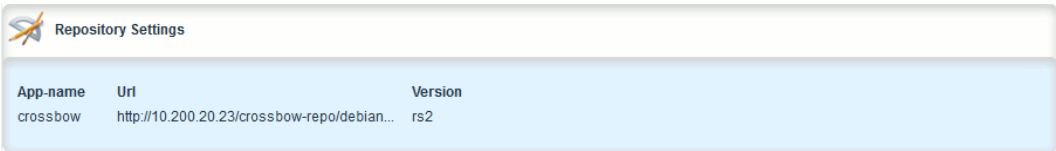
The following sections describe how to configure and manage ROX application repositories:

- [Section 3.12.5.1, “Viewing a List of Repositories”](#)
- [Section 3.12.5.2, “Checking the Repository Connection”](#)
- [Section 3.12.5.3, “Adding a Repository”](#)
- [Section 3.12.5.4, “Deleting a Repository”](#)

#### Section 3.12.5.1

### Viewing a List of Repositories

To view a list of RUGGEDCOM ROX II application repositories, navigate to **admin » software-upgrade » apps » repository**. If repositories have been configured, the **Repository Settings** table appears.



App-name	Url	Version
crossbow	http://10.200.20.23/crossbow-repo/debian...	rs2

Figure 76: Repository Settings Table

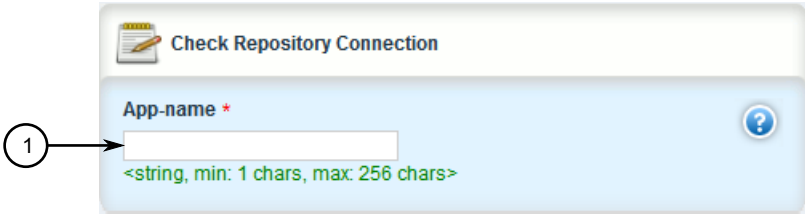
If no repositories have been configured, add repositories as needed. For more information, refer to [Section 3.12.5.3, “Adding a Repository”](#).

Section 3.12.5.2

Checking the Repository Connection

To check the connection with a repository, do the following:

- 1. Navigate to **admin » software-upgrade » apps** and click **check-repository-connection** in the menu. The **Check Repository Connection** and **Trigger Action** forms appear.

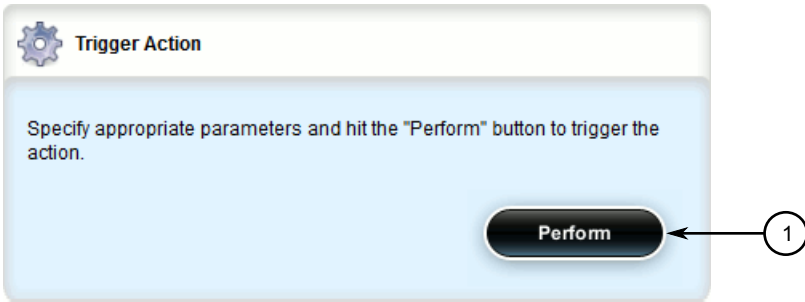


1 →

<string, min: 1 chars, max: 256 chars>

Figure 77: Check Repository Connection Form

- 1. App Name Box



Trigger Action

Specify appropriate parameters and hit the "Perform" button to trigger the action.

Perform → 1

Figure 78: Trigger Action Form

- 1. Perform Button

- 2. On the **Check Repository Connection** form, configure the following parameters:

Parameter	Description
app-name	<b>Synopsis:</b> A string 1 to 256 characters long

Parameter	Description
	The name of a configured app repository as it appears in the repository configuration. To check more than one repository, use a comma-separated list.

- On the **Trigger Action** form, click **Perform**. The connection results are displayed.

### Section 3.12.5.3

## 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.*

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » software-upgrade » apps » repository** and click **<Add repository>**. The **Key Settings** form appears.

**Figure 79: Key Settings Form**

1. App Name Box    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
app-name	<b>Synopsis:</b> A string 1 to 32 characters long The name of the app to upgrade or install. This name must be accurate. Consult the release notes for the app.

- Click **Add** to create the repository connection. The **Repository** form appears.

**Figure 80: Repository Form**

1. URL Box 2. Version Box

5. Configure the following parameter(s) as required:

Parameter	Description
url	<b>Synopsis:</b> A string 1 to 1024 characters long The URL of the upgrade server hosting the app repository (http, https, and ftp are supported).
version	<b>Synopsis:</b> A string 1 to 64 characters long The version of the app you are installing or upgrading.

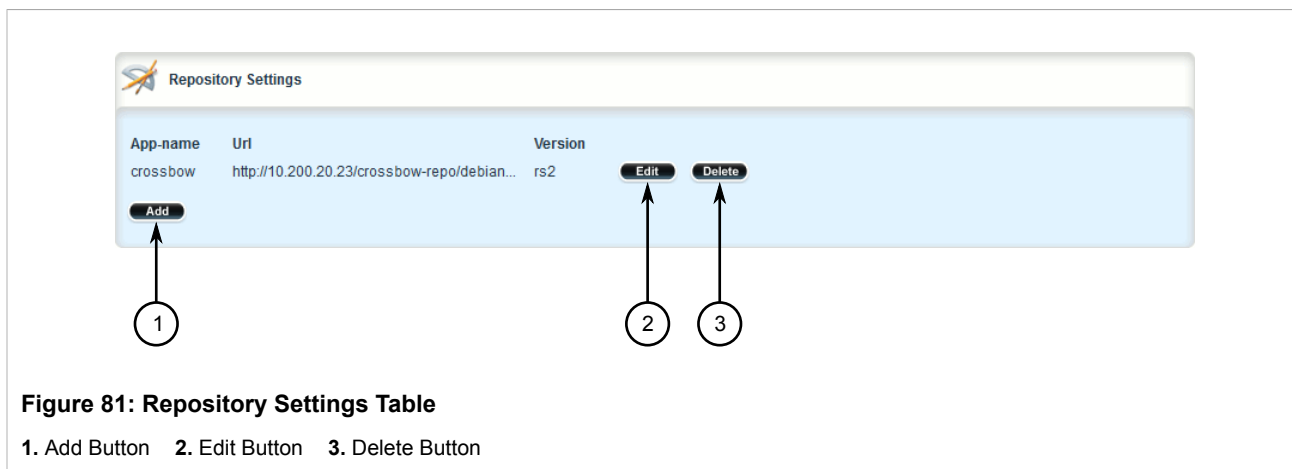
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 3.12.5.4

### Deleting a Repository

To delete an application repository, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » software-upgrade » apps » repository**. The **Repository Settings** table appears.



3. Click the **Delete** next to the chosen repository.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 3.13

## 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. This feature key is independent of the compact flash card or USB Mass Storage drive, and is retained by the device itself should the card be replaced. Additional file-based feature keys can be added as needed. File-based feature keys are stored on the compact flash card or a USB Mass Storage drive, and can be moved from device to device.

**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 [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom) or contact a Siemens Sales representative.*

**NOTE**

*File-based feature keys can be used on different devices. To tie a feature key to a specific device, contact a Siemens Canada Ltd. Sales representative to arrange for a RMA (Return to Manufacturer Authorization) to program the feature key into the device.*

When ordering feature levels, make sure to provide the *main* serial number and *cm* serial number for the device. An upgraded feature key file will be provided that is licensed to the device. For information on how to determine the *main* serial number and *cm* serial number, refer to [Section 3.1, “Determining the Product Version”](#).

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. For information on how to install new feature keys, refer to [Section 3.8.3, “Installing Files”](#).

For information on how to backup a feature key, refer to [Section 3.8.4, “Backing Up Files”](#).



To view the contents of a feature key, refer to the *RUGGEDCOM ROX II v2.9 CLI Web Interface User Guide* for the RUGGEDCOM RX5000/MX5000/MX5000RE.

Section 3.14

## Managing the Fan Controller

RUGGEDCOM RX5000/MX5000/MX5000RE devices may be equipped with an optional fan module to monitor and control the temperature of the device. When the internal temperature exceeds a user-specified value, one of the three fan arrays will activate automatically.

The following sections describe how to setup and monitor the fan controller:

- [Section 3.14.1, “Viewing the Fan Controller Status”](#)
- [Section 3.14.2, “Configuring the Activation Temperature”](#)

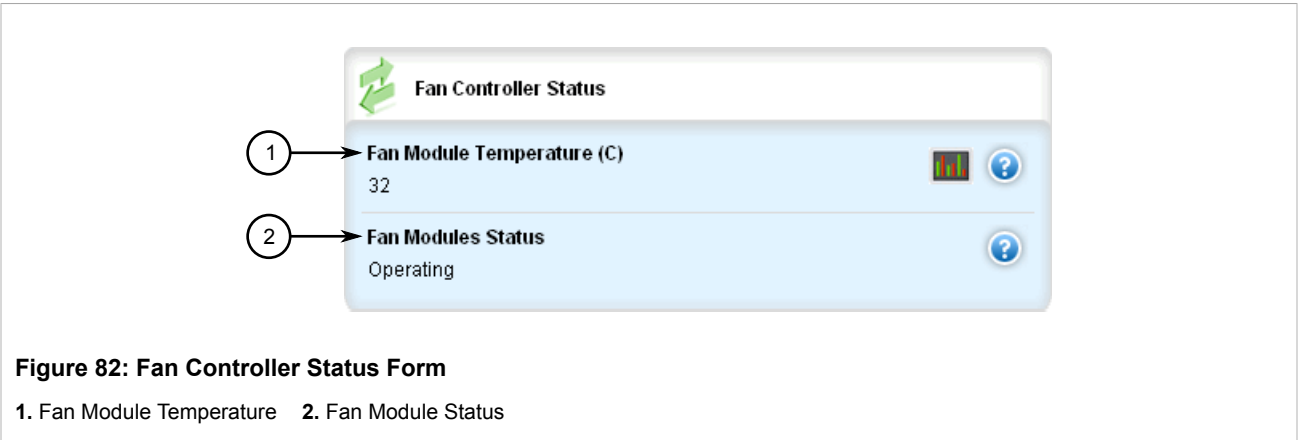
Section 3.14.1

### Viewing the Fan Controller Status

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

To view the status of the fan controller, do the following:

- Navigate to **chassis » fan-controller » status**. The **Fan Controller Status** form appears.



This form contains the following parameters:

Parameter	Description
Fan Module Temperature (C)	<b>Synopsis:</b> An integer between 55 and 125 The external temperature reading adjacent to the fans.
Fan Modules Status	<b>Synopsis:</b> A string 1 to 255 characters long Additional status details for the fan module.

To view the status of the individual fan arrays, do the following:

- Navigate to **chassis » fan-controller » status » fan**. The **Fan Status** form appears.

Fan ID	Fan State	Fan Status
fanA	standby	Normal
fanB	off	Normal

**Figure 83: Fan Status Form**  
1. Fan ID   2. Fan State   3. Fan Status

This form contains the following parameters:

Parameter	Description
Fan ID	<b>Synopsis:</b> A string 1 to 31 characters long The name of the fan module as it appears on the device.

Section 3.14.2

# Configuring the Activation Temperature

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

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

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *chassis » fan-controller*. The **Fan Controller** form appears.

1. Activation Temperature Box

**Figure 84: Fan Controller Form**  
1. Activation Temperature Box

- 3. Configure the following parameter(s) as required:

Parameter	Description
Activation Temperature (C)	<b>Synopsis:</b> An integer between 25 and 85 <b>Default:</b> 50

Parameter	Description
	The temperature above which the fans will be activated. The minimum and maximum values of this parameter are 25C and 85C.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 3.15

## Managing Fixed Modules

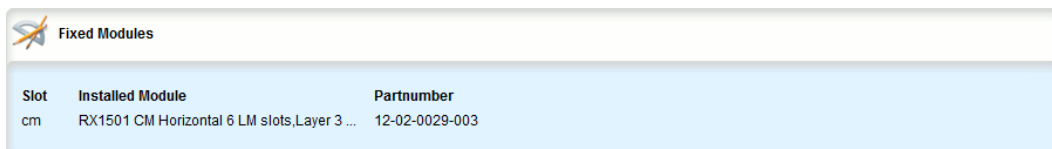
The following sections describe how to configure and manage fixed modules:

- [Section 3.15.1, “Viewing a List of Fixed Module Configurations”](#)
- [Section 3.15.2, “Adding a Fixed Module Configuration”](#)
- [Section 3.15.3, “Deleting a Fixed Module Configuration”](#)

## Section 3.15.1

### Viewing a List of Fixed Module Configurations

To view a list of fixed module configurations, navigate to **chassis » fixed-modules**. If fixed modules have been configured, the **Fixed Modules** table appears.



Fixed Modules		
Slot	Installed Module	Partnumber
cm	RX1501 CM Horizontal 6 LM slots, Layer 3 ...	12-02-0029-003

Figure 85: Fixed Modules Table

If no fixed modules have been configured, add fixed module configurations as needed. For more information, refer to [Section 3.15.2, “Adding a Fixed Module Configuration”](#).

## Section 3.15.2

### Adding a Fixed Module Configuration

To add a configuration for a fixed module, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **chassis » fixed-modules** and click **<Add fixed-module>**. The **Key Settings** form appears.

**Figure 86: Key Settings Form**

1. Slot Box 2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
slot	<p><b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, cm, em, trnk }</p> <p>The slot name, as marked on the silkscreen across the top of the chassis.</p>

- Click **Add**. The **Fixed Modules** form appears.

**Figure 87: Fixed Modules Form**

1. Installed Module Box 2. Part Number Box

- Configure the following parameter(s) as required:

Parameter	Description
Installed Module	<p><b>Synopsis:</b> A string 1 to 60 characters long</p> <p>The module type to be used in this slot.</p>
partnumber	<p><b>Synopsis:</b> A string 1 to 74 characters long</p> <p>The part number of the module type in this slot.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

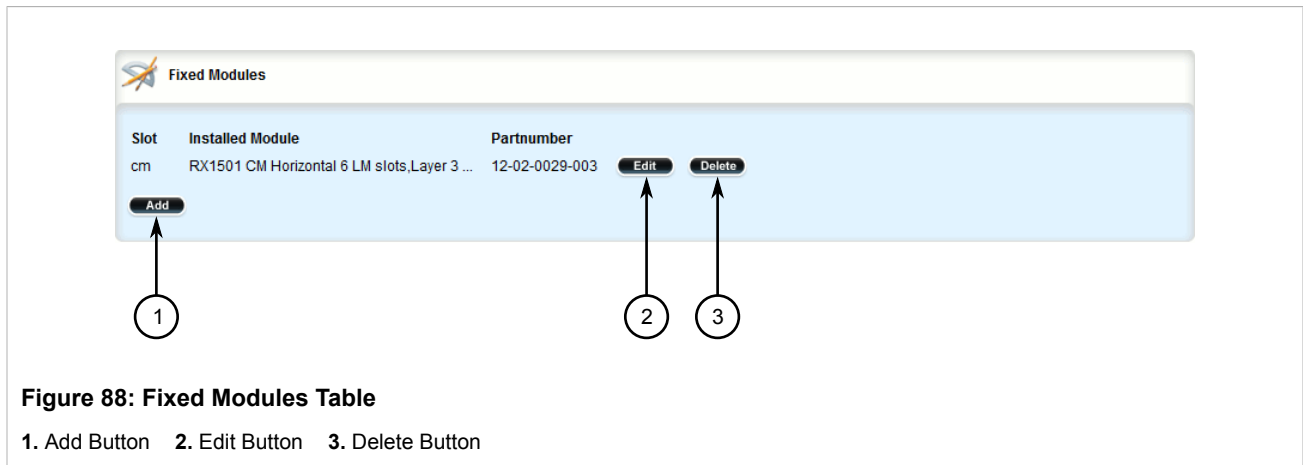
- Click **Exit Transaction** or continue making changes.

### Section 3.15.3

## Deleting a Fixed Module Configuration

To delete the configuration for a fixed module, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **chassis » fixed-modules**. The **Fixed Modules** table appears.



- Click **Delete** next to the chosen fixed module configuration.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 3.16

## Managing Line Modules

The following sections describe how to properly add, replace and configure line modules:

- [Section 3.16.1, “Removing a Line Module”](#)
- [Section 3.16.2, “Installing a New Line Module”](#)
- [Section 3.16.3, “Viewing a List of Line Module Configurations”](#)
- [Section 3.16.4, “Configuring a Line Module”](#)

### Section 3.16.1

## Removing a Line Module

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

- Shut down the device. The device will shutdown for a period of time before rebooting and restarting. The default time-out period is 300 seconds (five minutes). If more time is required to complete the procedure,

disconnect power from the device during the time-out period. For more information on how to shutdown the device, refer to [Section 3.4, “Shutting Down the Device”](#).

2. Remove the line module from the device.

### Section 3.16.2

## Installing a New Line Module

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

1. If equipped, remove the line module currently installed in the slot. For more information, refer to [Section 3.16.1, “Removing a Line Module”](#).
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to **chassis » line-modules » line-module » {slot}**, where **{slot}** is the name of the module location. The **Modules** form appears.

**Figure 89: Modules Form**

1. Detected Module Box    2. Module Type List    3. Admin State Check Box

4. Under **Module Type**, select **none** from the list. This allows RUGGEDCOM ROX II to automatically detect the new module during the next startup.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.
7. Shut down the device. The device will shutdown for a period of time before rebooting and restarting. The default time-out period is 300 seconds (five minutes). If more time is required to complete the procedure, disconnect power from the device during the time-out period. For more information on how to shutdown the device, refer to [Section 3.4, “Shutting Down the Device”](#).
8. Insert the new line module into the empty slot in the chassis.
9. Reboot the device. For more information, refer to [Section 3.5, “Rebooting the Device”](#).  
After the device is rebooted, the new line module is automatically detected and operational.
10. If the line module is different from the previous module installed in the same slot, configure the new line module. For more information, refer to [Section 3.16.4, “Configuring a Line Module”](#).

Section 3.16.3

# Viewing a List of Line Module Configurations

To view a list of line module configurations, navigate to **chassis » line-modules**. If line modules have been configured, the **Modules** table appears.

Slot	Detected-module	Module Type	Admin State
Im1	1000TX w/ 2x RJ45	1000TX w/ 2x RJ45	enabled
Im2	none	none	disabled
Im3	6x RS232/RS422/RS485 via RJ45	6x RS232/RS422/RS485 via RJ45	enabled
Im4	none	none	disabled
Im5	none	none	disabled
Im6	none	none	disabled

Figure 90: Modules Table

If no line modules have been configured, install line module as needed. For more information, refer to [Section 3.16.2, “Installing a New Line Module”](#).

Section 3.16.4

# Configuring a Line Module

To configure a line module, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **chassis » line-modules » {module}**, where *{module}* is the line module. The **Modules** form appears.

The screenshot shows the 'Modules' configuration form. It has three main sections: 'Detected-module' with a text input showing 'none', 'Module Type' with a dropdown menu showing 'none', and 'Admin State' with a checkbox labeled 'Enabled'. Each section has a blue question mark icon to its right. Three numbered callouts are present: 1 points to the 'Detected-module' input, 2 points to the 'Module Type' dropdown, and 3 points to the 'Admin State' checkbox.

Figure 91: Modules Form

1. Detected Module    2. Module Type List    3. Admin State Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Detected Module	<b>Synopsis:</b> A string 1 to 60 characters long The installed module's type specifier.
Module Type	Sets the module type to be used in this slot.
Admin State	<b>Synopsis:</b> typeless Sets the administrative state for a module. Enabling the module powers it on.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

**NOTE**

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

- Click **Exit Transaction** or continue making changes.

## Section 3.17

## 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.*

The following sections describe how to configure and manage event trackers:

- [Section 3.17.1, "Viewing a List of Event Trackers"](#)
- [Section 3.17.2, "Viewing Event Tracker Statistics"](#)
- [Section 3.17.3, "Adding an Event Tracker"](#)
- [Section 3.17.4, "Deleting an Event Tracker"](#)

## Section 3.17.1

### Viewing a List of Event Trackers

To view a list of event trackers, navigate to **global » tracking**. If event trackers have been configured, the **Event** table appears.



Event							
Name	Target	Source IP	Source Interface	Timeout (ms)	Interval (ms)	Fall	Rise
host-in-lan-11	192.168.11.100	not found	not found	500	500	3	3

Figure 92: Event Table

If no event trackers have been configured, add event trackers as needed. For more information, refer to [Section 3.17.3, “Adding an Event Tracker”](#).

Section 3.17.2

Viewing Event Tracker Statistics

RUGGEDCOM ROX II records statistics for each event tracker.



To view the statistics for an event tracker, navigate to *global » tracking » event » {name}*, where {name} is the name of the event tracker. The **Statistics** form appears.

Statistics

1

Echo Attempts



---



2

Echo Replies


---



3

Min RTT


---



4

Average RTT


---



5

Max RTT

---



6

Standard Deviation RTT

---




Figure 93: Statistics Form

1. Echo Attempts    2. Echo Replies    3. Min RTT    4. Average RTT    5. Max RTT    6. Standard Deviation RTT

This form provides the following information:

Parameter	Description
Echo Attempts	The number of echo attempts.
Echo Replies	The number of echo replies.
Min RTT	<b>Synopsis:</b> A string

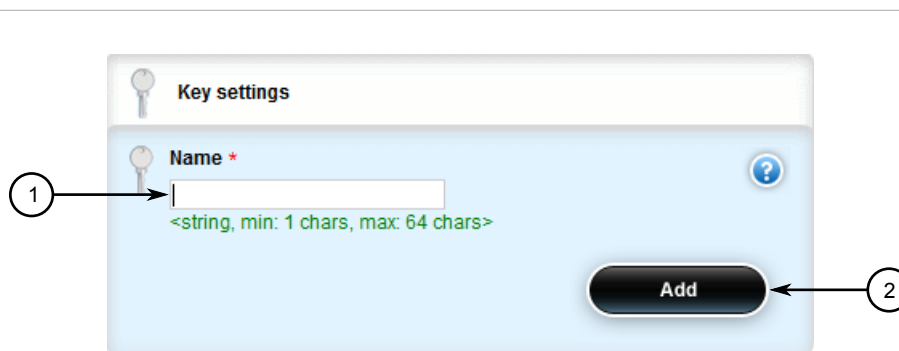
Parameter	Description
	The minimum of the round trip time (in milliseconds).
Average RTT	<b>Synopsis:</b> A string The average of the round trip time (in milliseconds).
Max RTT	<b>Synopsis:</b> A string The maximum of the round trip time (in milliseconds).
Standard Deviation RTT	<b>Synopsis:</b> A string The standard deviation of the round trip time (in milliseconds).

### Section 3.17.3

## Adding an Event Tracker

To add an event tracker, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **global » tracking** and click **<Add event>**. The **Key Settings** form appears.



**Figure 94: Key Settings Form**

1. Name Box 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 4095 characters long The name of the event.

4. Click **Add**. The **Event** form appears.

**Figure 95: Event Form**

1. Target Box   2. Source IP Box   3. Source Interface Box   4. Timeout Box   5. Interval Box   6. Fall Box   7. Rise Box   8. State Box

5. Configure the following parameter(s) as required:

Parameter	Description
Target	<b>Synopsis:</b> A string Configures the ping target as an IPv4 address or hostname.domain.
Source IP	<b>Synopsis:</b> 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	Forces a ping on a selected interface.
Timeout (ms)	Determines how many milliseconds to wait for the ICMP response.
Interval (ms)	<b>Synopsis:</b> A number with a value of 100 or greater

Parameter	Description
	Determines how many milliseconds to wait before sending another ICMP request.
Fall	<b>Synopsis:</b> An integer The number of times a failure occurs before changing the tracking state from up to down.
Rise	<b>Synopsis:</b> An integer The number of times success occurs before changing the tracking state from down to up.
state	<b>Synopsis:</b> { up, down } <b>Default:</b> up The state of the event.

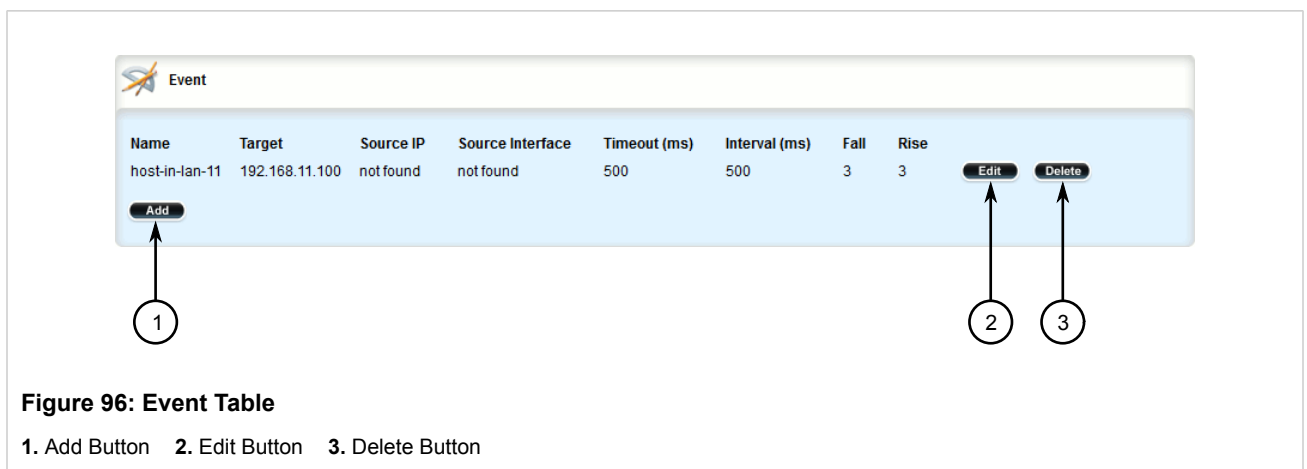
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 3.17.4

## Deleting an Event Tracker

To delete an event tracker, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **global » tracking**. The **Event** table appears.



- Click **Delete** next to the chosen event tracker.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 3.18

## Managing Switched Ethernet Ports

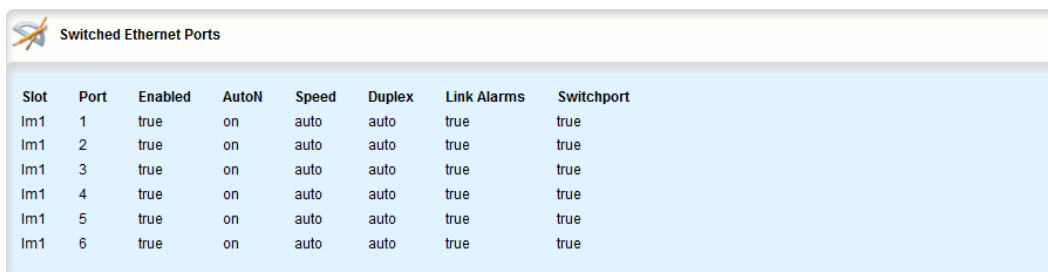
The following sections describe how to configure and manage switched Ethernet ports:

- [Section 3.18.1, “Viewing a List of Switched Ethernet Ports”](#)
- [Section 3.18.2, “Configuring a Switched Ethernet Port”](#)
- [Section 3.18.3, “Configuring Port Security”](#)
- [Section 3.18.4, “Viewing Switched Ethernet Port Statistics”](#)
- [Section 3.18.5, “Viewing RMON Port Statistics”](#)
- [Section 3.18.6, “Clearing Switched Ethernet Port Statistics”](#)
- [Section 3.18.7, “Resetting a Switched Ethernet Port”](#)
- [Section 3.18.8, “Testing Switched Ethernet Port Cables”](#)

## Section 3.18.1

### Viewing a List of Switched Ethernet Ports

To view a list of switched Ethernet ports configured on the device, navigate to **interface » switch**. The **Switched Ethernet Ports** table appears.



The screenshot shows a web interface window titled "Switched Ethernet Ports" with a table containing 8 columns: Slot, Port, Enabled, AutoN, Speed, Duplex, Link Alarms, and Switchport. The table lists 6 rows of data for slot Im1, with ports 1 through 6. All ports are enabled, have AutoN on, and are set to auto speed and duplex. Link Alarms are true for all ports, and the Switchport column is true for all ports.

Slot	Port	Enabled	AutoN	Speed	Duplex	Link Alarms	Switchport
Im1	1	true	on	auto	auto	true	true
Im1	2	true	on	auto	auto	true	true
Im1	3	true	on	auto	auto	true	true
Im1	4	true	on	auto	auto	true	true
Im1	5	true	on	auto	auto	true	true
Im1	6	true	on	auto	auto	true	true

Figure 97: Switched Ethernet Ports Table

## Section 3.18.2

### Configuring a Switched Ethernet Port

To configure a switched Ethernet port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » switch » {slot/port}**, where *{slot/port}* is the slot name and port number of the switched Ethernet port. The **Switched Ethernet Ports**, **Rate Limiting**, **LLDP**, **Multicast Filtering**, **CoS** and **VLAN** forms appear.

**NOTE**

*The Proxyarp, Mtu and Alias parameters are only available when the port is in dedicated routing mode.*

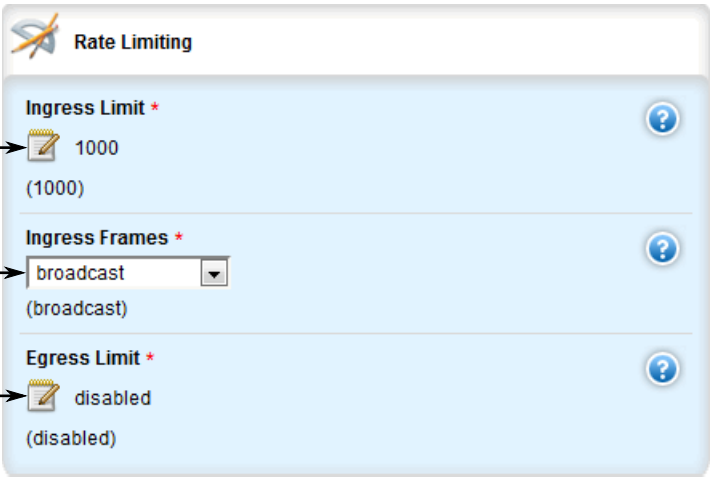
The screenshot shows the 'Switched Ethernet Ports' configuration form. It contains the following fields and settings, with numbered callouts on the left:

- 1** points to the **Enabled \*** checkbox, which is checked and labeled 'Enabled (true)'.
- 2** points to the **AutoN \*** dropdown menu, which is set to 'on'.
- 3** points to the **Speed \*** dropdown menu, which is set to 'auto'.
- 4** points to the **Duplex \*** dropdown menu, which is set to 'auto'.
- 5** points to the **Link Alarms \*** checkbox, which is checked and labeled 'Enabled (true)'.
- 6** points to the **Switchport** checkbox, which is unchecked.
- 7** points to the **Flow Control** checkbox, which is unchecked.
- 8** points to the **On-demand** checkbox, which is unchecked.
- 9** points to the **Ip-address-src** dropdown menu, which is set to 'static'.
- 10** points to the **Proxyarp** checkbox, which is unchecked.
- 11** points to the **Mtu \*** field, which is set to '1500 (1500)'.
- 12** points to the **Alias** field, which is empty.

Each field has a blue question mark icon to its right. There are also yellow bell icons next to the 'Switchport', 'Ip-address-src', and 'Alias' fields.

**Figure 98: Switched Ethernet Ports Form**

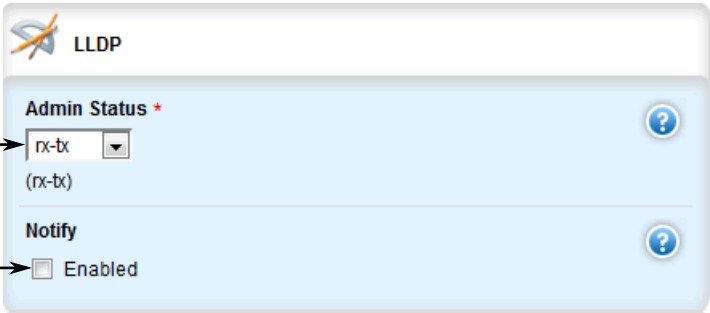
1. Enabled Check Box   2. AutoN List   3. Speed List   4. Duplex List   5. Link Alarms Check Box   6. Switchport Check Box  
7. Flow Control Check Box   8. On-Demand Check Box   9. ip-address-src List   10. Proxyarp Check Box   11. Mtu Box   12. Alias Box



The Rate Limiting form is titled "Rate Limiting" and contains three sections. The first section, "Ingress Limit \*", has a value of "1000" with "(1000)" below it. The second section, "Ingress Frames \*", has a dropdown menu showing "broadcast" with "(broadcast)" below it. The third section, "Egress Limit \*", has a value of "disabled" with "(disabled)" below it. Each section has a blue question mark icon to its right. Numbered callouts 1, 2, and 3 point to the "Ingress Limit", "Ingress Frames", and "Egress Limit" sections respectively.

Figure 99: Rate Limiting Form

1. Ingress Limit Box    2. Ingress Frames List    3. Egress Limit Box



The LLDP form is titled "LLDP" and contains two sections. The first section, "Admin Status \*", has a dropdown menu showing "rx-tx" with "(rx-tx)" below it. The second section, "Notify", has a checkbox labeled "Enabled". Each section has a blue question mark icon to its right. Numbered callouts 1 and 2 point to the "Admin Status" and "Notify" sections respectively.

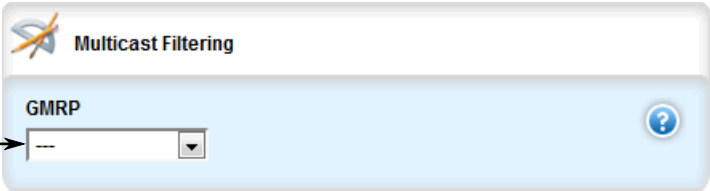
Figure 100: LLDP Form

1. Admin Status List    2. Notify Check Box



**NOTE**

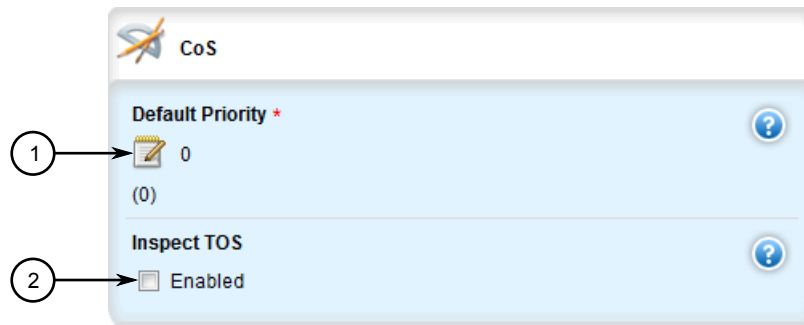
Parameters on the **Multicast Filtering**, **CoS** and **VLAN** forms are only available when the port is in switchport mode.



The Multicast Filtering form is titled "Multicast Filtering" and contains one section, "GMRP", with a dropdown menu showing "---". A blue question mark icon is to the right of the section. A numbered callout 1 points to the "GMRP" section.

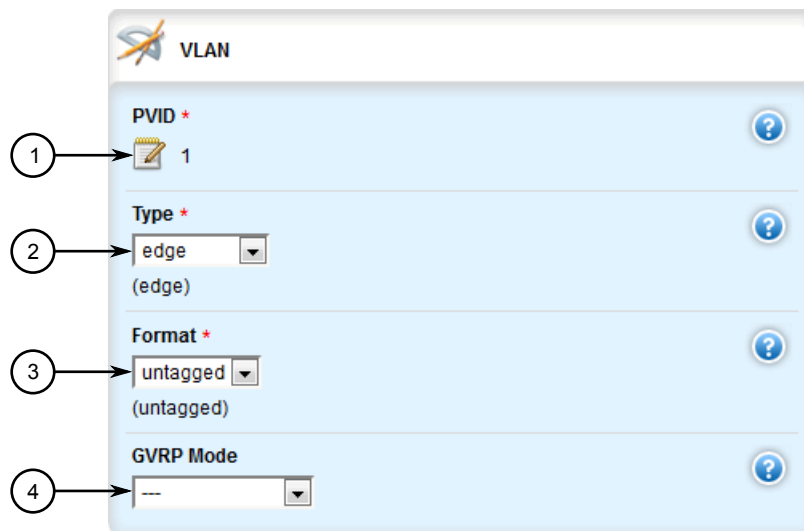
Figure 101: Multicast Filtering Form

1. GMRP List



**Figure 102: CoS Form**

1. Default Priority Box    2. Inspect TOS Check Box



**Figure 103: VLAN Form**

1. PVID Box    2. Type List    3. Format List    4. GVRP Mode List

3. On the **Switched Ethernet Ports** form, configure 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.*

Parameter	Description
Enabled	<p><b>Synopsis:</b> true or false <b>Default:</b> true</p> <p>Provides the option to enable or disable this interface. When unchecked(i.e disabled), the interface will prevent all frames from being sent and received on that interface.</p>
AutoN	<p>Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results.</p>
Speed	<p>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.</p>
Duplex	<p>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.</p>
Link Alarms	<p><b>Synopsis:</b> true or false <b>Default:</b> true</p> <p>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.</p>
Switchport	<p><b>Synopsis:</b> true or false</p> <p>Sets the physical port into either switched mode or a dedicated routing mode.</p>
Flow Control	<p><b>Synopsis:</b> typeless</p> <p>Flow control is useful for preventing frame loss during times of severe network traffic</p>
on-demand	<p><b>Synopsis:</b> typeless</p> <p>Bring up this interface on-demand only</p>
LFI	<p><b>Synopsis:</b> typeless</p> <p>Link Fault Indication (LFI) is specifically for FX interfaces.</p>
IP Address Source	<p><b>Synopsis:</b> { static, dynamic }</p> <p>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.</p>

Parameter	Description
Proxy ARP	<b>Synopsis:</b> typeless Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
MTU	<b>Synopsis:</b> An integer between 68 and 1500 <b>Default:</b> 1500 Maximum transmission unit (largest packet size allowed for this interface).
Alias	<b>Synopsis:</b> A string 1 to 64 characters long The SNMP alias name of the interface

4. On the **Rate Limiting** form, configure the following parameter(s) as required:

Parameter	Description
Ingress Limit	<b>Synopsis:</b> { disabled } or an integer between 62 and 256000 <b>Default:</b> 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	<b>Synopsis:</b> { broadcast, multicast, mcast-flood-ucast, all } <b>Default:</b> broadcast This parameter specifies the types of frames to rate-limit on this port. It applies only to received frames: <itemizedlist><listitem>BROADCAST : only broadcast frames will be limited.</listitem> <listitem>MULTICAST : all multicast frames (including broadcast) will be limited.</listitem> <listitem>MCAST-FLOOD-UCAST : all multicast frames (including broadcast) will be limited. Unicast will not be limited.</listitem> <listitem>ALL : all frames (both multicast and unicast) will be limited.</listitem></itemizedlist>
Egress Limit	<b>Synopsis:</b> { disabled } or an integer between 62 and 256000 <b>Default:</b> 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.

5. On the **LLDP** form, configure the following parameter(s) as required:

Parameter	Description
Admin Status	<b>Synopsis:</b> { tx-only, rx-only, rx-tx, no-ldp } <b>Default:</b> rx-tx <itemizedlist><listitem>no-ldp : The local LLDP agent can neither transmit nor receive LLDP frames.</listitem> <listitem>rxTx : The local LLDP agent can both transmit and receive LLDP frames through the port.</listitem> <listitem>txOnly : The local LLDP agent can only transmit LLDP frames.</listitem> <listitem>rxOnly : The local LLDP agent can only receive LLDP frames.</listitem></itemizedlist>
Notify	<b>Synopsis:</b> typeless

Parameter	Description
	Disabling notifications will prevent sending notifications and generating alarms for a particular interface from the LLDP agent.

6. On the **Multicast Filtering** form, configure the following parameter(s) as required:

Parameter	Description
GMRP	<b>Synopsis:</b> { advertise_only, learn_advertise } GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: <itemizedlist><listitem>DISABLED : the port is not capable of any GMRP processing.</listitem> <listitem>ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.</listitem> <listitem>ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.</listitem></itemizedlist>

7. On the **CoS** form, configure the following parameter(s) as required:

Parameter	Description
Default Priority	<b>Synopsis:</b> An integer between 0 and 7 <b>Default:</b> 0 The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. the priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
Inspect ToS	<b>Synopsis:</b> typeless 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.

8. On the **VLAN** form, configure the following parameter(s) as required:

Parameter	Description
PVID	<b>Synopsis:</b> An integer between 1 and 4094 The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.
Type	<b>Synopsis:</b> { edge, trunk, pvlanedge } <b>Default:</b> edge How the port determines its membership in VLANs. There are a few types of ports: <itemizedlist><listitem>EDGE : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter).</listitem> <listitem>PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN.</listitem> <listitem>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.</listitem></itemizedlist>
Format	<b>Synopsis:</b> { untagged, tagged }

Parameter	Description
	<b>Default:</b> untagged Whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.
GVRP Mode	<b>Synopsis:</b> { advertise_only, learn_advertise } GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: <itemizedlist><listitem>DISABLED : the port is not capable of any GVRP processing.</listitem> <listitem>ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.</listitem> <listitem>ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.</listitem></itemizedlist>

**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**.

- If the port is in switchport mode, configure the VLAN for the port. For more information, refer to [Section 5.36.3.2, “Configuring VLANs for Switch Ethernet Ports”](#).
- Configure the port security settings. For more information, refer to [Section 3.18.3, “Configuring Port Security”](#).
- Configure the spanning tree settings. For more information, refer to [Section 5.35.5, “Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 3.18.3

## Configuring Port Security

Port security (or Port Access Control) provides the ability to authenticate access through individual ports, either through IEEE 802.1x authentication, static MAC address-based authorization, or both.

Using IEEE 802.1x authentication, RUGGEDCOM ROX II authenticates a source device against a remote RADIUS authentication server. Access is granted if the source device provides the proper credentials.

Using static MAC address-based authorization, RUGGEDCOM ROX II authenticates the source device based on its MAC address. Access is granted if the MAC address appears on the Static MAC Address table.

**NOTE**

RUGGEDCOM ROX II only supports the authentication of one host per port that has the port security mode set to 802.1x or 802.1x/MAC-Auth.

**NOTE**

RUGGEDCOM ROX II supports both PEAP and EAP-MD5. PEAP is more secure and is recommended over EAP-MD5.



### 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.*

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » switch » {slot/port} » port-security**, where {slot/port} is the slot name and port number of the switched Ethernet port. The **Port Security** and **802.1x Parameters** forms appear.

**Figure 104: Port Security Form**

1. Security Mode List   2. Auto Learn Box   3. Shutdown Time Box   4. Shutdown Enable Check Box

802.1x Parameters

1

Transmission Period \*

30

(30)

2

Quiet-period \*

60

(60)

3

Reauthorization

Enabled

4

Reauth-period \*

3600

(3600)

5

Reauthorization Max Attempts \*

2

(2)

6

Supplicant Timeout \*

30

(30)

7

Server Timeout \*

30

(30)

8

Max Requests \*

2

(2)

**Figure 105: 802.1x Parameters**

1. Transmission Period Box   2. Quiet Period Box   3. Reauthorization Check Box   4. Reauthorize Period Box   5. Reauthorization Max Attempts Box   6. Supplicant Timeout Box   7. Server Timeout Box   8. Max Requests Box

3. On the **Port Security** form, configure the following parameter(s) as required:

Parameter	Description
Security Mode	<p><b>Synopsis:</b> { dot1x_mac_auth, dot1x, per_macaddress, off }</p> <p><b>Default:</b> off</p> <p>Enables or disables the security feature for the port. The following port access control types are available:</p> <ul style="list-style-type: none"><li>Static MAC address based. With this method, authorized MAC address(es) should be configured in the static MAC address table. If some MAC addresses are not known in advance (or which port they are going to reside behind is unknown), there is still an option to configure the switch to auto-learn a certain number of MAC addresses.</li></ul>

Parameter	Description
	<p>&lt;listitem&gt;IEEE 802.1X standard authentication.&lt;/listitem&gt;          &lt;listitem&gt;IEEE 802.1X with MAC Authentication, also known as MAC-Authentication Bypass. With this method, the device can authenticate clients based on the client's MAC address, if IEEE 802.1X authentication times out.&lt;/listitem&gt;&lt;/itemizedlist&gt;</p>
Auto Learn	<p><b>Synopsis:</b> An integer between 0 and 16  <b>Default:</b> 0</p> <p>The maximum number of MAC addresses that can be dynamically learned on the port. If there are static addresses configured on the port, the actual number of addresses allowed to be learned is this number minus the number of the static MAC addresses.</p>
Shutdown Time	<p><b>Synopsis:</b> An integer between 1 and 86400          How long to shut down an interface if a security violation occurs.</p>
Shutdown Enable	<p><b>Synopsis:</b> typeless          Enables/disables administrative shutdown if a security violation occurs.</p>

4. On the **802.1x Parameters** form, configure the following parameter(s) as required:

Parameter	Description
Transmission Period	<p><b>Synopsis:</b> An integer between 1 and 65535  <b>Default:</b> 30</p> <p>IEEE 802.1X PAE (Port Access Entity) parameters</p>
quiet-period	<p><b>Synopsis:</b> An integer between 0 and 65535  <b>Default:</b> 60</p> <p>The period of time not to attempt to acquire a supplicant after the authorization session failed.</p>
Reauthorization	<p><b>Synopsis:</b> typeless          Enables or disables periodic reauthentication</p>
Reauthorization Period	<p><b>Synopsis:</b> An integer between 60 and 86400  <b>Default:</b> 3600</p> <p>The time between successive reauthentications of the supplicant.</p>
Reauthorization Max Attempts	<p><b>Synopsis:</b> An integer between 1 and 10  <b>Default:</b> 2</p> <p>The number of reauthentication attempts that are permitted before the port becomes unauthorized.</p>
Supplicant Timeout	<p><b>Synopsis:</b> An integer between 1 and 300  <b>Default:</b> 30</p> <p>The time to wait for the supplicant's response to the authentication server's EAP packet.</p>
Server Timeout	<p><b>Synopsis:</b> An integer between 1 and 300  <b>Default:</b> 30</p> <p>The time to wait for the authentication server's response to the supplicant's EAP packet.</p>
Max Requests	<p><b>Synopsis:</b> An integer between 1 and 10  <b>Default:</b> 2</p>

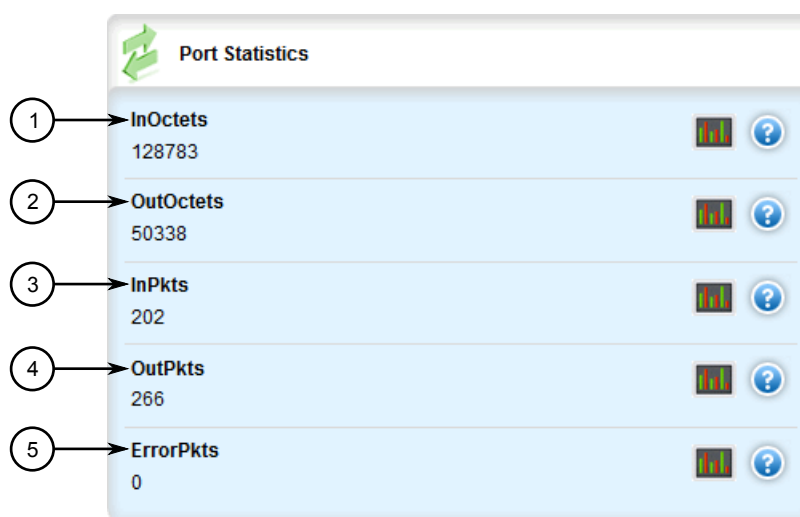
Parameter	Description
	The maximum number of times to retransmit the authentication server's EAP Request packet to the supplicant before the authentication session times out.

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 4.8.3, “Configuring RADIUS Authentication for Switched Ethernet Ports”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 3.18.4

## Viewing Switched Ethernet Port Statistics

To view statistics collected for a specific switched Ethernet port, navigate to **interfaces » switch » {slot/port}**, where **{slot/port}** is the slot name and port number of the switched Ethernet port. The **Port Statistics** form appears.



**Figure 106: Port Statistics Form**

1. InOctets   2. OutOctets   3. InPkts   4. OutPkts   5. ErrorPkts

This form provides the following information:

Parameter	Description
InOctets	The number of octets in received good packets. (Unicast+Multicast +Broadcast) and dropped packets.
OutOctets	The number of octets in transmitted good packets.
InPkts	The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.

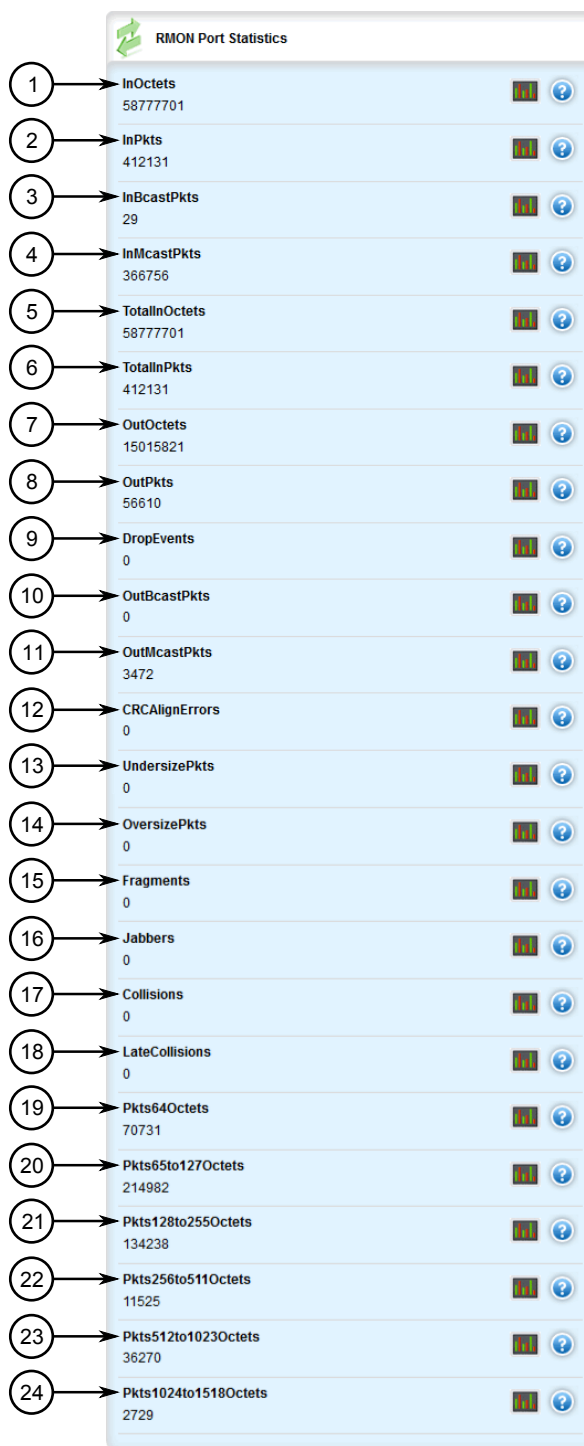


Parameter	Description
OutPkts	The number of transmitted good packets.
ErrorPkts	The number of any type of erroneous packets.

Section 3.18.5

## Viewing RMON Port Statistics

To view Remote Network Monitoring (RMON) statistics collected for a specific switched Ethernet port, navigate to ***interfaces » switch » {slot/port}***, where *{slot/port}* is the slot name and port number of the switched Ethernet port. The **RMON Port Statistics** form appears.



**Figure 107: RMON Port Statistics Form**

1. InOctets 2. InPkts 3. InBcastPkts 4. InMcastPkts 5. TotalInOctets 6. TotalInPkts 7. OutOctets 8. OutPkts 9. DropEvents  
10. OutBcastPkts 11. OutMcastPkts 12. CRCAAlignErrors 13. UndersizePkts 14. OversizePkts 15. Fragments 16. Jabbers  
17. Collisions 18. LateCollisions 19. Pkts64Octets 20. Pkts65to127Octets 21. Pkts128to255Octets 22. Pkts256to511Octets  
23. Pkts512to1023Octets 24. Pkts1024to1518Octets

This form provides the following information:

Parameter	Description
InOctets	The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
InPkts	The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
InBcastPkts	The number of good broadcast packets received.
InMcastPkts	The number of good multicast packets received.
TotalInOctets	The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
TotalInPkts	The number of received packets. This includes rejected, dropped and local packets, as well as packets which are not forwarded to the switching core for transmission. It should reflect all packets received on the line.
OutOctets	The number of octets in transmitted good packets.
OutPkts	The number of transmitted good packets.
DropEvents	The number of received packets that are dropped due to lack of receive buffers.
OutBcastPkts	The number of transmitted broadcast packets.
OutMcastPkts	The number of transmitted multicast packets. This does not include broadcast packets.
CRCAlignErrors	The number of packets received which meet all the following conditions: <ol style="list-style-type: none"> <li>1. The packet data length is between 64 and 1536 octets inclusive.</li> <li>2. The packet has invalid CRC.</li> <li>3. A Collision Event has not been detected.</li> <li>4. A Late Collision Event has not been detected.</li> </ol>
UndersizePkts	The number of received packets which meet all the following conditions: <ol style="list-style-type: none"> <li>1. The packet data length is less than 64 octets.</li> <li>2. A Collision Event has not been detected.</li> <li>3. A Late Collision Event has not been detected.</li> <li>4. The packet has valid CRC.</li> </ol>
OversizePkts	The number of packets received with data length greater than 1536 octets and valid CRC.
Fragments	The number of packets received which meet all the following conditions: <ol style="list-style-type: none"> <li>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.</li> </ol>

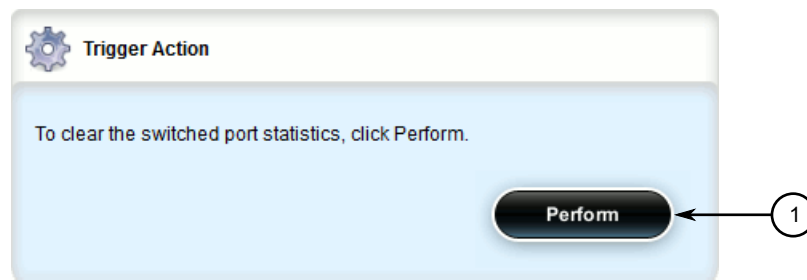
Parameter	Description
	<ul style="list-style-type: none"> <li>2. A Collision Event has not been detected.</li> <li>3. A Late Collision Event has not been detected.</li> <li>4. The packet has invalid CRC.</li> </ul>
Jabbers	<p>The number of packets which meet all the following conditions:</p> <ul style="list-style-type: none"> <li>1. The packet data length is greater than 1536 octets.</li> <li>2. The packet has invalid CRC.</li> </ul>
Collisions	The number of received packets for which a Collision Event has been detected.
LateCollisions	The number of received packets for which a Late Collision Event has been detected.
Pkts64Octets	<p>The number of received and transmitted packets with a size of 64 octets. This</p> <p>includes received and transmitted packets as well as dropped and local</p> <p>received packets. This does not include rejected received packets.</p>
Pkts65to127Octets	<p>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</p>
Pkts128to255Octets	<p>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</p>
Pkts256to511Octets	<p>The number of received and transmitted packets with size of 256 to 511 octets.</p> <p>This includes received and transmitted packets as well as dropped and local</p> <p>received packets. This does not include rejected received packets.</p>
Pkts512to1023Octets	<p>The number of received and transmitted packets with size of 512 to 1023 octets.</p> <p>This includes received and transmitted packets as well as dropped and local</p> <p>received packets. This does not include rejected received packets</p>
Pkts1024to1518Octets	<p>The number of received and transmitted packets with a size of 1024 to 1536</p> <p>octets. This includes received and transmitted packets as well as dropped and</p> <p>local received packets. This does not include rejected received packets.</p>

### Section 3.18.6

## Clearing Switched Ethernet Port Statistics

To clear the statistics collected for a specific switched Ethernet port, do the following:

1. Navigate to **interfaces » switch » {slot/port}**, where {slot/port} is the slot name and port number of the switched Ethernet port.
2. Click **clear-serial-port-statistics** in the menu. The **Trigger Action** form appears.



**Figure 108: Trigger Action Form**

1. Perform Button

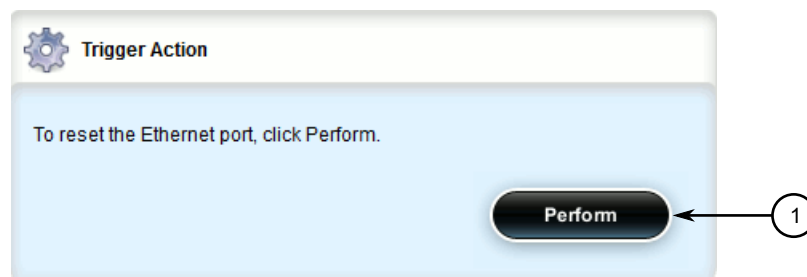
3. Click **Perform**.

#### Section 3.18.7

## Resetting a Switched Ethernet Port

To reset a switched Ethernet port, do the following:

1. Navigate to **interfaces » switch » {slot/port}**, where *{slot/port}* is the slot name and port number of the switched Ethernet port.
2. Click **reset-port** in the menu. The **Trigger Action** form appears.



**Figure 109: Trigger Action Form**

1. Perform Button

3. Click **Perform**.

#### Section 3.18.8

## Testing Switched Ethernet Port Cables

Diagnostics can be performed on switched Ethernet port cables to assess their overall quality.

The following sections describe how to test and diagnose switched Ethernet port cables:

- [Section 3.18.8.1, "Running a Cable Diagnostic Test"](#)

- [Section 3.18.8.2, “Viewing Cable Diagnostic Statistics”](#)
- [Section 3.18.8.3, “Clearing Cable Diagnostic Statistics”](#)

#### Section 3.18.8.1

### Running a Cable Diagnostic Test

To run a cable diagnostic test on a specific port, do the following:



#### 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.*

1. Navigate to **interfaces » switch » {slot/port} » diagnostics**, where {slot/port} is the slot name and port number of the switched Ethernet port.
2. Click **start-cable-test** in the menu. The **Trigger Action** and **Start Cable Test** forms appear.

**Trigger Action**

Select the Slot/Port to be tested, the number of runs to perform, and the calibration value

**Runs:** The total number of times to perform the cable diagnostics on the selected port. If set to 0, cable diagnostics are performed forever on the selected port.

**Calibration:** Adjusts or calibrates the estimated distance to fault. To calibrate the cable diagnostics estimated distance to fault:

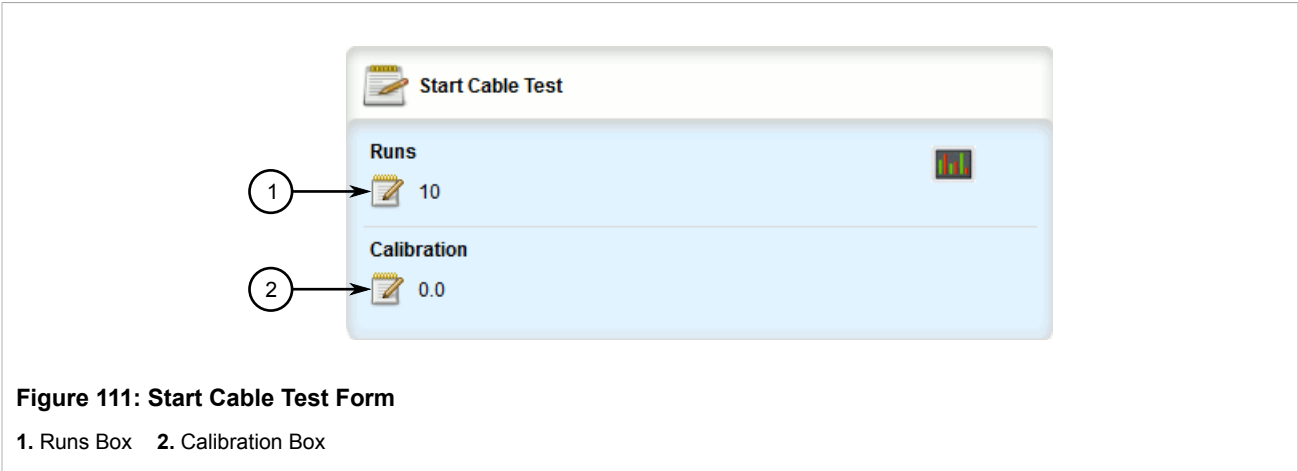
1. Pick a particular port on which calibration is needed.
2. Connect an Ethernet cable with a known length (for example, 50m) to the port.
3. DO NOT connect the other end of the cable to any link partner.
4. Run cable diagnostics a few times on the port. An OPEN fault should be detected.
5. In the log, find the average distance to the OPEN fault and compare it to the known cable length. Use the difference as the calibration value.
6. Enter the calibration value and run cable diagnostics a few more times.
7. The distance to the OPEN fault should now similar to the known cable length. The distance to fault for the selected port is now calibrated.

To start the test, click Perform.

**Perform** 1

**Figure 110: Trigger Action Form**

1. Perform Button



3. On the **Start Cable Test** form, configure the following parameter(s) as required:

Parameter	Description
runs	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 10
calibration	<b>Synopsis:</b> A string <b>Default:</b> 0.0

4. Read and follow the instructions on the **Start Cable Diagnostics Test**.
5. Click **Perform** to start the test. For information about how to view the test results, refer to [Section 3.18.8.2, “Viewing Cable Diagnostic Statistics”](#).

Section 3.18.8.2

**Viewing Cable Diagnostic Statistics**

Navigate to *interfaces » switch » {slot/port} » diagnostics*, where *{slot/port}* is the slot name and port number of the switched Ethernet port. The **Cable Diagnostic Results** form appears.

The screenshot shows a web interface titled "Cable Diagnostic Results" with a green refresh icon. The form contains the following fields:

- 1. **Running**: A checkbox labeled "Enabled" with a blue question mark icon.
- 2. **Good Termination**: A text field showing "20" with a bar chart icon and a blue question mark icon.
- 3. **Open**: A text field showing "0" with a bar chart icon and a blue question mark icon.
- 4. **Short**: A text field showing "20" with a bar chart icon and a blue question mark icon.
- 5. **Impedance Mismatch**: A text field showing "0" with a bar chart icon and a blue question mark icon.
- 6. **PassFailTotal**: A text field showing "10/ 0/ 10" with a blue question mark icon.
- 7. **Run Count**: A text field showing "0" with a bar chart icon and a blue question mark icon.
- 8. **Pass Count**: A text field showing "0" with a bar chart icon and a blue question mark icon.
- 9. **Failure Count**: A text field showing "0" with a bar chart icon and a blue question mark icon.

**Figure 112: Cable Diagnostic Results Form**

1. Running Check Box   2. Good Termination   3. Open   4. Short   5. Impedance Mismatch   6. PassFailTotal   7. Run Count   8. Pass Count   9. Failure Count

This form provides the following information:

Parameter	Description
Running	<b>Synopsis:</b> true or false Whether or not a cable test is currently running on this port
Good Termination	The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
Open	The number of times OPEN is detected on the cable pairs of the selected port.
Short	The number of times SHORT is detected on the cable pairs of the selected port.
Impedance Mismatch	The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
PassFailTotal	<b>Synopsis:</b> A string 1 to 19 characters long This field summarizes the results of the cable diagnostics performed so far. <itemizedlist><listitem>Pass : the number of times cable diagnostics were successfully completed on the selected port.</listitem> <listitem>Fail : the number of times cable diagnostics failed



Parameter	Description
	to complete on the selected port.</listitem> <listitem>Total : the total number of times cable diagnostics have been attempted on the selected port.</listitem></itemizedlist>
Run Count	Run Count : The total number of iterations
Pass Count	Pass Count
Failure Count	Failure Count

## Section 3.18.8.3

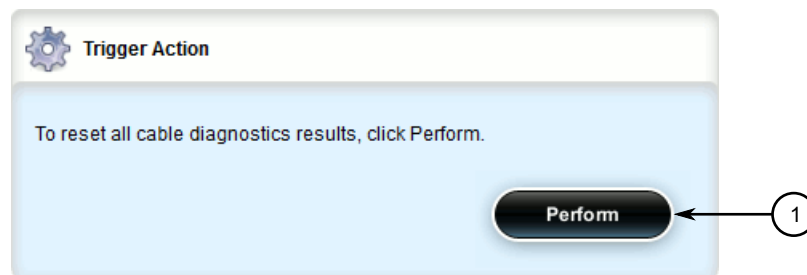
## Clearing Cable Diagnostic Statistics

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, do the following:

1. Navigate to **interfaces » switch » {slot/port}**, where {slot/port} is the slot name and port number of the switched Ethernet port.
2. Click **clear-cable-stats-all** in the menu. The **Trigger Action** form appears.



**Figure 113: Trigger Action Form**

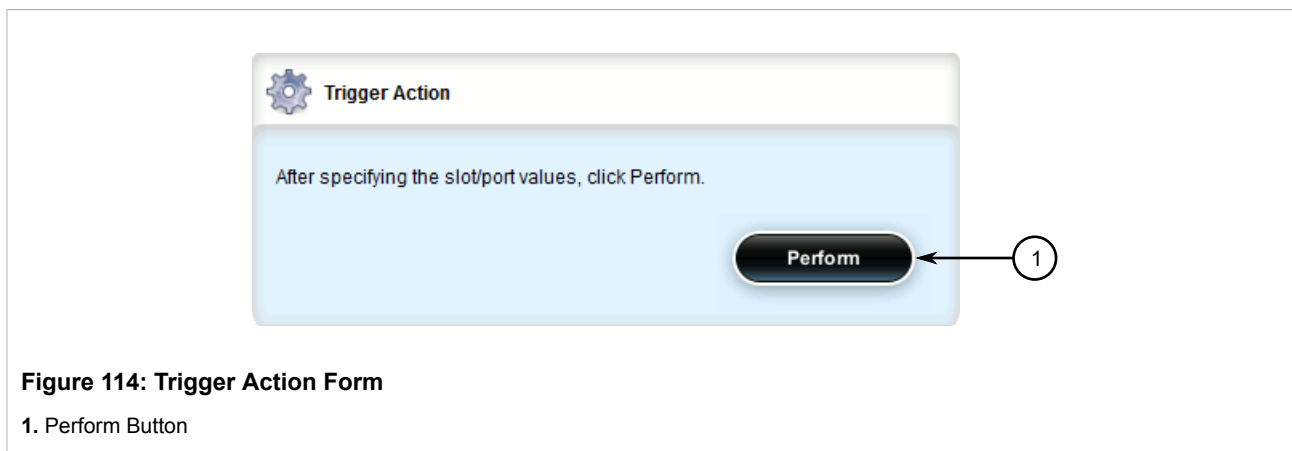
1. Perform Button

3. Click **Perform** to clear the statistics.

### » Clearing Cable Diagnostic Statistics for a Specific Switchport

To clear only the statistics for a specific switchport, do the following:

1. Navigate to **interfaces » switch » {slot/port} » diagnostics**, where {slot/port} is the slot name and port number of the switched Ethernet port.
2. Click **clear-cable-stats-port** in the menu. The **Trigger Action** form appears.



3. Click **Perform** to clear the statistics.

## Section 3.19

## Managing Rutable Ethernet Ports

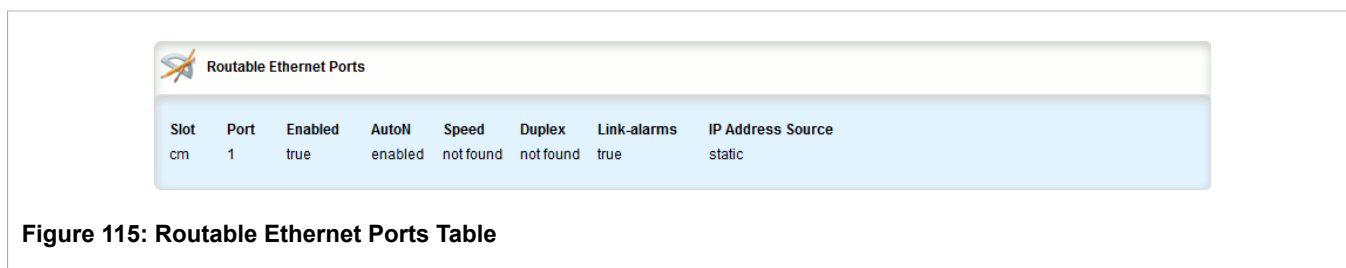
The following sections describe how to configure and manage rutable Ethernet ports:

- [Section 3.19.1, “Viewing a List of Rutable Ethernet Ports”](#)
- [Section 3.19.2, “Configuring a Rutable Ethernet Port”](#)

## Section 3.19.1

### Viewing a List of Rutable Ethernet Ports

To view a list of rutable Ethernet ports, navigate to **interface » eth**. The **Rutable Ethernet Ports** table appears.



## Section 3.19.2

### Configuring a Rutable Ethernet Port

To configure a rutable Ethernet port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **interface » eth » {interface}**, where {interface} is the routable Ethernet port. The **Routable Ethernet Ports** and **LLDP** forms appear.

**Figure 116: Routable Ethernet Ports Form**

1. Enabled Check Box   2. AutoN Check Box   3. Speed List   4. Duplex List   5. Link Alarms Check Box   6. IP Address Source List   7. ProxyARP Check Box   8. On-Demand Check Box   9. Alias Box

**Figure 117: LLDP Form**

1. Admin Status List 2. Notify Check Box

3. On the **Routable Ethernet Ports** form, configure the following parameters as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables/Disables the network communications on this port.
AutoN	<b>Synopsis:</b> typeless Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results.
Speed	<b>Synopsis:</b> { 10, 100, 1000 } Speed (in Megabit-per-second or Gigabit-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes.
Duplex	<b>Synopsis:</b> { half, full } If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes.
link-alarms	<b>Synopsis:</b> true or false <b>Default:</b> true Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
IP Address Source	<b>Synopsis:</b> { static, dynamic } <b>Default:</b> static Determines whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces.
Proxy ARP	<b>Synopsis:</b> typeless

Parameter	Description
	Enables/Disables whether the port will respond to ARP requests for hosts other than itself.
on-demand	<b>Synopsis:</b> typeless This interface is up or down on demand of link fail over.
alias	<b>Synopsis:</b> A string 1 to 64 characters long The SNMP alias name of the interface

4. On the **LLDP** form, configure the following parameters as required:

Parameter	Description
Admin Status	<b>Synopsis:</b> { tx-only, rx-only, rx-tx, no-ldp } <b>Default:</b> rx-tx <itemizedlist><listitem>no-ldp : The local LLDP agent can neither transmit nor receive LLDP frames.</listitem> <listitem>rxTx : The local LLDP agent can both transmit and receive LLDP frames through the port.</listitem> <listitem>txOnly : The local LLDP agent can only transmit LLDP frames.</listitem> <listitem>rxOnly : The local LLDP agent can only receive LLDP frames.</listitem></itemizedlist>
Notify	<b>Synopsis:</b> typeless Disabling notifications will prevent sending notifications and generating alarms for a particular interface from the LLDP agent.

5. Add a VLAN ID (VID) for the port. For more information, refer to [Section 5.36.7.2, “Adding a VLAN to a Routable Ethernet Port”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 3.20

# Managing Serial Ports

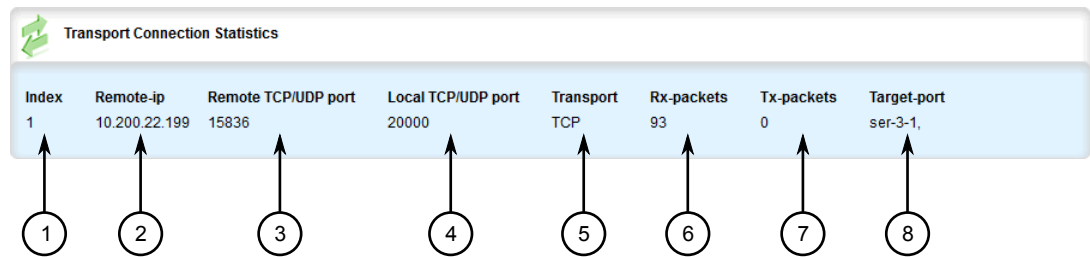
The following sections describe how to configure and manage serial ports:

- [Section 3.20.1, “Viewing Transport Connection Statistics”](#)
- [Section 3.20.2, “Viewing DNP Device Table Statistics”](#)
- [Section 3.20.3, “Restarting the Serial Server”](#)

## Section 3.20.1

# Viewing Transport Connection Statistics

To view the statistics collected for all transport connections, navigate to **interfaces » serial » transport-connections**. The **Transport Connection Statistics** table appears.



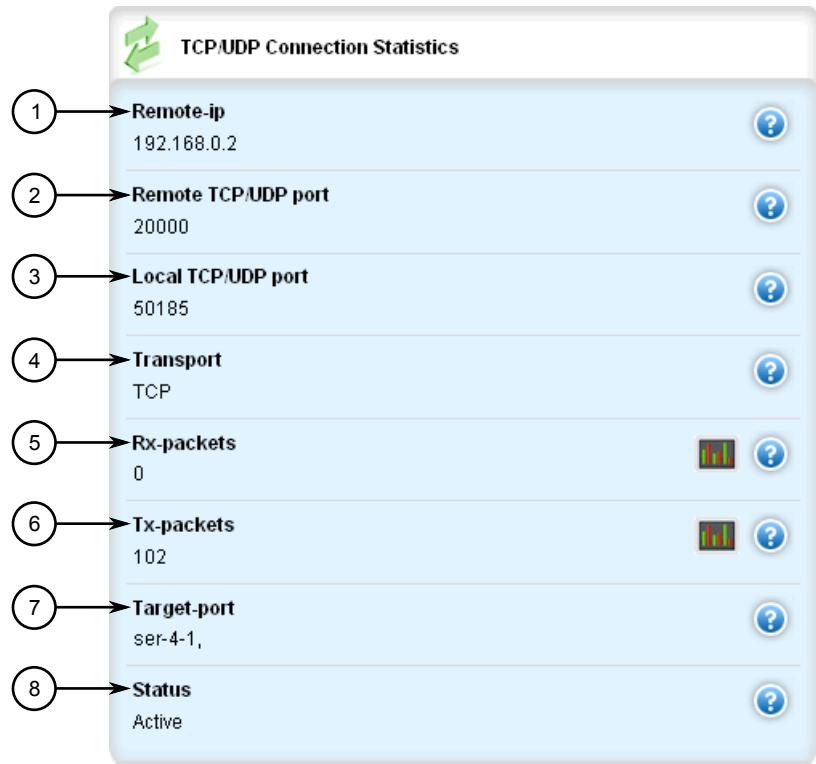
The image shows a table titled "Transport Connection Statistics" with a green icon. Below the table, eight numbered circles (1-8) have arrows pointing to specific columns in the table.

Index	Remote-ip	Remote TCP/UDP port	Local TCP/UDP port	Transport	Rx-packets	Tx-packets	Target-port
1	10.200.22.199	15836	20000	TCP	93	0	ser-3-1,

Figure 118: Transport Connection Statistics Table

1. Index   2. Remote IP   3. Remote TCP/UDP Port   4. Local TCP/UDP Port   5. Transport   6. Rx-packets   7. Tx-packets   8. Target Port

To view the statistics collected for a specific transport connection, navigate to **interfaces » serial » transport-connections » {index}**, where {index} is the index number assigned to the transport connection. The **TCP/UDP Connection Statistics** form appears.



The image shows a form titled "TCP/UDP Connection Statistics" with a green icon. It contains eight fields, each with a numbered circle (1-8) pointing to it. Each field has a question mark icon to its right. Fields 5 and 6 have a small bar chart icon next to them.

1	Remote-ip	192.168.0.2	?
2	Remote TCP/UDP port	20000	?
3	Local TCP/UDP port	50185	?
4	Transport	TCP	?
5	Rx-packets	0	?
6	Tx-packets	102	?
7	Target-port	ser-4-1,	?
8	Status	Active	?

Figure 119: TCP/UDP Connection Statistics Form

1. Remote IP   2. Remote TCP/UDP Port   3. Local TCP/UDP Port   4. Transport   5. Rx-packets   6. Tx-packets   7. Target Port   8. Status

These tables and forms provide the following information:

Parameter	Description
remote-ip	<b>Synopsis:</b> A string 1 to 32 characters long

Parameter	Description
	The IP address of the remote serial server.
Remote TCP/UDP port	The port of the remote serial server.
Local TCP/UDP port	The local port for the incoming connection.
transport	<b>Synopsis:</b> A string 1 to 8 characters long The transport protocol (UDP or TCP) for this serial port.
rx-packets	The number of packets received from TCP/UDP.
tx-packets	The number of packets transmitted to TCP/UDP.
target-port	<b>Synopsis:</b> A string 1 to 1024 characters long The target serial port.
status	<b>Synopsis:</b> A string 1 to 31 characters long The connection status of the serial port.

## Section 3.20.2

## Viewing DNP Device Table Statistics

To view the statistics collected for DNP device tables, navigate to **interfaces » serial » dnp-device-table**. The **DNP Device Table** table appears.

The screenshot shows a web interface for the path `/interfaces/serial/dnp-device-table`. It displays a table with the following data:

Device-address	Remote-ip	Serial-port
10	-	ser-3-1
20	10.200.22.199	-

Below the table, three numbered circles (1, 2, 3) have arrows pointing to the columns: 1 points to Device-address, 2 points to Remote-ip, and 3 points to Serial-port.

**Figure 120: DNP Device Table**

1. Device Address    2. Remote IP    3. Serial Port

This table provides the following information:

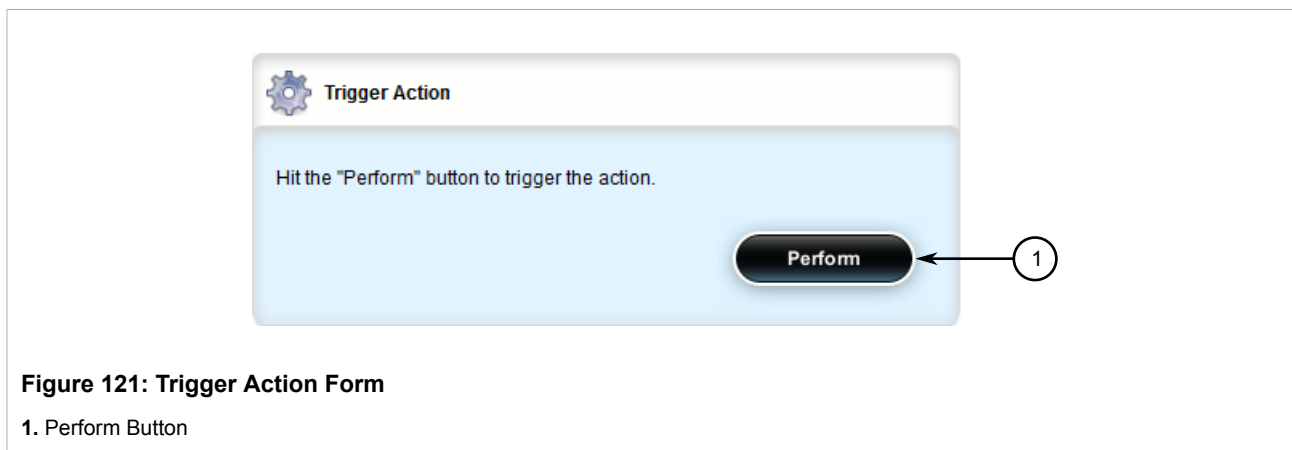
Parameter	Description
device-address	<b>Synopsis:</b> A string 1 to 32 characters long The DNP device address.
remote-ip	<b>Synopsis:</b> A string 1 to 32 characters long The IP address of the remote host that provides a connection to the this DNP device address.
serial-port	<b>Synopsis:</b> A string 1 to 128 characters long The target serial port.

Section 3.20.3

## Restarting the Serial Server

To restart the serial server, do the following:

1. Navigate to **interfaces** » **serial** and click **restart-serserver** in the menu. The **Trigger Action** form appears.



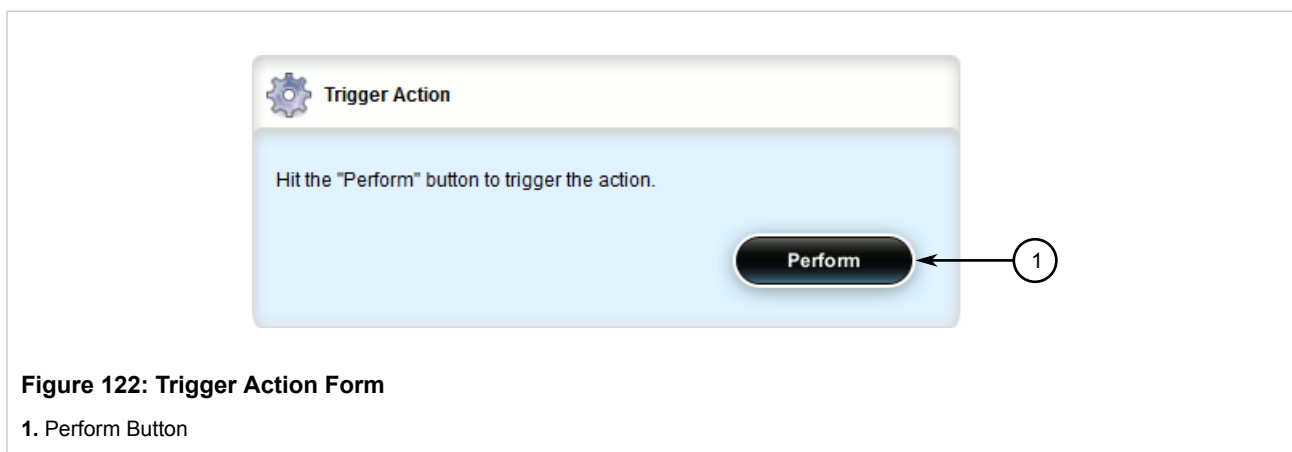
2. Click **Perform**.

Section 3.20.4

## Resetting a Serial Port

To reset a serial port, do the following:

1. Click **reset** in the menu. The **Trigger Action** form appears.



2. Click **Perform**.



Section 3.21

# Managing Serial Port Protocols

The following sections describe how to configure and manage serial port protocols:

- [Section 3.21.1, “Serial Port Protocol Concepts”](#)
- [Section 3.21.2, “Viewing a List of Serial Port Protocols”](#)
- [Section 3.21.3, “Adding a Serial Port Protocol”](#)
- [Section 3.21.4, “Configuring the DNP Protocol”](#)
- [Section 3.21.5, “Configuring the Modbus TCP Protocol”](#)
- [Section 3.21.6, “Configuring the Raw Socket Protocol”](#)
- [Section 3.21.7, “Deleting a Serial Port Protocol”](#)
- [Section 3.21.8, “Managing Device Address Tables”](#)
- [Section 3.21.9, “Managing Remote Hosts”](#)

Section 3.21.1

## Serial Port Protocol Concepts

The following sections describe some of the concepts important to the implementation of serial port protocols in RUGGEDCOM ROX II:

- [Section 3.21.1.1, “Raw Socket Applications”](#)
- [Section 3.21.1.2, “Modbus TCP Applications”](#)
- [Section 3.21.1.3, “DNP Applications”](#)
- [Section 3.21.1.4, “Incoming/Outgoing Serial Connections”](#)

Section 3.21.1.1

### 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 3.21.1.2

## 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 3.21.1.3

## 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 3.21.1.4

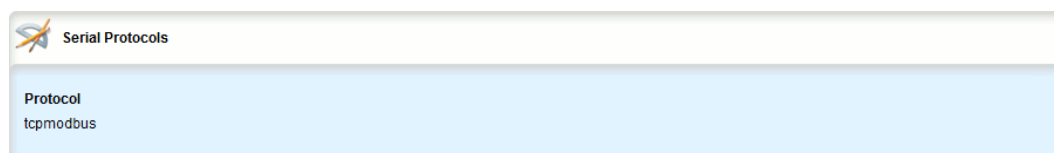
## Incoming/Outgoing Serial Connections

The RUGGEDCOM RX5000/MX5000/MX5000RE supports up to 32 TCP/UDP connections per serial port, up to a total of 128 TCP/UDP connections to the serial server.

### Section 3.21.2

## Viewing a List of Serial Port Protocols

To view a list of serial port protocols configured on the device, navigate to **interface » serial » {interface} » protocols**, where **{interface}** is the slot name and port number of the serial port. If protocols have been configured, the **Serial Protocols** table appears.



Protocol
tcpmodbus

**Figure 123: Serial Protocols Table**

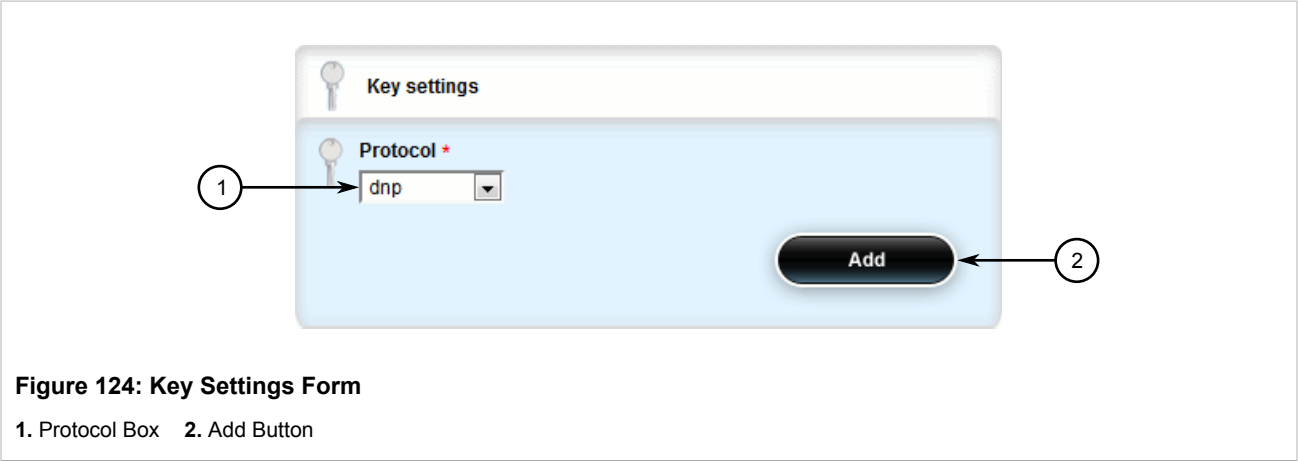
If no serial port protocols have been configured, add protocols as needed. For more information, refer to [Section 3.21.3, “Adding a Serial Port Protocol”](#).

Section 3.21.3

## Adding a Serial Port Protocol

To add a serial port protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *interface* » *serial* » *{interface}* » *protocols*, where *{interface}* is the slot name and port number of the serial port.
3. Click **<Add protocols>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
protocol	<b>Synopsis:</b> { rawsocket, tcpmodbus, dnp, vmserial }

5. Click **Add** to create the protocol.
6. Configure the protocol.
  - For information about configuring a DNP protocol, refer to [Section 3.21.4, “Configuring the DNP Protocol”](#).
  - For information about configuring a Modbus TCP protocol, refer to [Section 3.21.5, “Configuring the Modbus TCP Protocol”](#).
  - For information about configuring a raw socket protocol, refer to [Section 3.21.6, “Configuring the Raw Socket Protocol”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 3.21.4

## Configuring the DNP Protocol

To configure the DNP protocol for a serial port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *interface* » *serial* » *{interface}* » *protocols* » *dnp* » *setdnp*, where *{interface}* is the serial port.

- Click the **+** symbol next to *setdnp*. The **DNP Protocols Configuration** form appears.

**Figure 125: DNP Protocols Configuration Form**

1. Address Learning Box    2. Aging Timer Box    3. Max Connection Box

- Configure the following parameter(s) as required:

Parameter	Description
address-learning	<b>Synopsis:</b> A string 1 to 15 characters long The interface to learn the RTU address from.
aging-timer	<b>Synopsis:</b> An integer between 60 and 10800 <b>Default:</b> 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	<b>Synopsis:</b> An integer between 1 and 32 <b>Default:</b> 1 The maximum number of incoming DNP connections.

- Add a Device Address table. For more information about adding Device Address tables, refer to [Section 3.21.8.2, “Adding a Device Address Table”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 3.21.5

## Configuring the Modbus TCP Protocol

To configure the modbus TCP protocol for a serial port, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **interface » serial » {interface} » protocols » tcpmodbus » settcpmodbus**, where {interface} is the serial port. The **TCP Modbus Configuration** form appears.

The image shows a web interface for 'TCP Modbus Configuration'. It contains several input fields, each with a default value and a range in parentheses. Numbered callouts point to each field:

- 1. Response-timer \*: 100 (100)
- 2. Pack-timer \*: 1000 (1000)
- 3. Turnaround \*: 0 (0)
- 4. Retransmit \*: 0 (0)
- 5. Max-connection \*: 1 (1)
- 6. Local-port \*: 502 (502)
- 7. Rtu-list \*: <string>

Figure 126: TCP Modbus Configuration Form

1. Response Timer Box    2. Packet Timer Box    3. Turnaround Box    4. Retransmit Box    5. Max Connection Box    6. Local Port Box    7. RTU-List Box

- 3. In the menu, click the + symbol next to *settcpmodbus* to add the protocol.
- 4. Configure the following parameter(s) as required:

Parameter	Description
response-timer	<b>Synopsis:</b> An integer between 50 and 1000 <b>Default:</b> 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	<b>Synopsis:</b> An integer between 5 and 1000 <b>Default:</b> 1000  The maximum allowable time to wait for a response to a Modbus request to complete once it has started.

Parameter	Description
turnaround	<p><b>Synopsis:</b> An integer between 0 and 1000  <b>Default:</b> 0</p> <p>The amount of delay (if any) to insert after the transmissions of Modbus broadcast messages out the serial port.</p>
retransmit	<p><b>Synopsis:</b> An integer between 0 and 2  <b>Default:</b> 0</p> <p>The number of times to retransmit the request to the RTU before giving up.</p>
max-connection	<p><b>Synopsis:</b> An integer between 1 and 32  <b>Default:</b> 1</p> <p>The maximum number of incoming connections.</p>
local-port	<p><b>Default:</b> 502</p> <p>The alternate local TCP port number. If this field is configured, a single connection (per serial port) may be made to this alternate port number. Note that Modbus TCP uses a default local port number of 502. There is no limit imposed on the number of connections to the default TCP port.</p>
rtu-list	<p><b>Synopsis:</b> A string</p> <p>The ID of the RTU(s) connected to the serial port. Specify multiple RTUs with a space (e.g. 1 2 3 4) or a comma and space (e.g. 1, 2, 3, 4). A strictly comma-separated list (e.g. 1,2,3,4) is not permitted.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 3.21.6

## Configuring the Raw Socket Protocol

To configure the raw socket protocol for a serial port, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **interface » serial » {interface} » protocols » rawsocket**, where *{interface}* is the serial port.
- Click the **+** symbol in the menu next to **setrawsocket**. The **Raw Socket Configuration** form appears.



The image shows a 'Rawsocket Configuration' form with the following fields and their values:

- Pack-char \***: off (off)
- Pack-timer \***: 1000 (1000)
- Pack-size \***: max (max)
- Turnaround \***: 0 (0)
- Call-direction \***: out (out)
- Max-connection \***: 1 (1)
- Remote-ip**: ---
- Remote-port**: ---
- Local-ip**: ---
- Local-port**: ---
- Transport \***: tcp (tcp)

Numbered callouts (1-11) point to the following fields:

1. Pack-char \*
2. Pack-timer \*
3. Pack-size \*
4. Turnaround \*
5. Call-direction \*
6. Max-connection \*
7. Remote-ip
8. Remote-port
9. Local-ip
10. Local-port
11. Transport \*

**Figure 127: Raw Socket Configuration Form**

1. Packet Character Box   2. Packet Timer Box   3. Packet Size Box   4. Turnaround Box   5. Call Direction Box   6. Max Connection Box   7. Remote IP Box   8. Remote Port Box   9. Local IP Box   10. Local Port Box   11. Transport Box

4. Configure the following parameter(s) as required:

Parameter	Description
pack-char	<b>Synopsis:</b> { off } or an integer between 0 and 255 <b>Default:</b> off The numeric value of the ASCII character which will force forwarding of accumulated data to the network.
pack-timer	<b>Synopsis:</b> An integer between 5 and 1000 <b>Default:</b> 1000 The delay from the last received character until when data is forwarded.
pack-size	<b>Synopsis:</b> { max } or an integer between 16 and 1400 <b>Default:</b> max The maximum number of bytes received from the serial port to be forwarded.
turnaround	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0 The amount of delay (if any) to insert between the transmissions of individual messages out the serial port.
call-direction	<b>Synopsis:</b> { in, out, both } <b>Default:</b> out Whether to accept an incoming connection, place an outgoing connection or do both.
max-connection	<b>Synopsis:</b> An integer between 1 and 32 <b>Default:</b> 1 The maximum number of incoming connections to permit when the call direction is incoming.
remote-ip	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long The IP address used when placing an outgoing connection.
remote-port	<b>Synopsis:</b> An integer between 1024 and 65535 The TCP destination port used in outgoing connections.
local-ip	<b>Synopsis:</b> A string 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	<b>Synopsis:</b> An integer between 1024 and 65535 The local TCP port to use to accept incoming connections.
transport	<b>Synopsis:</b> { tcp, udp } <b>Default:</b> tcp The transport connection protocol (UDP or TCP).

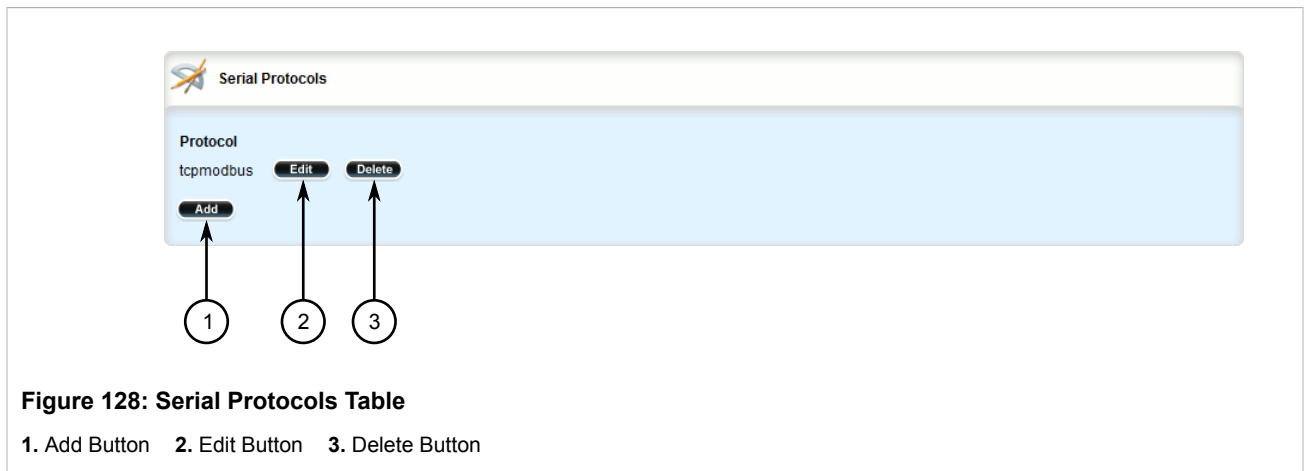
5. If the transport connection protocol is set to UDP, configure one or more remote hosts for the port. For more information about adding a remote host, refer to [Section 3.21.9.2, “Adding a Remote Host”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 3.21.7

## Deleting a Serial Port Protocol

To delete a serial port protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » serial » {interface} » protocols**, where *{interface}* is the slot name and port number of the serial port. The **Serial Protocols** table appears.



3. Click **Delete** next to the chosen protocol.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 3.21.8

## Managing Device Address Tables

The following sections describe how to configure and manage Device Address tables:

- [Section 3.21.8.1, “Viewing a List of Device Address Tables”](#)
- [Section 3.21.8.2, “Adding a Device Address Table”](#)
- [Section 3.21.8.3, “Deleting a Device Address Table”](#)

### Section 3.21.8.1

## Viewing a List of Device Address Tables

To view a list of Device Address tables configured for a serial port using the DNP protocol, navigate to **interface » serial » {interface} » protocols » dnp » setdnp » device-table**, where *{interface}* is the slot name and port number of the serial port. If Device Address tables have been configured, the **DNP Device Address Table Configuration** table appears.



Device Address	Remote-ip	Remote-device
12	172.30.130.2	enabled

**Figure 129: DNP Device Address Table Configuration Table**

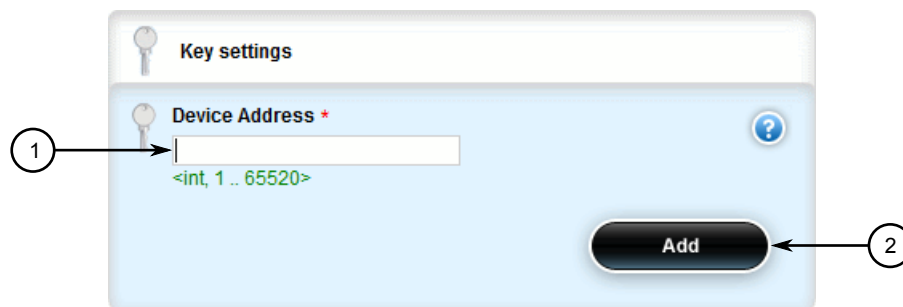
If no Device Address tables have been configured, add tables as needed. For more information, refer to [Section 3.21.8.2, “Adding a Device Address Table”](#).

#### Section 3.21.8.2

### Adding a Device Address Table

To add a Device Address table for a serial port using the DNP protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » serial » {interface} » protocols » dnp » setdnp » device-table**, where {interface} is the slot name and port number of the serial port.
3. Click **<Add device-table>**. The **Key Settings** form appears.



The image shows a 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a section titled 'Device Address \*' with a question mark icon. Inside this section is a text input field with a value of '<int, 1 .. 65520>'. To the left of the input field is a circled number '1' with an arrow pointing to the field. To the right of the input field is a dark blue button labeled 'Add'. To the right of the button is a circled number '2' with an arrow pointing to the button.

**Figure 130: Key Settings Form**

1. Device Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
deviceAddress	<p><b>Synopsis:</b> An integer between 1 and 65520</p> <p>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.</p>

5. Click **Add** to create the Device Address table. The **DNP Device Address Table Configuration** form appears.

**Figure 131: DNP Device Address Table Configuration Form**

1. Remote IP Box    2. Remote Device Check Box

6. Configure the following parameter(s) as required:

Parameter	Description
remote-ip	<p><b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long</p> <p>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.</p>
remote-device	<p><b>Synopsis:</b> typeless</p> <p>Enables forwarding of DNP messages that match the device address to the remote IP.</p>

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 3.21.8.3

## Deleting a Device Address Table

To delete a Device Address table, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » serial » {interface} » protocols » dnp » setdnp » device-table**, where *{interface}* is the slot name and port number of the serial port. The **DNP Device Address Table Configuration** table appears.

Device Address	Remote-ip	Remote-device
12	172.30.130.2	enabled

Buttons: Add, Edit, Delete

Annotations: 1 points to Add, 2 points to Edit, 3 points to Delete

**Figure 132: DNP Device Address Table Configuration Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen Device Address table.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.21.9

## Managing Remote Hosts

Remote hosts are required when the UDP transport connection protocol is selected for the raw socket protocol.

The following sections describe how to configure and manage remote hosts:

- [Section 3.21.9.1, “Viewing a List of Remote Hosts”](#)
- [Section 3.21.9.2, “Adding a Remote Host”](#)
- [Section 3.21.9.3, “Deleting a Remote Host”](#)

#### Section 3.21.9.1

### Viewing a List of Remote Hosts

To view a list of remote hosts configured for a serial port using the raw socket protocol, navigate to **interface » serial » {slot/port} » protocols » rawsocket » setrawsocket » remote-host**, where {slot/port} is the slot name and port number of the serial port. If remote hosts have been configured, the **Remote Host Configuration** table appears.

Remote-ip	Remote-port
172.30.130.2	1

**Figure 133: Remote Host Configuration Table**

If no remote hosts have been configured, add hosts as needed. For more information, refer to [Section 3.21.9.2, “Adding a Remote Host”](#).

## Section 3.21.9.2

## Adding a Remote Host

To add a remote host for a serial port using the raw socket protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » serial » {interface} » protocols » rawsocket » setrawsocket » remote-host**, where {interface} is the slot name and port number of the serial port.
3. Click **<Add remote-host>**. The **Key Settings** form appears.

Key settings

1 Remote-ip \*  
<string, min: 1 chars, max: 15 chars>

2 Remote-port \*  
<int>

3 Add

**Figure 134: Key Settings Form**

1. Remote IP Box   2. Remote Port Box   3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
remote-ip	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the remote host.
remote-port	The transport port of the remote host.

5. Click **Add** to create the remote host.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

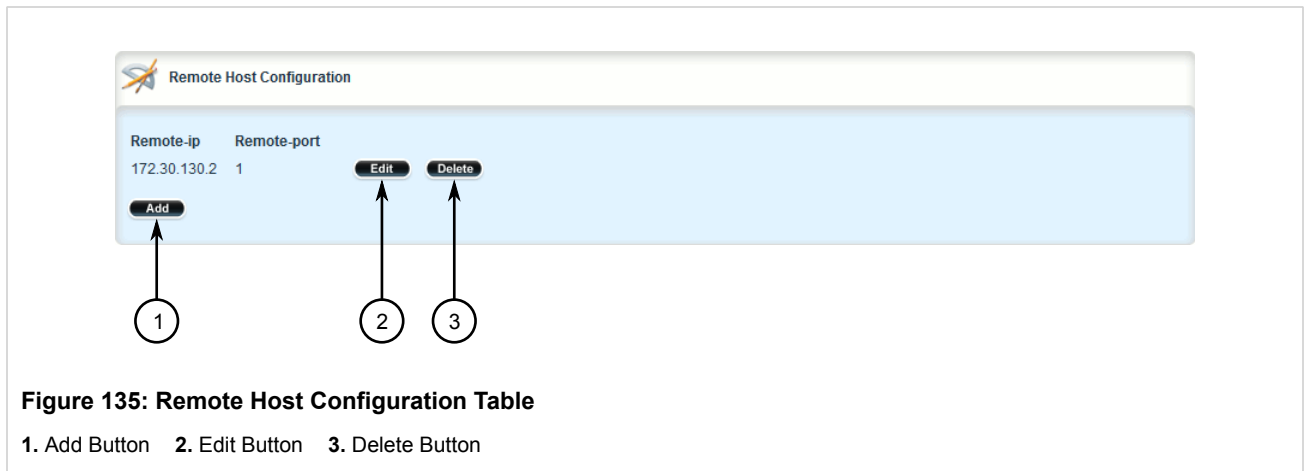
## Section 3.21.9.3

## Deleting a Remote Host

To delete a remote host, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **interface » serial » {interface} » protocols » rawsocket » setrawsocket » remote-host**, where *{interface}* is the slot name and port number of the serial port. The **Remote Host Configuration** table appears.



3. Click **Delete** next to the chosen host.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 3.22

# Managing Ethernet Trunk Interfaces

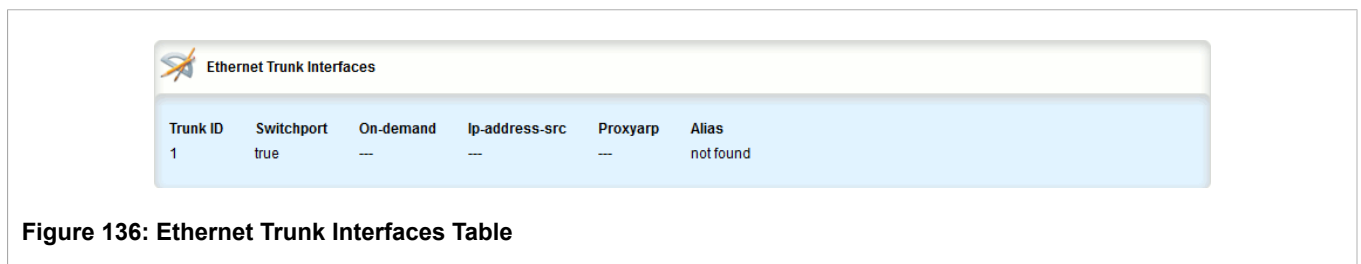
The following sections describe how to configure and manage Ethernet trunk interfaces:

- [Section 3.22.1, “Viewing a List of Ethernet Trunk Interfaces”](#)
- [Section 3.22.2, “Adding an Ethernet Trunk Interface”](#)
- [Section 3.22.3, “Deleting an Ethernet Trunk Interface”](#)
- [Section 3.22.4, “Managing Ethernet Trunk Ports”](#)

## Section 3.22.1

# Viewing a List of Ethernet Trunk Interfaces

To view a list of Ethernet trunk interfaces, navigate to **interface » trunks**. If trunks have been configured, the **Ethernet Trunk Interfaces** table appears.





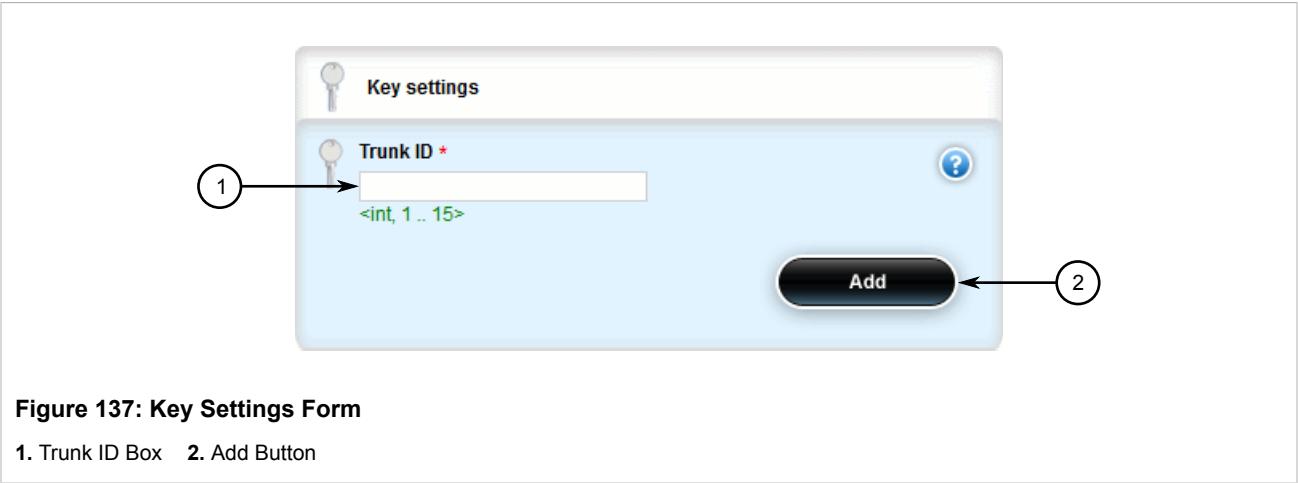
If no Ethernet trunk interfaces have been configured, add trunks as needed. For more information, refer to [Section 3.22.2, “Adding an Ethernet Trunk Interface”](#).

Section 3.22.2

## Adding an Ethernet Trunk Interface

To add an Ethernet trunk interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » trunks** and click **<Add trunks>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Trunk ID	<b>Synopsis:</b> An integer between 1 and 15 <int, 1 \\. 15>;The trunk number. It doesn't affect port trunk operation in any way and is only used for identification.

4. Click **Add** to create the new trunk. The **Ethernet Trunk Interfaces, Multicast Filtering, CoS and VLAN** forms appear.



**NOTE**  
*The `Proxyarp`, `Mtu` and `Alias` parameters are only available when the interface is in dedicated routing mode.*

The image shows a web interface form titled "Ethernet Trunk Interfaces". It contains several configuration options, each with a callout number in a circle pointing to it:

- 1. Points to the "Switchport" checkbox, which is currently unchecked.
- 2. Points to the "On-demand" checkbox, which is currently unchecked.
- 3. Points to the "Ip-address-src" dropdown menu, which is currently set to "static".
- 4. Points to the "Proxyarp" checkbox, which is currently unchecked.
- 5. Points to the "Mtu" field, which is currently set to "1500 (1500)".
- 6. Points to the "Alias" field, which is currently set to "--".

Each configuration option also has a help icon (a blue circle with a question mark) to its right.

**Figure 138: Ethernet Trunk Interfaces Form**

1. Switchport Check Box   2. On-Demand Check Box   3. IP Address Src List   4. Proxyarp Box   5. Mtu Box   6. Alias Box

The image shows a web interface form titled "Multicast Filtering". It contains a single configuration option, "GMRP", which is a dropdown menu. A callout number "1" in a circle points to the dropdown menu, which is currently set to "--". A help icon (a blue circle with a question mark) is located to the right of the dropdown menu.

**Figure 139: Multicast Filtering Form**

1. GMRP List

**Figure 140: CoS Form**  
1. Default Priority Box    2. Inspect TOS Check Box

**Figure 141: VLAN Form**  
1. PVID Box    2. Type List    3. Format List    4. GVRP Mode List

5. On the **Ethernet Trunk Interfaces** form, configure the following parameter(s) as required:

Parameter	Description
Switchport	<b>Synopsis:</b> true or false The physical port into either Switched mode or a dedicated Routing mode.
on-demand	<b>Synopsis:</b> typeless Bring up this interface on-demand only
ip-address-src	<b>Synopsis:</b> { static, dynamic } Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP

Parameter	Description
	and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
proxyarp	<b>Synopsis:</b> typeless Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
mtu	<b>Synopsis:</b> An integer between 68 and 1500 <b>Default:</b> 1500 Maximum transmission unit (largest packet size allowed for this interface).
alias	<b>Synopsis:</b> A string 1 to 64 characters long The SNMP alias name of the interface

6. On the **Multicast Filtering** form, configure the following parameter(s) as required:

Parameter	Description
GMRP	<b>Synopsis:</b> { advertise_only, learn_advertise } GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: <itemizedlist><listitem>DISABLED : the port is not capable of any GMRP processing.</listitem> <listitem>ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.</listitem> <listitem>ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.</listitem></itemizedlist>

7. On the **CoS** form, configure the following parameter(s) as required:

Parameter	Description
Default Priority	<b>Synopsis:</b> An integer between 0 and 7 <b>Default:</b> 0 The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
Inspect ToS	<b>Synopsis:</b> typeless 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.

8. On the **VLAN** form, configure the following parameter(s) as required:

Parameter	Description
PVID	<b>Synopsis:</b> An integer between 1 and 4094 The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.
Type	<b>Synopsis:</b> { edge, trunk, pvlannedge } <b>Default:</b> edge

Parameter	Description
	How the port determines its membership in VLANs. There are the following port types: <itemizedlist><listitem>EDGE : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter).</listitem> <listitem>PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN.</listitem> <listitem>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.</listitem></itemizedlist>
Format	<b>Synopsis:</b> { untagged, tagged } <b>Default:</b> untagged  Whether frames transmitted out of the port on its native VLAN(specified by the 'PVID' parameter) will be tagged or untagged.
GVRP Mode	<b>Synopsis:</b> { advertise_only, learn_advertise }  GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: <itemizedlist><listitem>DISABLED : the port is not capable of any GVRP processing.</listitem> <listitem>ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.</listitem> <listitem>ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.</listitem></itemizedlist>

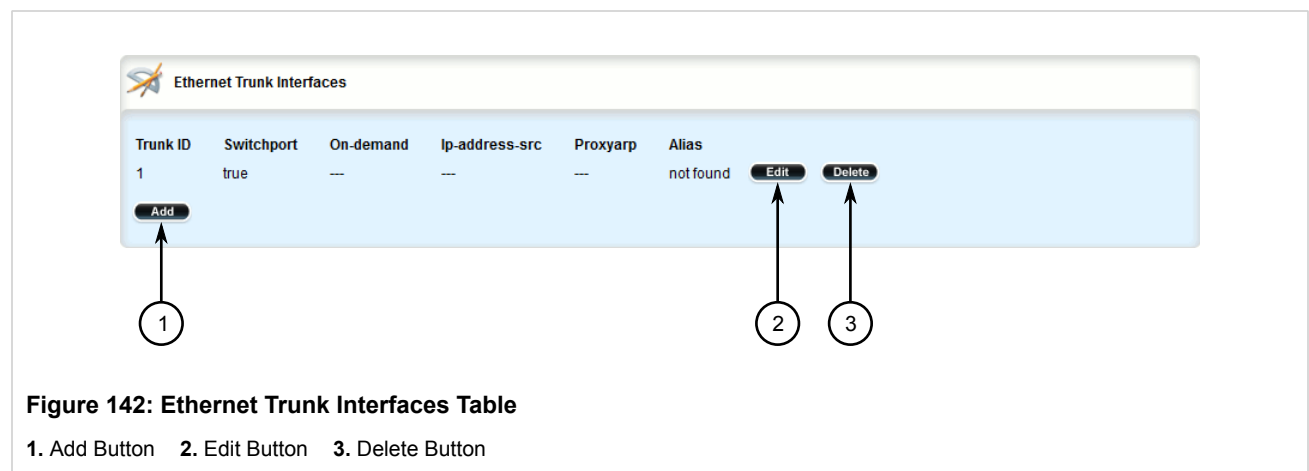
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 3.22.3

## Deleting an Ethernet Trunk Interface

To delete an Ethernet trunk interface, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **interface » trunks**. The **Ethernet Trunk Interfaces** table appears.



3. Click **Delete** next to the chosen trunk.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 3.22.4

## Managing Ethernet Trunk Ports

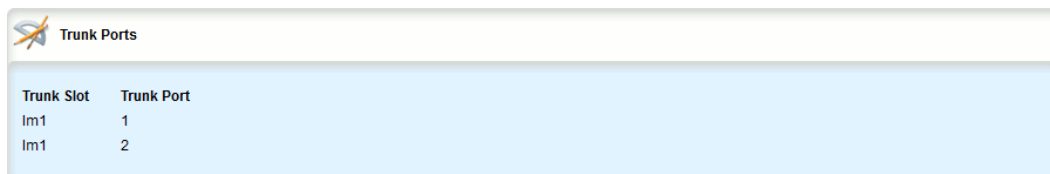
The following sections describe how to configure and manage Ethernet trunk ports:

- [Section 3.22.4.1, “Viewing a List of Ethernet Trunk Ports”](#)
- [Section 3.22.4.2, “Adding an Ethernet Trunk Port”](#)
- [Section 3.22.4.3, “Deleting an Ethernet Trunk Port”](#)

## Section 3.22.4.1

### Viewing a List of Ethernet Trunk Ports

To view a list of Ethernet trunk ports, navigate to **interface » trunks » {id} » trunk-ports**, where {id} is the ID given to the interface. If trunk ports have been configured, the **Trunk Ports** table appears.



Trunk Slot	Trunk Port
Im1	1
Im1	2

**Figure 143: Trunk Ports Table**

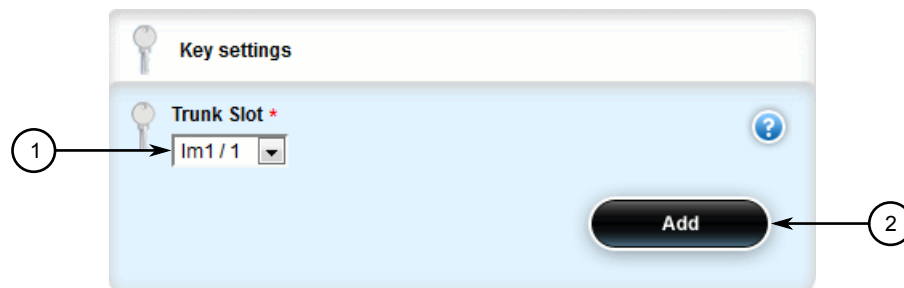
If no Ethernet trunk ports have been configured, add ports as needed. For more information, refer to [Section 3.22.4.2, “Adding an Ethernet Trunk Port”](#).

## Section 3.22.4.2

### Adding an Ethernet Trunk Port

To add an Ethernet trunk port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » trunks » {id} » trunk-ports**, where {id} is the ID given to the interface.
3. Click **<Add trunk-ports>**. The **Key Settings** form appears.



**Figure 144: Key Settings Form**

1. Trunk Slot List   2. Add Button

4. Configure the following parameter(s) as required:



**NOTE**

*Routable Ethernet ports cannot be configured as trunk ports.*

Parameter	Description
Trunk Slot	The name of the module location provided on the silkscreen across the top of the device.
Trunk Port	The selected ports on the module installed in the indicated slot.

5. Click **Add** to create the new trunk port.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 3.22.4.3

## Deleting an Ethernet Trunk Port

To delete an Ethernet trunk port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » trunks » {id} » trunk-ports**, where *{id}* is the ID given to the interface. The **Trunk Ports** table appears.

Trunk Slot	Trunk Port		
Im1	1	Edit	Delete
Im1	2	Edit	Delete
		Add	

**Figure 145: Trunk Ports Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen trunk port.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 3.23

## 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 L2 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 L2 traffic going through the virtual switch, network latency is minimized for the traffic between end devices.

The virtual switch appears on the device as a virtual Ethernet interface over a physical interface (i.e. T1/E1 HDLC-ETH or Ethernet port) between two routers. Physically, the two routers can be in different locations.

There can be multiple virtual switch instances in a router. Each instance can include two or more interfaces, but an interface can only be a member of one virtual switch instance.

**NOTE**

*There can be multiple virtual switch interfaces over a T1/E1 HDLC-ETH interface, in which the virtual switch interfaces are separated by creating a VLAN over the T1/E1 HDLC-ETH interface.*

A virtual switch interface in a router can be a routable interface when an IP address is assigned either statically or through DHCP. The network address assigned to the virtual switch interface can be included in the dynamic routing protocol. The interface can also call a routing update. The IP address assigned to the virtual switch can be used as the default gateway for the end devices connected to the virtual switch interface. Network services, such as SSH, DHCP, NTP, VRRP, etc., can be configured to run on the virtual switch interface.



Network traffic can be filtered for select virtual switch interfaces based on destination MAC address, source MAC address, and/or protocol (e.g. iso, arp, ipv4, ipv6, etc.). If a packet meets the filter criteria, it is routed to the appropriate destination. Otherwise, it is dropped.

When configuring a virtual switch, be aware of the following:

- Be careful when adding a VLAN interface (assigned to a switch port on a given line module) in the virtual switch. The VLAN tag on a tagged frame received on the VLAN interface of a switch port may not be preserved when the traffic is egressed through a routable interface (i.e. T1/E1 HLDC-ETH or FE-CM-1), which is also part of the same virtual switch instance. However, a VLAN tag is preserved when tagged traffic is received on a routable interface.
- Any IP address assigned to an interface becomes inactive and hidden when the interface is added to the virtual switch. The address on the interface is reactivated after removing the interface from the virtual switch.
- Be careful when adding interfaces to the virtual switch. Any network services running on the individual interfaces will need to be reconfigured after adding the interface to the virtual switch. For example, if a DHCP server running on FE-CM-1 is subsequently made a member of the VirtualSwitch vsw-1, the DHCP configuration must be changed to refer to vsw-1.
- The virtual switch is implemented in the RUGGEDCOM ROX II software. Therefore, a CPU resource is needed to forward broadcast, multicast and unicast traffic.
- If the router is running as a firewall, the **routeback** parameter under **firewall » fwconfig » fwinterface** must be enabled for the virtual switch interface. For more information, refer to [Section 5.16.9, “Managing Interfaces”](#).

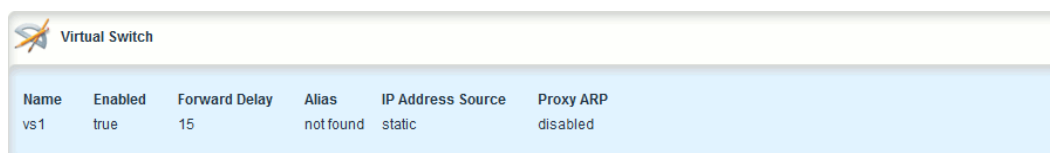
The following sections describe how to configure and manage virtual switches:

- [Section 3.23.1, “Viewing a List of Virtual Switches”](#)
- [Section 3.23.2, “Adding a Virtual Switch”](#)
- [Section 3.23.3, “Deleting a Virtual Switch”](#)
- [Section 3.23.4, “Managing Virtual Switch Interfaces”](#)
- [Section 3.23.5, “Filtering Virtual Switch Traffic”](#)
- [Section 3.23.6, “Managing Filtering Rules”](#)
- [Section 3.23.7, “Managing In/Out Interfaces”](#)

### Section 3.23.1

## Viewing a List of Virtual Switches

To view a list of virtual switches, navigate to **interface » virtualswitch**. If virtual switches have been configured, the **Virtual Switch** table appears.



Name	Enabled	Forward Delay	Alias	IP Address Source	Proxy ARP
vs1	true	15	not found	static	disabled

**Figure 146: Virtual Switch Table**

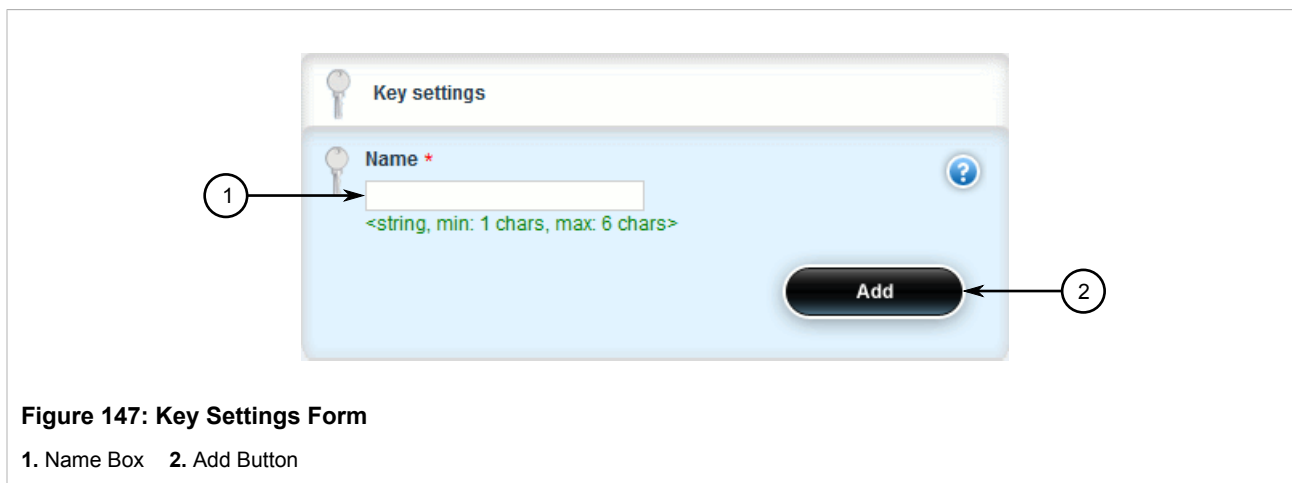
If no virtual switches have been configured, add switches as needed. For more information, refer to [Section 3.23.2, “Adding a Virtual Switch”](#).

Section 3.23.2

## Adding a Virtual Switch

To add virtual switch, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » virtualswitch** and click **<Add virtualswitch>** in the menu. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Name	<p><b>Synopsis:</b> A string 1 to 6 characters long</p> <p>The virtual switch interface name - the interface name must start with a lowercase letter, but may contain any combination of lowercase letters, numbers and dashes up to 6 characters. The prefix 'vsw-' will be added to this interface name.</p>

4. Click **Add** to create the new switch. The **Virtual Switch** form appears.

The screenshot shows the 'Virtual Switch' configuration form. It has a light blue background and a title bar with a switch icon and the text 'Virtual Switch'. The form contains several settings, each with a title, a value, and a help icon (a blue circle with a question mark). Numbered callouts point to the following fields:

- 1. Points to the 'Enabled' checkbox, which is checked and labeled 'Enabled (true)'.
- 2. Points to the 'Retain IP on Bridge Device' checkbox, which is unchecked and labeled 'Enabled (false)'.
- 3. Points to the 'Forward Delay' field, which is a text box containing '15' and labeled '(15)'.
- 4. Points to the 'Alias' field, which is a text box containing '--'.
- 5. Points to the 'IP Address Source' dropdown menu, which is set to 'static' and labeled '(static)'.
- 6. Points to the 'Proxy ARP' checkbox, which is unchecked and labeled 'Enabled'.

**Figure 148: Virtual Switch Form**

1. Enabled Check Box   2. Retain IP on Bridge Device Check Box   3. Forward Delay Box   4. Alias Box   5. IP Address Source List   6. ProxyARP Check Box

5. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables this interface.
Retain IP on Bridge Device	<b>Synopsis:</b> true or false <b>Default:</b> false Retain IP on bridge device.
Forward Delay	<b>Default:</b> 15 Delay (in seconds) of the listening and learning state before goes to forwarding state.
Alias	<b>Synopsis:</b> A string 1 to 64 characters long The SNMP alias name of the interface
IP Address Source	<b>Synopsis:</b> { static, dynamic } <b>Default:</b> static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
Proxy ARP	<b>Synopsis:</b> typeless

Parameter	Description
	Enables/Disables whether the port will respond to ARP requests for hosts other than itself

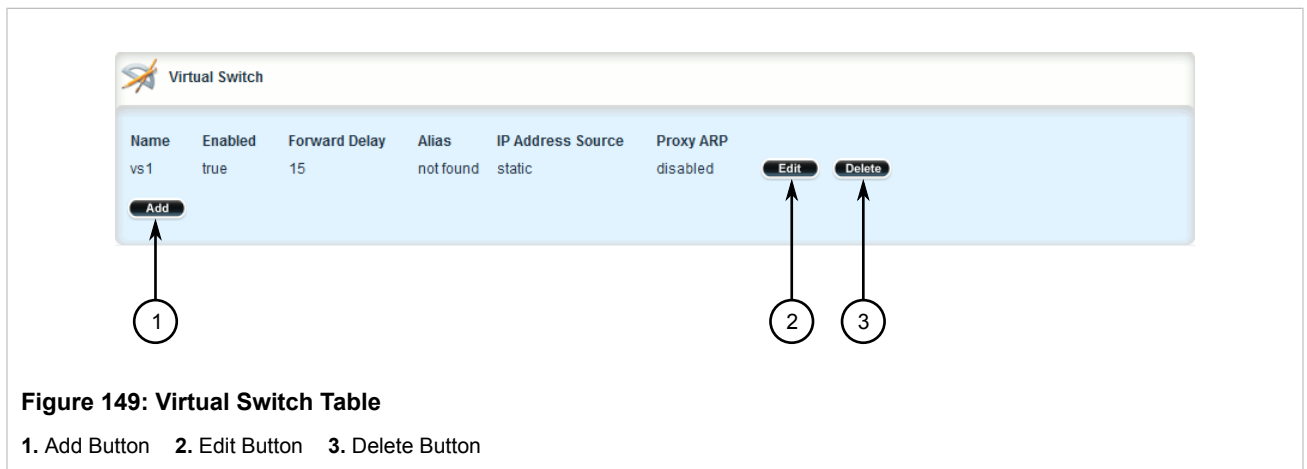
6. Add one or more interfaces for the virtual switch. For more information, refer to [Section 3.23.4.2, “Adding a Virtual Switch Interface”](#).
7. [Optional] Assign one or more VLANs to the virtual switch. For more information, refer to [Section 5.36.6.2, “Adding a Virtual Switch VLAN”](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

### Section 3.23.3

## Deleting a Virtual Switch

To delete a virtual switch, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » virtualswitch**. The **Virtual Switch** table appears.



3. Click **Delete** next to the chosen switch.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 3.23.4

## Managing Virtual Switch Interfaces

The following sections describe how to configure and manage virtual switch interfaces:

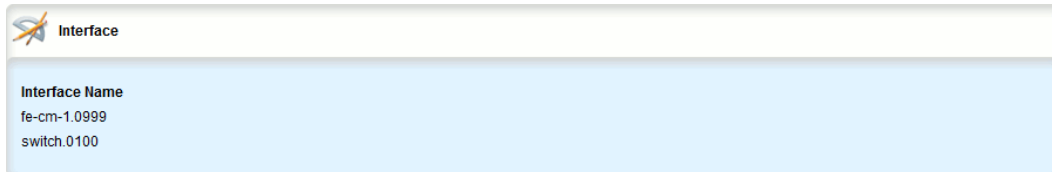
- [Section 3.23.4.1, “Viewing a List of Virtual Switch Interfaces”](#)
- [Section 3.23.4.2, “Adding a Virtual Switch Interface”](#)

- [Section 3.23.4.3, “Deleting a Virtual Switch Interface”](#)

## Section 3.23.4.1

## Viewing a List of Virtual Switch Interfaces

To view a list of virtual switch interfaces, navigate to **interface » virtualswitch » {name} » interface**, where **{name}** is the name assigned to the virtual switch. If interfaces have been configured, the **Interface** table appears.



Interface Name
fe-cm-1.0999
switch.0100

**Figure 150: Interface Table**

If no virtual switches have been configured, add switches as needed. For more information, refer to [Section 3.23.2, “Adding a Virtual Switch”](#).

## Section 3.23.4.2

## Adding a Virtual Switch Interface

To add a virtual switch interface, do the following:

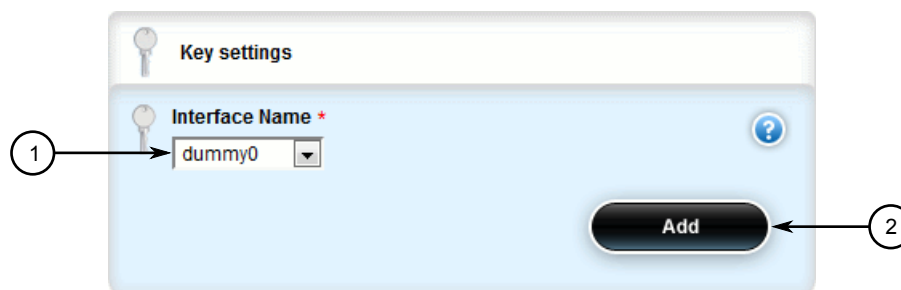
**IMPORTANT!**

*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 access the Web interface. Active Web sessions will be lost and the Web interface will be unreachable until the virtual switch is disabled.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » virtualswitch » {name} » interface**, where **{name}** is the name assigned to the virtual switch.
3. Click **<Add interface>**. The **Key Settings** form appears.



**Figure 151: Key Settings Form**

1. Interface Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	Interface name.

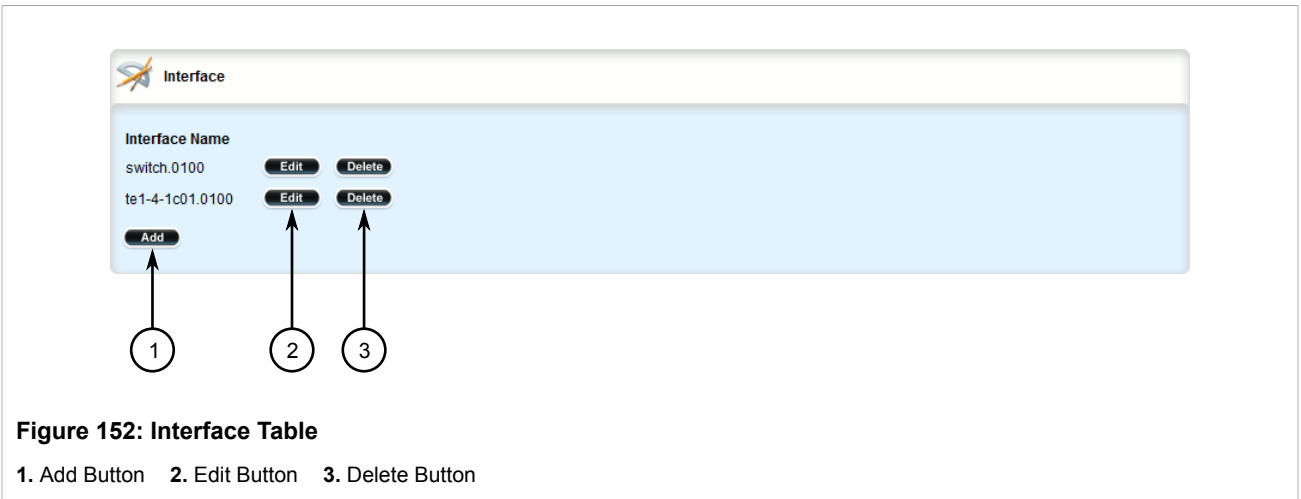
5. Click **Add** to create the new interface. The new interface is now visible under the *ip* menu. The name of the interface is the name of the virtual switch preceded by *vsw-* (i.e. *vsw-vs1*, *vsw-vs2*, etc.).
6. Assign an IPv4 or IPv6 address to the interface. For more information, refer to [Section 5.39.3.2, “Adding an IPv4 Address”](#) or [Section 5.39.6.2, “Adding an IPv6 Address”](#).
7. If necessary, add one or more VLANs to the virtual switch interface. For more information, refer to [Section 5.36.6.2, “Adding a Virtual Switch VLAN”](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

#### Section 3.23.4.3

### Deleting a Virtual Switch Interface

To delete a virtual switch interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » virtualswitch » {name} » interface**, where *{name}* is the name assigned to the virtual switch. The **Interface** table appears.



3. Click **Delete** next to the chosen interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.23.5

## 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.

The following sections describe how to configure and manage virtual switch filters:

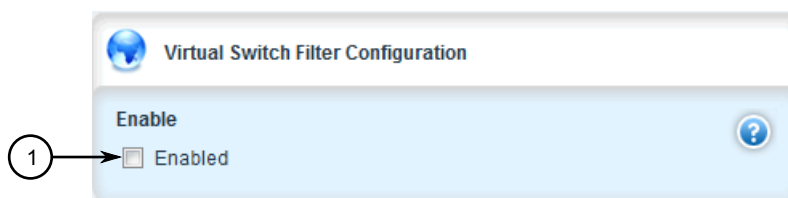
- [Section 3.23.5.1, “Enabling/Disabling Virtual Switch Filtering”](#)
- [Section 3.23.5.2, “Viewing a List of Virtual Switch Filters”](#)
- [Section 3.23.5.3, “Adding a Virtual Switch Filter”](#)
- [Section 3.23.5.4, “Deleting a Virtual Switch Filter”](#)

#### Section 3.23.5.1

### Enabling/Disabling Virtual Switch Filtering

To enable or disable virtual switch filtering, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter**. The **Virtual Switch Filter Configuration** form appears.



**Figure 153: Virtual Switch Filter Configuration Form**

1. Enabled Check Box

3. Click **Enabled** to enable virtual switch filtering, or clear **Enabled** to disable virtual switch filtering.
4. 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 3.23.2, "Adding a Virtual Switch"](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 3.23.5.2

### Viewing a List of Virtual Switch Filters

To view a list of virtual switch filters, navigate to **security » virtualswitch-filter » virtualswitch**. If filters have been configured, the **Virtualswitch** table appears.

Virtual Switch
Interface Name vs1

**Figure 154: Virtual Switch Table**

If no virtual switch filters have been configured, add filters as needed. For more information, refer to [Section 3.23.5.3, "Adding a Virtual Switch Filter"](#).

#### Section 3.23.5.3

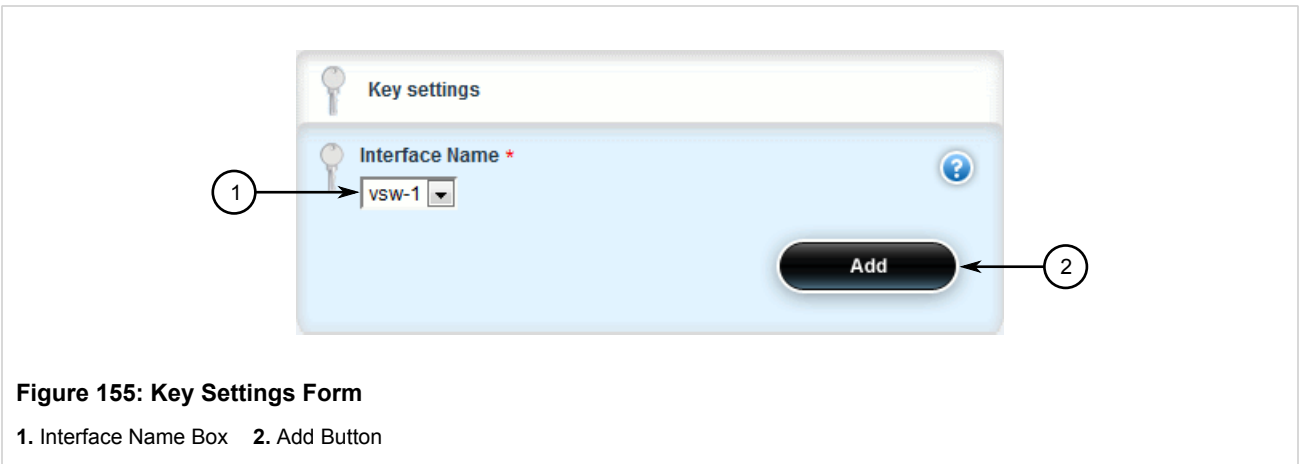
### Adding a Virtual Switch Filter

To add a virtual switch filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure one or more virtual switches are configured and **Retain IP on Bridge Device** is enabled. For more information, refer to [Section 3.23.2, "Adding a Virtual Switch"](#).



3. Navigate to **security » virtualswitch-filter » virtualswitch** and click **<Add virtualswitch>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	The name of the target virtual switch.

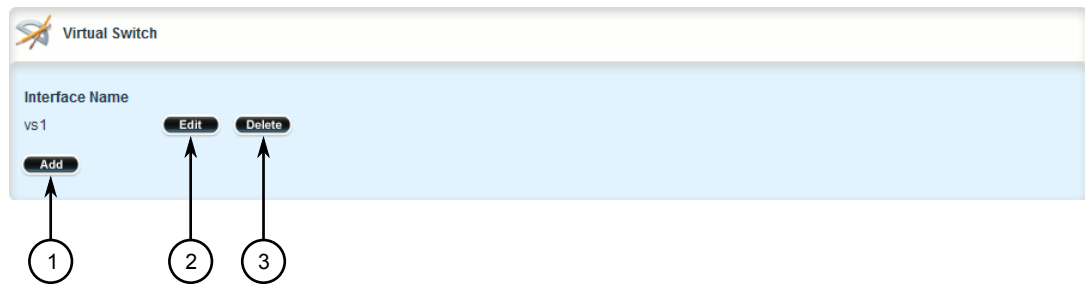
5. Configure one or more rules to be used when filtering. For more information, refer to [Section 3.23.6.3, “Adding a Rule”](#).
6. Add the desired rules to the virtual switch filter. For more information, refer to [Section 3.23.6.4, “Adding a Rule to a Virtual Switch Filter”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 3.23.5.4

### Deleting a Virtual Switch Filter

To delete a virtual switch filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter » virtualswitch**. The **Virtualswitch** table appears.



**Figure 156: Virtual Switch Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen filter.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.23.6

## Managing Filtering Rules

A virtual switch filter can apply one or more rules to traffic traversing a virtual switch.

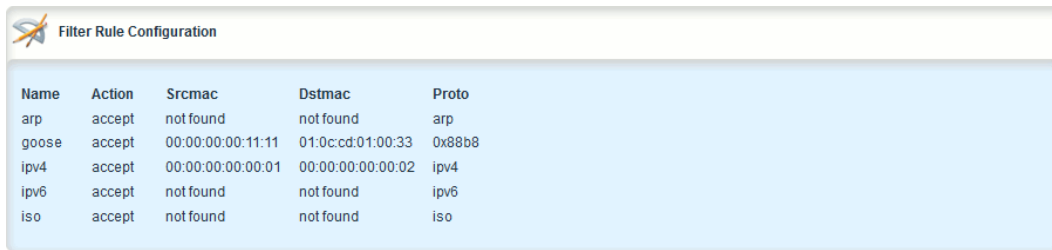
The following sections describe how to configure and manage the individual rules and apply them to a virtual switch filter:

- [Section 3.23.6.1, “Viewing a List of Rules”](#)
- [Section 3.23.6.2, “Viewing a List of Rules Assigned to a Virtual Switch Filter”](#)
- [Section 3.23.6.3, “Adding a Rule”](#)
- [Section 3.23.6.4, “Adding a Rule to a Virtual Switch Filter”](#)
- [Section 3.23.6.5, “Deleting a Rule”](#)
- [Section 3.23.6.6, “Deleting a Rule from a Virtual Switch Filter”](#)

#### Section 3.23.6.1

### Viewing a List of Rules

To view a list of rules that can be used by a virtual switch filter, navigate to **security » virtualswitch-filter » rules**. If rules have been configured, the **Filter Rule Configuration** table appears.



The image shows a screenshot of the 'Filter Rule Configuration' window. It contains a table with five columns: Name, Action, Srcmac, Dstmac, and Proto. The table lists six rules: arp, goose, ipv4, ipv6, and iso. The 'Srcmac' and 'Dstmac' columns for 'arp' and 'iso' are 'not found', while 'goose', 'ipv4', and 'ipv6' have specific MAC addresses. The 'Proto' column shows 'arp', '0x88b8', 'ipv4', 'ipv6', and 'iso' respectively.

Name	Action	Srcmac	Dstmac	Proto
arp	accept	not found	not found	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	not found	not found	ipv6
iso	accept	not found	not found	iso

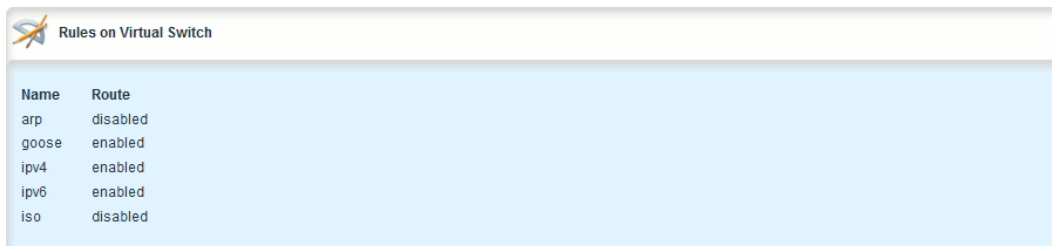
**Figure 157: Filter Rule Configuration Table**

If no rules have been configured, add rules as needed. For more information, refer to [Section 3.23.6.3, “Adding a Rule”](#).

#### Section 3.23.6.2

### Viewing a List of Rules Assigned to a Virtual Switch Filter

To view a list of rules assigned to a virtual switch filter, navigate to **security » virtualswitch-filter » virtualswitch » {name} » rule**, where {name} is the name of the virtual switch filter. If filters have been configured, the **Rules on Virtual Switch** table appears.



The image shows a screenshot of the 'Rules on Virtual Switch' window. It contains a table with two columns: Name and Route. The table lists five rules: arp, goose, ipv4, ipv6, and iso. The 'Route' column shows 'disabled' for 'arp' and 'iso', and 'enabled' for 'goose', 'ipv4', and 'ipv6'.

Name	Route
arp	disabled
goose	enabled
ipv4	enabled
ipv6	enabled
iso	disabled

**Figure 158: Rules on Virtual Switch Table**

If no rules have been assigned, assign them as needed. For more information, refer to [Section 3.23.6.4, “Adding a Rule to a Virtual Switch Filter”](#).

#### Section 3.23.6.3

### Adding a Rule

To add a rule that can be used by a virtual switch filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter » rules** and click **<Add rules>**. The **Key Settings** form appears.

**Figure 159: Key Settings Form**

1. Name Box 2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 32 characters long Description of virtual switch rule

- Click **Add**. The **Virtual Switch Rules** form appears.

**Figure 160: Virtual Switch Rules Form**

1. Action List 2. Source MAC Address Box 3. Destination MAC Address Box 4. Protocol Box

- Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { accept, drop } <b>Default:</b> accept The action taken when an incoming frame meets the criteria.

Parameter	Description
Source MAC Address	<b>Synopsis:</b> A string The required source MAC address for incoming frames.
Destination MAC Address	<b>Synopsis:</b> A string The required destination MAC address for incoming frames.
Protocol	<b>Synopsis:</b> { iso, arp, ipv4, ipv6 } or a string The pre-defined protocol or hex-string (i.e. 0x88A2) used to create the frames.

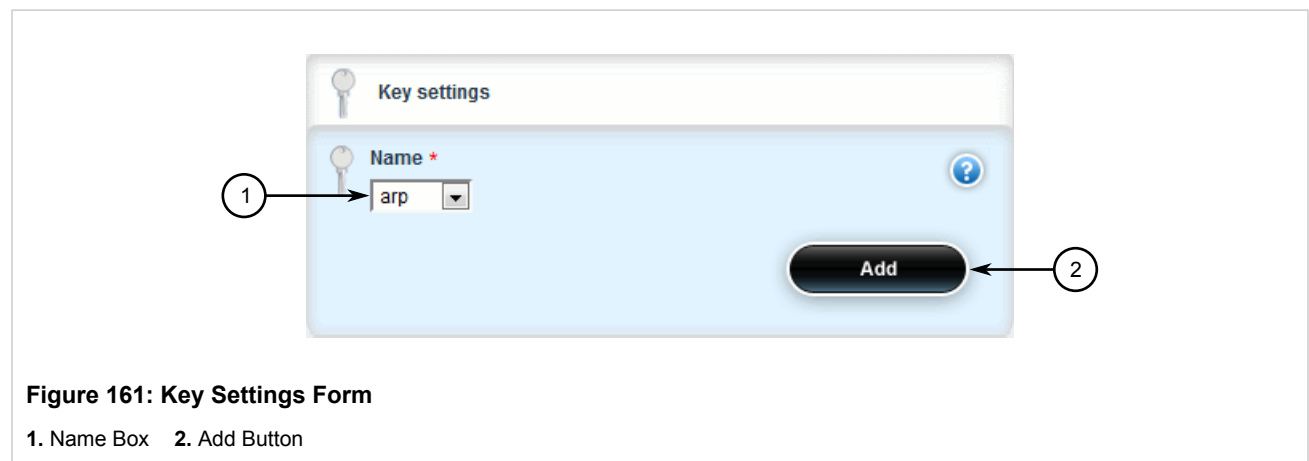
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.
- Add the rule to a virtual switch filter. For more information, refer to [Section 3.23.6.4, “Adding a Rule to a Virtual Switch Filter”](#).

#### Section 3.23.6.4

### Adding a Rule to a Virtual Switch Filter

To add a rule to a virtual switch filter, do the following:

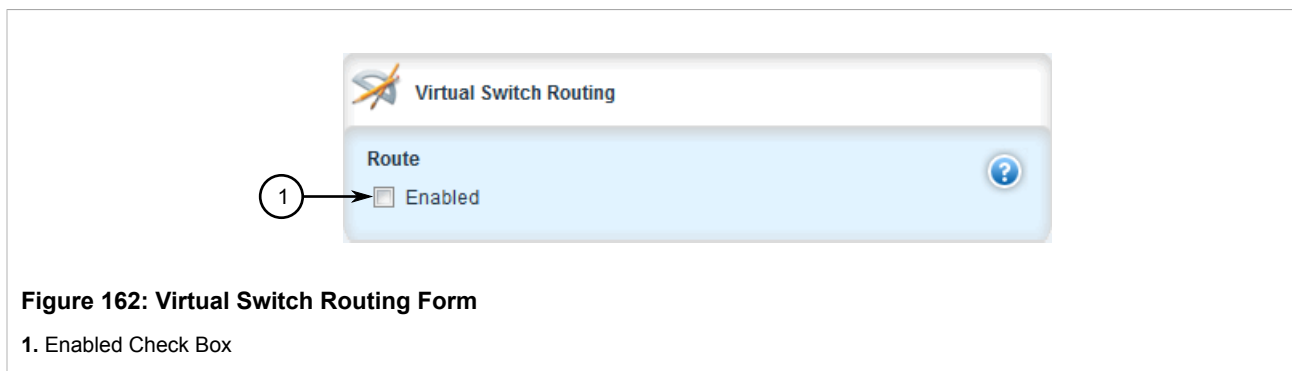
- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » virtualswitch-filter » virtualswitch » {name} » rule** and click **<Add rule>**. The **Key Settings** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
name	The rule applied to traffic traversing the virtual switch.

- Click **Add**. The **Virtual Switch Routing** form appears.



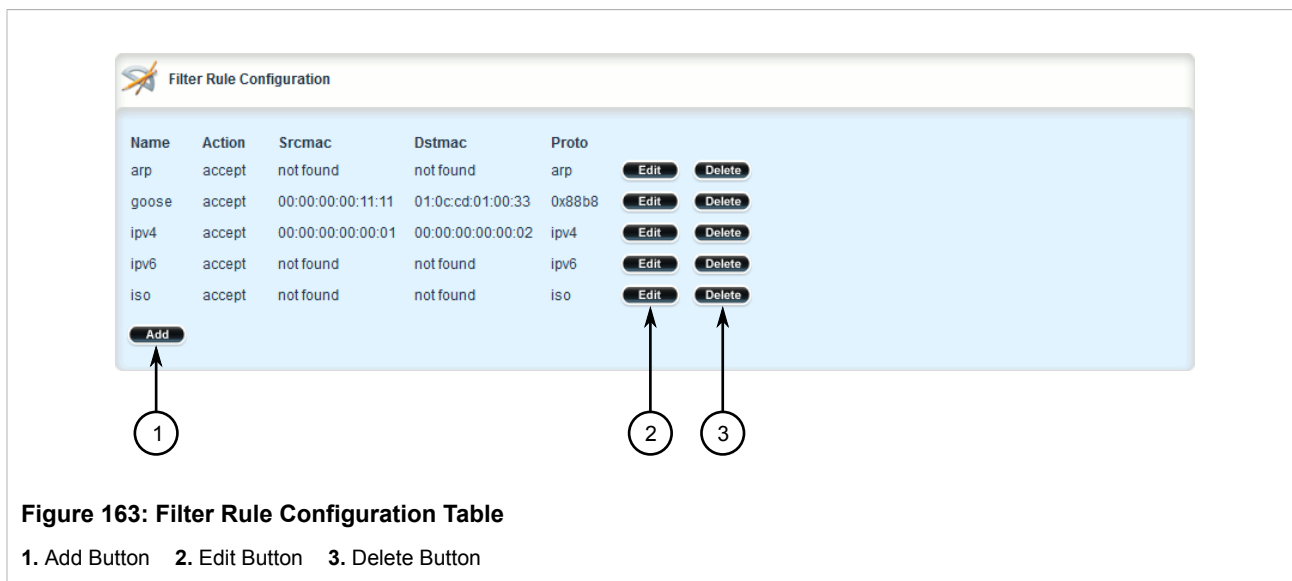
5. Select **Enable**.
6. Configure the in/out interfaces for the rule. For more information, refer to [Section 3.23.7.2, “Adding In/Out Interfaces”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 3.23.6.5

### Deleting a Rule

To delete a rule used to filter virtual switch traffic, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter » rules**. The **Filter Rule Configuration** table appears.



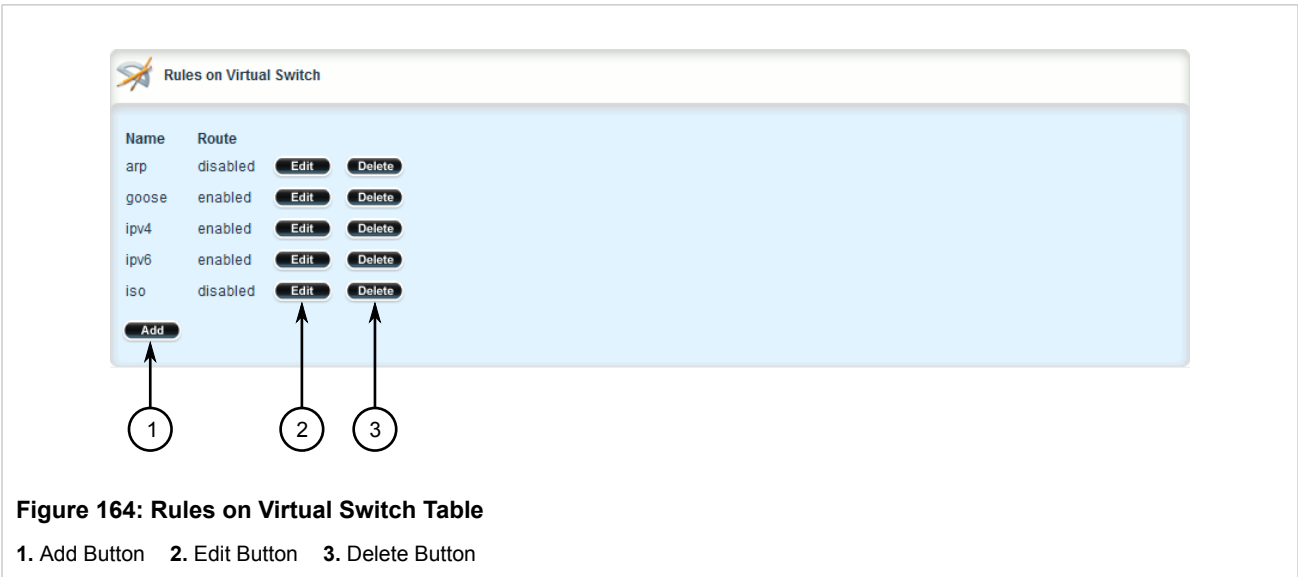
3. Click **Delete** next to the chosen rule.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 3.23.6.6

## Deleting a Rule from a Virtual Switch Filter

To delete a rule from a virtual switch filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter » virtualswitch » {name} » rule**, where {name} is the name of the virtual switch filter. The **Rules on Virtual Switch** table appears.



3. Click **Delete** next to the chosen rule.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 3.23.7

## 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.

The following sections describe how to configure and manage the in/out interfaces a virtual switch filter:

- [Section 3.23.7.1, "Viewing a List of In/Out Interfaces"](#)
- [Section 3.23.7.2, "Adding In/Out Interfaces"](#)
- [Section 3.23.7.3, "Deleting an In/Out Interface"](#)

## Section 3.23.7.1

### Viewing a List of In/Out Interfaces

To view a list of in/out interfaces that can be used by a virtual switch filter, navigate to **security » virtualswitch-filter » virtualswitch » {name} » rule » {rule} » in-interface|out-interface**, where {name} is the name of the

virtual switch filter and *{rule}* is the name of the rule. If in/out interfaces have been configured, the **Rules on an in-interface virtualswitch** or **Rules on an out-interface virtualswitch** table appears.



**Figure 165: Rules on an in-interface virtualswitch Table (Example)**

If no in/out interfaces have been configured, add interfaces as needed. For more information, refer to [Section 3.23.7.2, “Adding In/Out Interfaces”](#).

### Section 3.23.7.2

## Adding In/Out Interfaces

To add an in/out interface that can be used by a virtual switch filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter » virtualswitch » {name} » rule » {rule} » in-interface|out-interface**, where *{name}* is the name of the virtual switch filter and *{rule}* is the name of the rule.
3. Click **<Add in-interface>** or **<Add out-interface>** in the menu. The **Key Settings** form appears.



**Figure 166: Key Settings Form**

1. Name List 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
name	The input interface to be monitored.

5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

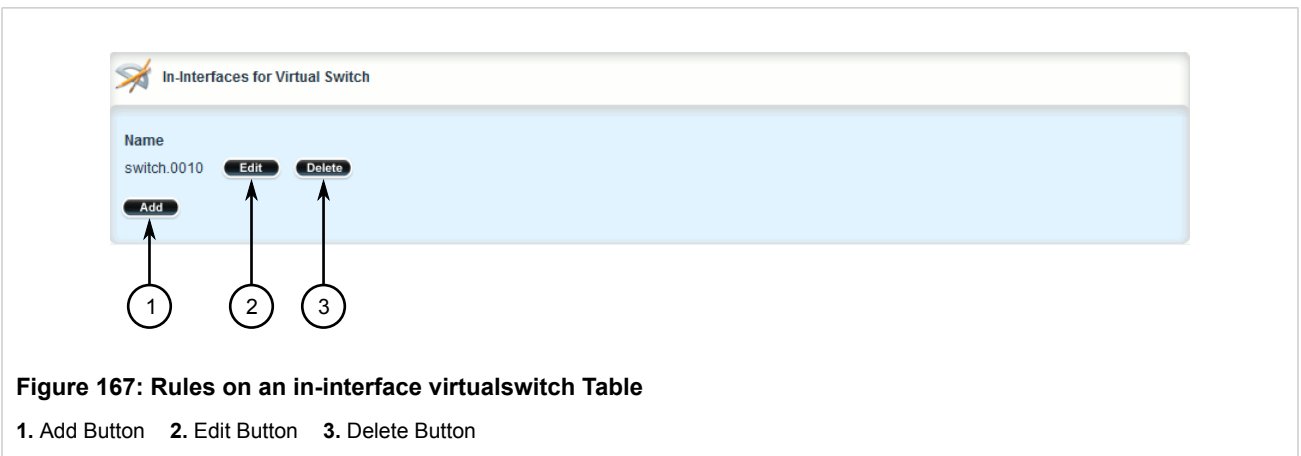


## Section 3.23.7.3

## Deleting an In/Out Interface

To delete an in/out interface that can be used by a virtual switch filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » virtualswitch-filter » virtualswitch » {name} » rule » {rule} » in-interface|out-interface**, where {name} is the name of the virtual switch filter and {rule} is the name of the rule. The **Rules on an in-interface virtualswitch** or **Rules on an out-interface virtualswitch** table appears.



3. Click **Delete** next to the chosen interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 3.24

## Managing a Domain Name System (DNS)

The following sections describe how to configure and manage a Domain Name Server (DNS):

- [Section 3.24.1, "Managing Domain Names"](#)
- [Section 3.24.2, "Managing Domain Name Servers"](#)

## Section 3.24.1

### 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).

The following sections describe how to configure and manage a list of domain names:

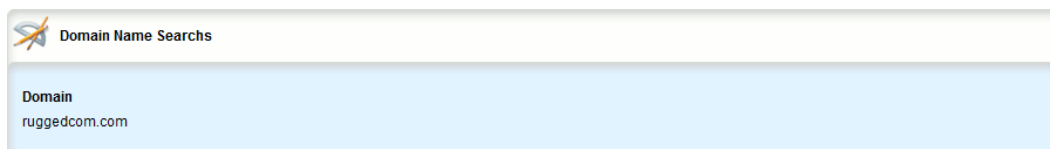
- [Section 3.24.1.1, "Viewing a List of Domain Names"](#)
- [Section 3.24.1.2, "Adding a Domain Name"](#)

- [Section 3.24.1.3, “Deleting a Domain Name”](#)

#### Section 3.24.1.1

### Viewing a List of Domain Names

To view a list of domain names, navigate to **admin » dns » search**. If domain names have been configured, the **Domain Name Searches** table appears.



Domain
ruggedcom.com

**Figure 168: Domain Name Searches Table**

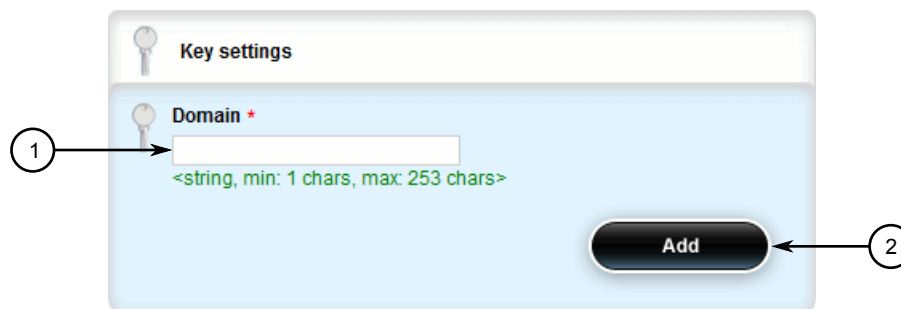
If no domain names have been configured, add names as needed. For more information, refer to [Section 3.24.1.2, “Adding a Domain Name”](#).

#### Section 3.24.1.2

### Adding a Domain Name

To add a domain name, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » dns » search** and click **<Add search>**. The **Key Settings** form appears.



**Figure 169: Key Settings Form**

1. Domain Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
domain	<b>Synopsis:</b> A string

4. Click **Add**.

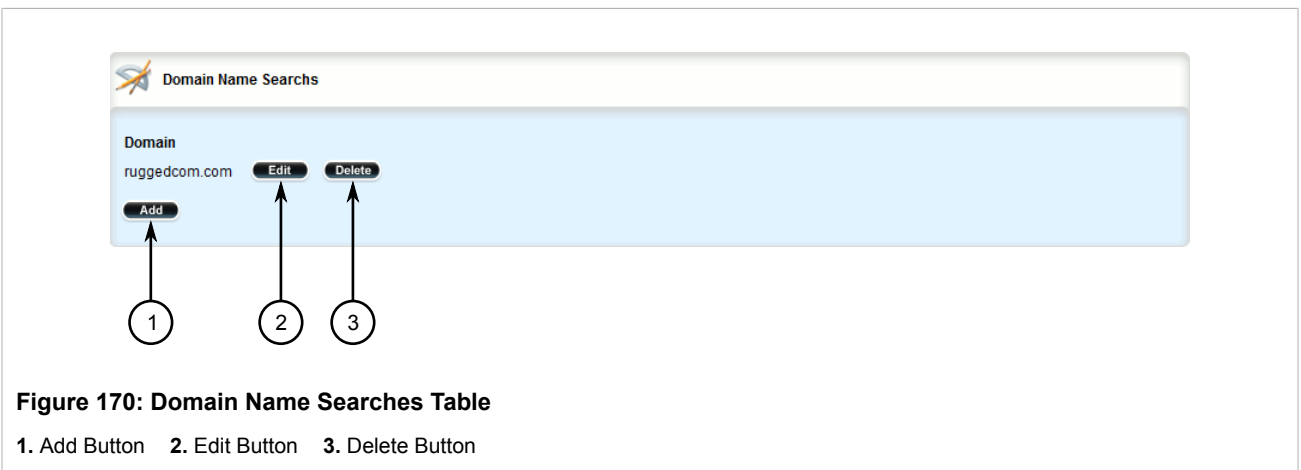
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 3.24.1.3

### Deleting a Domain Name

To delete a domain name, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » dns » search**. The **Domain Name Searches** table appears.



3. Click **Delete** next to the chosen domain name.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 3.24.2

### 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.

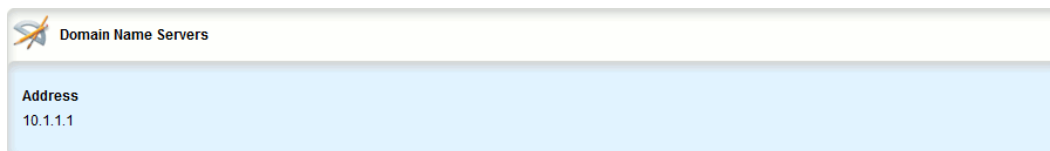
The following sections describe how to configure and manage a list of domain name servers:

- [Section 3.24.2.1, “Viewing a List of Domain Name Servers”](#)
- [Section 3.24.2.2, “Adding a Domain Name Server”](#)
- [Section 3.24.2.3, “Deleting a Domain Name Server”](#)

### Section 3.24.2.1

## Viewing a List of Domain Name Servers

To view a list of domain name servers, navigate to **admin » dns » server**. If domain name servers have been configured, the **Domain Name Servers** table appears.



Address
10.1.1.1

**Figure 171: Domain Name Servers Table**

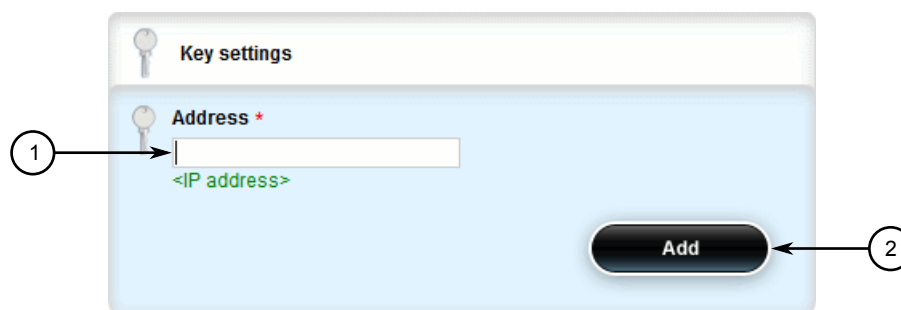
If no domain name servers have been configured, add servers as needed. For more information, refer to [Section 3.24.2.2, “Adding a Domain Name Server”](#).

### Section 3.24.2.2

## Adding a Domain Name Server

To add a domain name server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » dns » server** and click **<Add server>**. The **Key Settings** form appears.



**Figure 172: Key Settings Form**

1. Address Box 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
address	<b>Synopsis:</b> A string

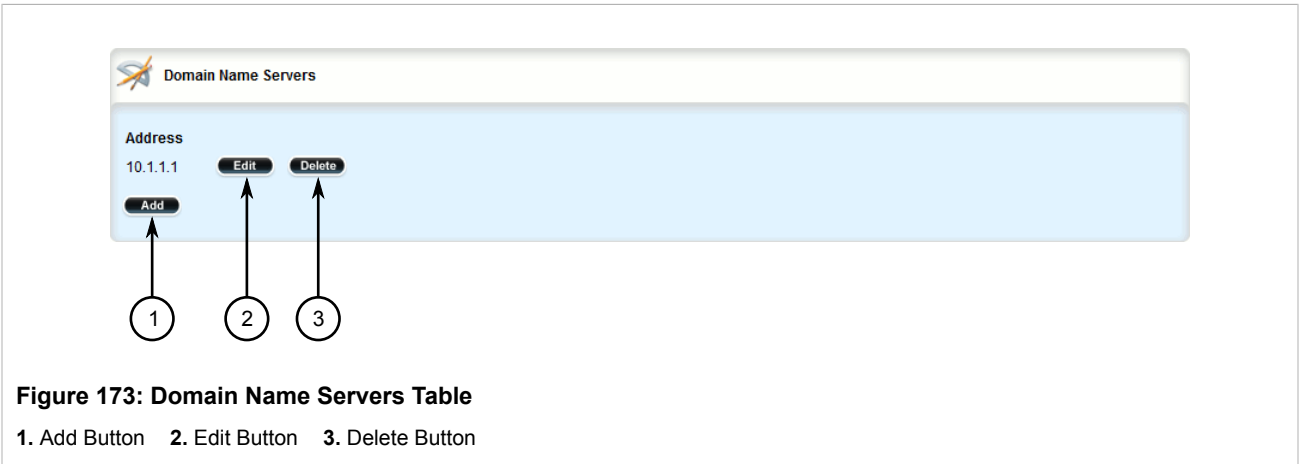
4. Click **Add**.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

Section 3.24.2.3

## Deleting a Domain Name Server

To delete a domain name server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » dns » server**. The **Domain Name Servers** table appears.



3. Click **Delete** next to the chosen domain name server.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.



# 4 System Administration

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

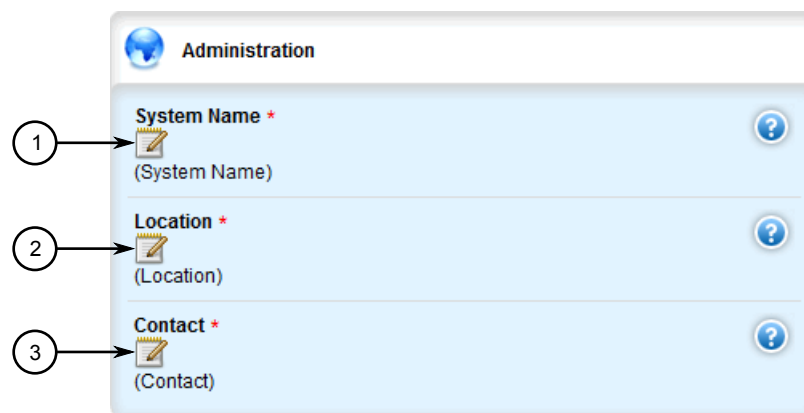
- [Section 4.1, “Configuring the System Name and Location”](#)
- [Section 4.2, “Configuring the Hostname”](#)
- [Section 4.3, “Customizing the Welcome Screen”](#)
- [Section 4.4, “Setting the User Authentication Mode”](#)
- [Section 4.5, “Setting the Maximum Number of Sessions”](#)
- [Section 4.6, “Managing Alarms”](#)
- [Section 4.7, “Managing Certificates and Keys”](#)
- [Section 4.8, “Managing RADIUS Authentication”](#)
- [Section 4.9, “Managing Users”](#)
- [Section 4.10, “Managing Passwords and Passphrases”](#)
- [Section 4.11, “Scheduling Jobs”](#)

## Section 4.1

# Configuring the System Name and Location

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin**. The **Administration** form appears.



The screenshot shows the 'Administration' form with a light blue header and a white body. The form contains three main sections, each with a yellow notepad icon and a blue question mark icon. The sections are labeled 'System Name \*', 'Location \*', and 'Contact \*'. Below each label is a text input field. To the left of the form, three numbered circles (1, 2, 3) have arrows pointing to the input fields for System Name, Location, and Contact respectively.

**Figure 174: Administration Form**

1. System Name Box   2. Location Box   3. Contact Box

- Configure the following parameter(s) as required:

Parameter	Description
System Name	<p><b>Synopsis:</b> A string 1 to 255 characters long  <b>Default:</b> System Name</p> <p>An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.</p>
Location	<p><b>Synopsis:</b> A string 1 to 255 characters long  <b>Default:</b> Location</p> <p>The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string.</p>
contact	<p><b>Synopsis:</b> A string 1 to 255 characters long  <b>Default:</b> Contact</p> <p>The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 4.2

## Configuring the Hostname

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

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin**. The **Hostname** form appears.

**Figure 175: Hostname Form**

1. Name Box    2. Domain Box

- Configure the following parameter(s) as required:



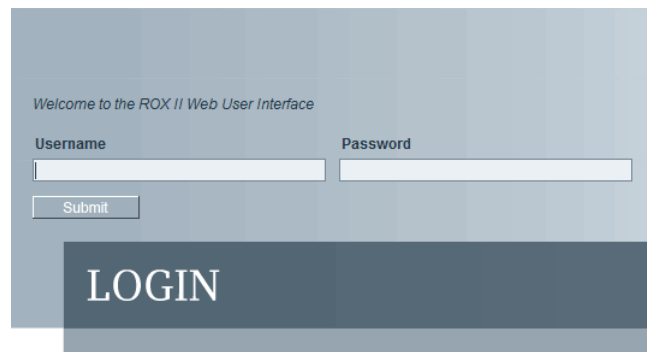
Parameter	Description
name	<b>Synopsis:</b> A string 1 to 63 characters long <b>Default:</b> ruggedcom The hostname that is the name of this device.
domain	<b>Synopsis:</b> A string <b>Default:</b> localdomain The domain for this hostname.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 4.3

## Customizing the Welcome Screen

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



**Figure 176: A Customized Welcome Screen**

To add a welcome message, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » authentication**. The **Authentication** form appears.

**Figure 177: Authentication Form**

1. Mode List    2. Banner Box

3. Under **Banner**, type the welcome message.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

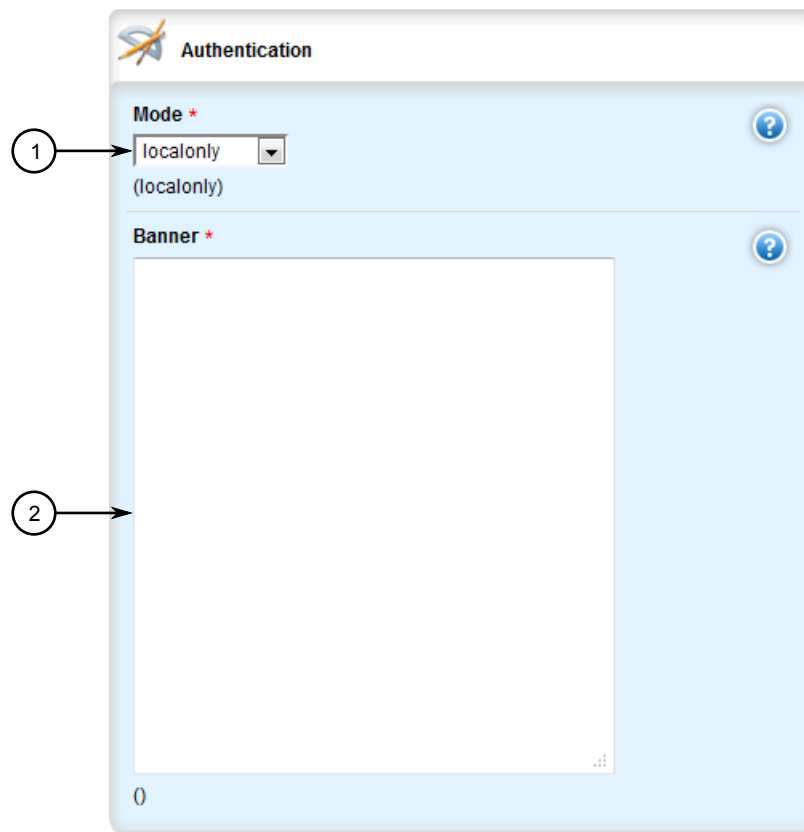
#### Section 4.4

## Setting the User Authentication Mode

The user authentication mode controls whether user log in attempts are authenticated locally or by a RADIUS server.

To set the authentication mode, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » authentication**. The **Authentication** form appears.



**Figure 178: Authentication Form**

1. Mode List    2. Banner Box

3. Under **Mode**, select the authentication method.
  - If **localonly** is selected, users will be authenticated locally, regardless of whether or not a RADIUS 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\_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.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

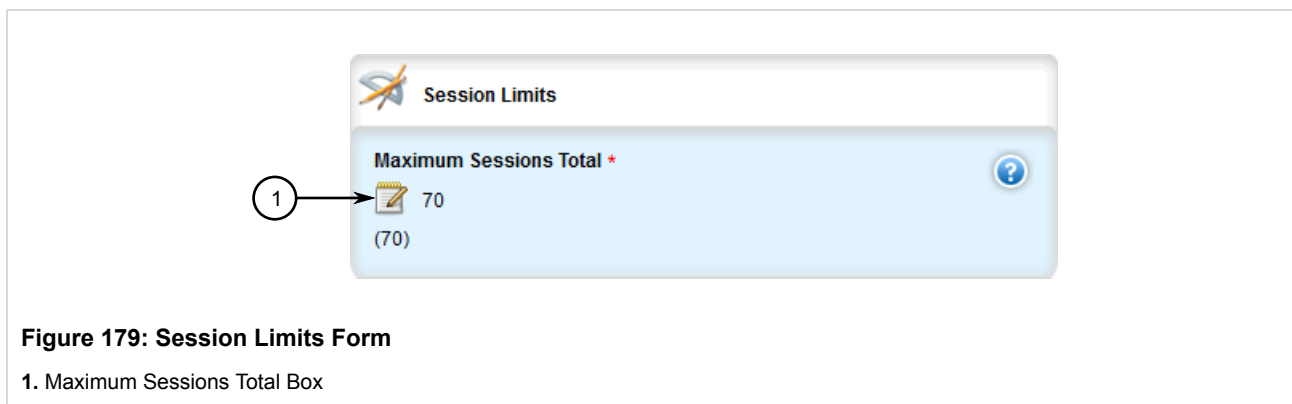
#### Section 4.5

## Setting the Maximum Number of Sessions

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.

- Navigate to **admin**. The **Session Limits** form appears.



- Configure the following parameter(s) as required:

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

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 4.6

## Managing Alarms

The alarm system in RUGGEDCOM ROX II notifies users when events of interest occur. The system is highly configurable, allowing users to:

- Enable/disable most alarms, with the exception of mandatory alarms
- Configure whether or not an alarm triggers the failsafe relay and illuminates the alarm indicator LED on the device
- Configure the severity of most alarms (i.e. emergency, alert, critical, error, etc.), with the exception of some where the severity is fixed

Each alarm is categorized by its type (or subsystem):

Alarm Type	Description
Admin	Admin alarms are for administrative aspects of the device, such as feature-key problems.
Chassis	Chassis alarms are for physical or electrical problems, or similar events of interest. This includes irregular voltages at the power supply or the insertion or removal of a module.
Switch	Switch alarms are for link up/down events on switch interfaces.
Eth	Eth alarms are for fe-cm and fe-em port related events, such as link up/down events.
WAN	WAN alarms are for T1/E1 and DDS interface related events, such as link up/down events.
Cellmodem	Cellular alarms are for cellular interface related events, such as link up/down events.

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.

The following sections describe how to configure and manage alarms:

- [Section 4.6.1, “Pre-Configured Alarms”](#)
- [Section 4.6.2, “Viewing a List of Active Alarms”](#)
- [Section 4.6.3, “Clearing and Acknowledging Alarms”](#)
- [Section 4.6.4, “Configuring an Alarm”](#)

#### Section 4.6.1

## Pre-Configured Alarms

RUGGEDCOM ROX II is equipped with a series of pre-configured alarms designed to monitor and protect the device.

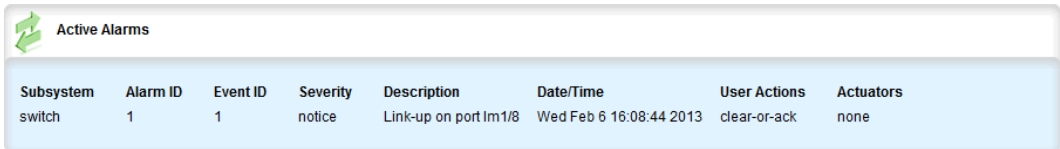
Alarm Type	Alarm	Description	Suggested Resolution
Admin	Featurekey mismatch	The featurekey does not match the serial numbers for the control module and backplane hardware.	Move the featurekey to the correct device with the matching hardware or request an updated key from Siemens Customer Support.
	Featurekey partial mismatch	The featurekey does not match the serial number for either the control module or backplane hardware.	Move the featurekey to the correct device with the matching hardware or request an updated key from Siemens Customer Support.
Chassis	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.
	PM2 bad supply	Input power to the power module is outside nominal operating range.	Make sure the input power operating range meets the device requirements.
	PM1 MOV protection bad	The Metal Oxide Varistor (MOV) protection component within the PM1 power module is damaged.	Contact Siemens Customer Support to return the power module.
	PM2 MOV protection bad	The Metal Oxide Varistor (MOV) protection component within the PM2 power module is damaged.	Contact Siemens Customer Support to return the power module.
	Real-time clock battery low	The Real-Time Clock (RTC) battery in the control module is depleted.	Contact Siemens Customer Support to return the device for repair.
	LM Watchdog Failure	The specified line module has stopped sending its heartbeat message to the control module.	Inspect the line module to make sure it is functioning properly.
	Fan-Controller Hardware Failure (For MX5000RE Only)	The fan tray is damaged. One or more fan trays may stop spinning.	Contact Siemens Customer Support to return the fan module.
	Fan-Controller Overtemp (For MX5000RE Only)	The ambient temperature within the RuggedEnclosure has exceeded the maximum operating temperature range of the device.	Power down the device until the ambient temperature has cooled.
	Module Type Mismatch	The configured module type does not match the detected module type.	Updated the chassis configuration or install the correct module type.

Alarm Type	Alarm	Description	Suggested Resolution
	Line Module Removed	The specified line module has either been removed or lost contact with the chassis.	Inspect the line module.
	Line Module Inserted	A new line module has been inserted in the specified slot.	

## Section 4.6.2

## Viewing a List of Active Alarms

To view a list of active alarms, navigate to **admin » alarms**. If any alarms are currently active, the **Active Alarms** table appears.



**Figure 180: Active Alarms Table**

For information on how to clear or acknowledge an active alarm, refer to [Section 4.6.3, “Clearing and Acknowledging Alarms”](#).

## Section 4.6.3

## 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.

The following sections describe how to acknowledge and clear alarms:

- [Section 4.6.3.1, “Clearing Alarms”](#)
- [Section 4.6.3.2, “Acknowledging Alarms”](#)

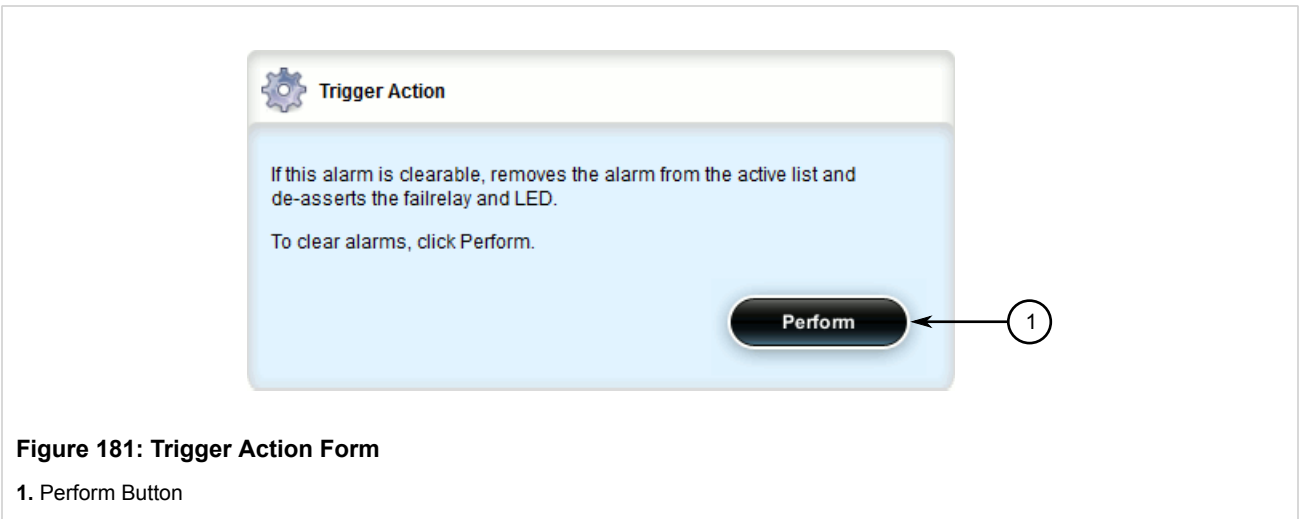
## Section 4.6.3.1

### Clearing Alarms

Non-conditional alarms must be cleared by the user. Conditional alarms, when configured, are cleared automatically.

To clear all clear-able, non-conditional alarms, do the following:

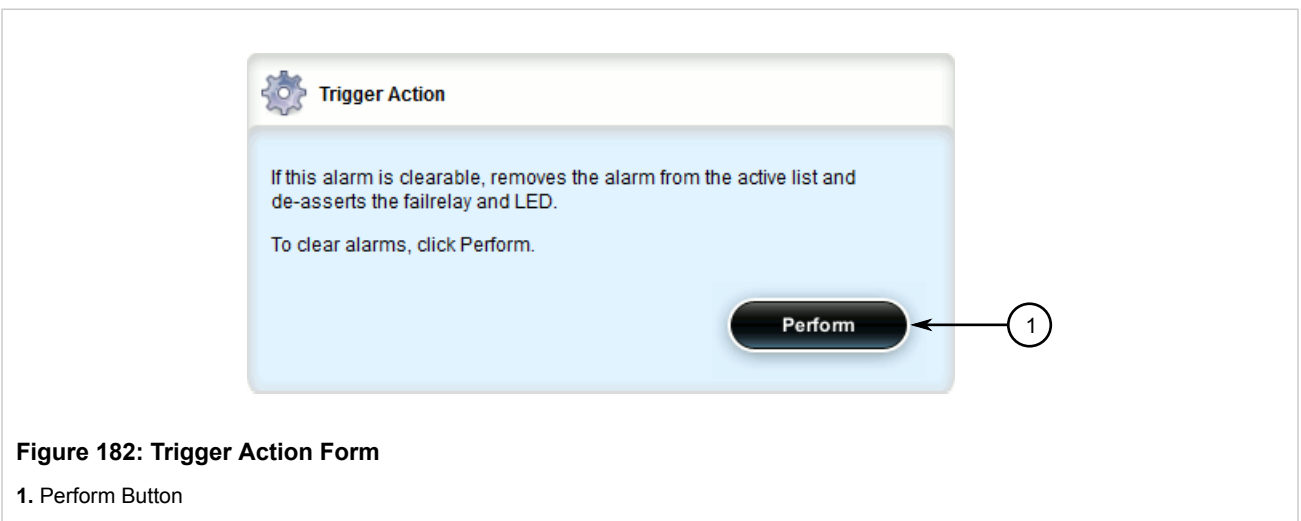
1. Navigate to **admin** and click **clear-all-alarms** in the menu. The **Trigger Action** form appears.



2. Click **Perform** to clear all clear-able alarms.

Alternatively, to clear an individual non-conditional alarm, do the following:

1. Navigate to **admin » alarms » {alarm}**, where **{alarm}** is the chosen alarm in the form of **{interface}/{alarm ID}/{alarm event}**. For example, **switch/1/1**.
2. Click **clear** in the menu. The **Trigger Action** form appears.



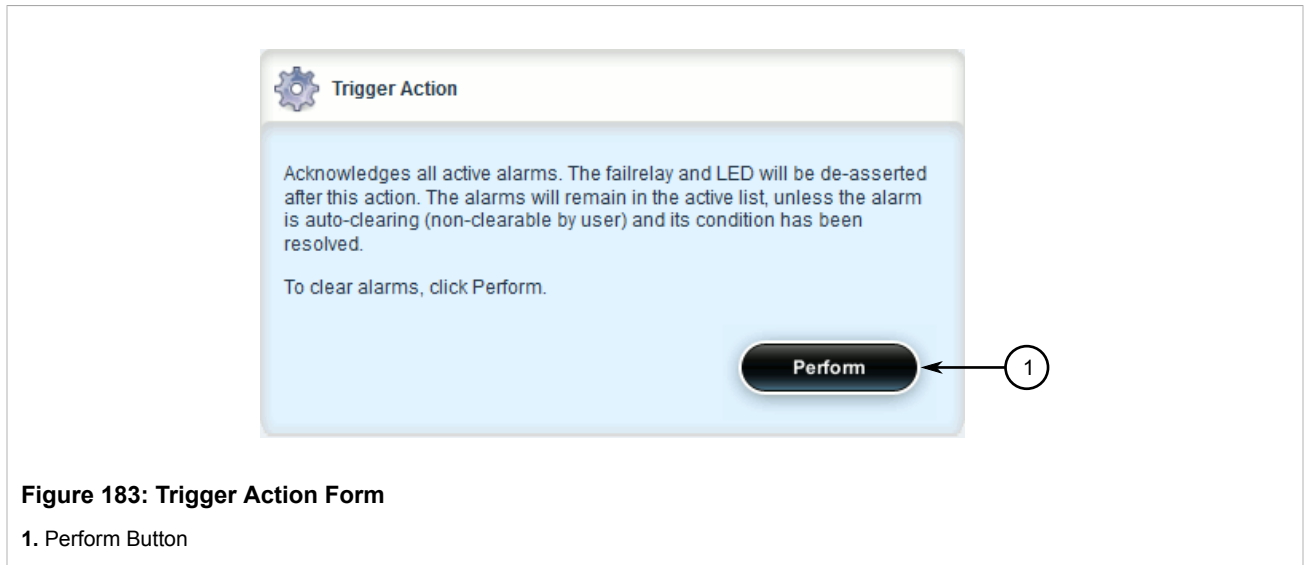
3. Click **Perform** to clear the alarm.

#### Section 4.6.3.2

### Acknowledging Alarms

To acknowledge all active alarms, do the following:

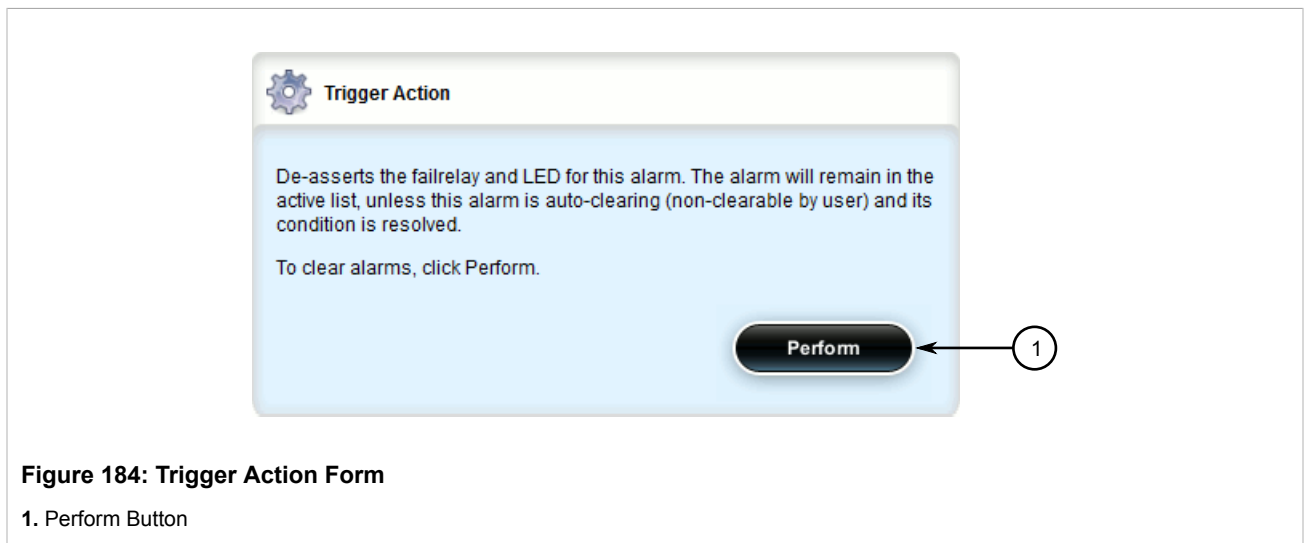
1. Navigate to **admin** and click **acknowledge-all-alarms** in the menu. The **Trigger Action** form appears.



2. Click **Perform** to acknowledge all active alarms.

Alternatively, to acknowledge an individual alarm, do the following:

1. Navigate to **admin » alarms » {alarm}**, where *{alarm}* is the chosen alarm in the form of *{interface}/{alarm ID}/{alarm event}*. For example, *switch/1/1*.
2. Click **acknowledge** in the menu. The **Trigger Action** form appears.



3. Click **Perform** to acknowledge the alarm.

#### Section 4.6.4

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » alarms » alarm-config » {type} » {alarm}**, where {type} is the type of alarm and {alarm} is the alarm ID. The **Alarm Configuration** form appears.



**NOTE**  
Depending on the alarm type, some of the parameters shown are not available.

Admin Alarm Configuration

1 → Description \* Featurekey mismatch ?

2 → Severity \* alert ?

3 → Admin-enable ☒ Enabled ?

4 → Failrelay-enable ☒ Enabled ?

5 → Led-enable ☒ Enabled ?

6 → Auto-clear ☒ Enabled ?

**Figure 185: Alarm Configuration Form**  
1. Description Box   2. Severity List   3. Admin Enable Check Box   4. Failrelay Enable Check Box   5. LED Enable Check Box  
6. Auto Clear Check Box

3. Configure the following parameters as required:

Parameter	Description
description	<b>Synopsis:</b> A string 1 to 127 characters long The name of the alarm.
severity	<b>Synopsis:</b> { emergency, alert, critical, error, warning, notice, info, debug } The severity level can be one of emergency, alert, critical, error, warning, notice, info, and debug. This cannot be changed for some alarms.
Admin Enable	<b>Synopsis:</b> typeless

Parameter	Description
	If disabled, the alarm is not reported in the active list and does not actuate LED/failrelay.
Failrelay Enable	<b>Synopsis:</b> typeless If enabled, this alarm will assert the failrelay.
LED Enable	<b>Synopsis:</b> typeless 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	<b>Synopsis:</b> typeless If enabled, the LED and failrelay will be cleared automatically when condition is met.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 4.7

## Managing Certificates and Keys

The following sections describe how to configure and manage certificates and keys on the device:

**NOTE**

*Only admin users can read/write certificates and keys on the device.*

- [Section 4.7.1, “Managing CA Certificates and CRLs”](#)
- [Section 4.7.2, “Managing Private Keys”](#)
- [Section 4.7.3, “Managing Public Keys”](#)
- [Section 4.7.4, “Managing Certificates”](#)

## Section 4.7.1

### Managing CA Certificates and CRLs

The following sections describe how to configure and manage CA certificates and their associated Certificate Revocation Lists (CRLs) on the device:

- [Section 4.7.1.1, “Viewing a List of CA Certificates and CRLs”](#)
- [Section 4.7.1.2, “Viewing the Status of a CA Certificate and CRL”](#)
- [Section 4.7.1.3, “Adding a CA Certificate and CRL”](#)
- [Section 4.7.1.4, “Deleting a CA Certificate and CRL”](#)

Section 4.7.1.1

Viewing a List of CA Certificates and CRLs

To view a list of certificates issued by a Certified Authority (CA) and the Certificate Revocation Lists (CRLs) associated with them, navigate to **security » crypto » ca**. If certificates have been configured, the **Certificate Authorities** table appears.

Certificate Authorities			
Name	Key Cert Sign Certificate	CRL Sign Certificate	CRL Contents
ca-cert	Certificate: Data: Version: ...	not found	-----BEGIN X509 CRL----- MIIBJDCBjjANBgk...

Figure 186: Certificate Authorities Table

If no certificates have been configured, add certificates as needed. For more information, refer to [Section 4.7.1.3, “Adding a CA Certificate and CRL”](#).

Section 4.7.1.2

Viewing the Status of a CA Certificate and CRL

To view the status of a CA certificate and its associated Certificate Revocation List (CRL), navigate to **security » crypto » ca » {name}**, where {name} is the name of the CA certificate. The **Key Cert Sign Certificate Status**, **CRL Sign Certificate Status** and **CRL Status** forms appear.

Key Cert Sign Certificate Status

1

Issuer

---

2

Subject

---

3

Not Before

---

?

4

Not After

---

?

Figure 187: Key Cert Sign Certificate Status Form

1. Issuer   2. Subject   3. Not Before   4. Not After

**CRL Sign Certificate Status**

1 → Issuer  
---

2 → Subject  
---

3 → Not Before  
--- ?

4 → Not After  
--- ?

**Figure 188: CRL Sign Certificate Status Form**

1. Issuer 2. Subject 3. Not Before 4. Not After

**CRL Status**

1 → Issuer  
---

2 → This Update  
--- ?

3 → Next Update  
--- ?

**Figure 189: CRL Status Form**

1. Issuer 2. This Update 3. Next Update

The **Key Cert Sign Certificate Status** form provides the following information:

Parameter	Description
issuer	<b>Synopsis:</b> A string
subject	<b>Synopsis:</b> A string
Not Before	<b>Synopsis:</b> A string This certificate is not valid before this date.
Not After	<b>Synopsis:</b> A string This certificate is not valid after this date.

The **CRL Sign Certificate Status** form provides the following information:

Parameter	Description
issuer	<b>Synopsis:</b> A string

Parameter	Description
subject	<b>Synopsis:</b> A string
Not Before	<b>Synopsis:</b> A string This certificate is not valid before this date.
Not After	<b>Synopsis:</b> A string This certificate is not valid after this date.

The **CRL Status** form provides the following information:

Parameter	Description
issuer	<b>Synopsis:</b> A string
This Update	<b>Synopsis:</b> A string This CRL was updated at this date and time.
Next Update	<b>Synopsis:</b> A string This certificate must be updated by this date and time.

#### Section 4.7.1.3

### Adding a CA Certificate and CRL

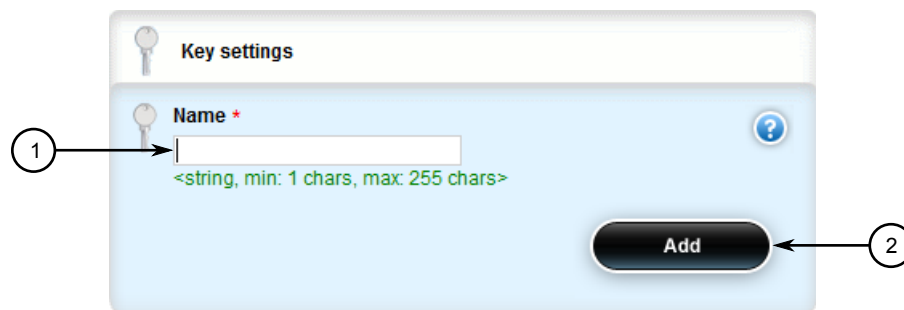
To add a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:



#### NOTE

Only admin users can read/write certificates and keys on the device.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » crypto » ca** and click **<Add ca>**. The **Key Settings** form appears.



**Figure 190: Key Settings Form**

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 255 characters long The name of the CA certificate.

- Click **Add**. The **CA** form appears.

**Figure 191: CA Form**

1. Key Cert Sign Certificate Box    2. CRL Sign Certificate Box    3. CRL Contents Box

- Copy the contents of the CA certificate into the **Key Cert Sign Certificate** box.



**NOTE**

*Large CRLs (bigger than 100KB) are not currently supported and may be difficult to add/view in the configuration.*

- Add the associated Certificate Revocation List (CRL).
  - If the CRL is signed by a separate certificate, copy the contents of the CRL into the **CRL Sign Certificate** box
  - If the CRL is not signed, copy the contents of the CRL into the **CRL Contents** box
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

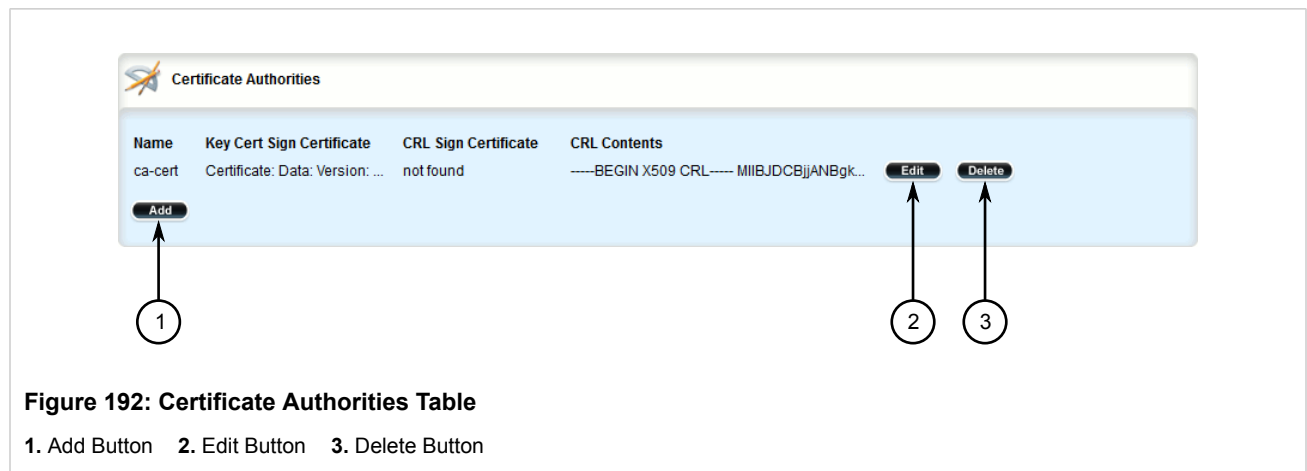
8. Click **Exit Transaction** or continue making changes.

#### Section 4.7.1.4

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » crypto » ca**. The **Certificate Authorities** table appears.



3. Click **Delete** next to the chosen certificate.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 4.7.2

### Managing Private Keys

The following sections describe how to configure and manage unsigned private keys on the device:



#### NOTE

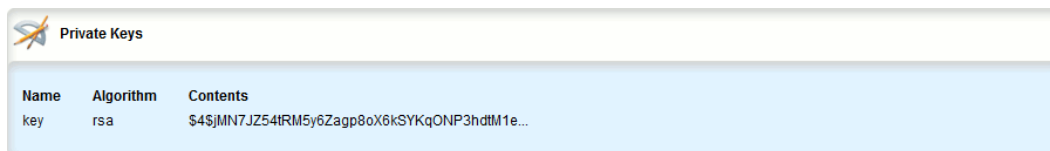
*Private keys are automatically encrypted using an AES-CFB-128 cipher to protect them from being viewed by unauthorized users.*

- [Section 4.7.2.1, “Viewing a List of Private Keys”](#)
- [Section 4.7.2.2, “Adding a Private Key”](#)
- [Section 4.7.2.3, “Deleting a Private Key”](#)

### Section 4.7.2.1

## Viewing a List of Private Keys

To view a list of unsigned private keys, navigate to **security » crypto » private-key**. If private keys have been configured, the **Private Key** table appears.



Name	Algorithm	Contents
key	rsa	\$4\$JMN7JZ54tRM5y6Zagp8oX6kSYKqONP3hdtM1e...

**Figure 193: Private Key Table**

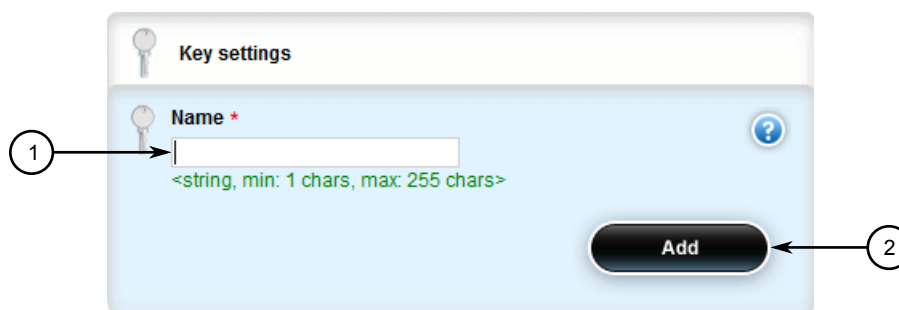
If no private keys have been configured, add keys as needed. For more information, refer to [Section 4.7.2.2, “Adding a Private Key”](#).

### Section 4.7.2.2

## Adding a Private Key

To add an unsigned private key, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » crypto » private-key** and click **<Add private-key>**. The **Key Settings** form appears.



**Figure 194: Key Settings Form**

1. Name Box    2. Add Button

3. In the **Key Settings** form, configure the following parameters as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 255 characters long The name of the key.

4. Click **Add** to create the new private key. The **Private Key** form appears.



**Figure 195: Private Key Form**

1. Algorithm List   2. Contents Box

5. In the **Private Key** form, configure the following parameters as required:

Parameter	Description
algorithm	<b>Synopsis:</b> { rsa, dsa } The type of key.
Contents	<b>Synopsis:</b> A string The contents of the unsigned private key.

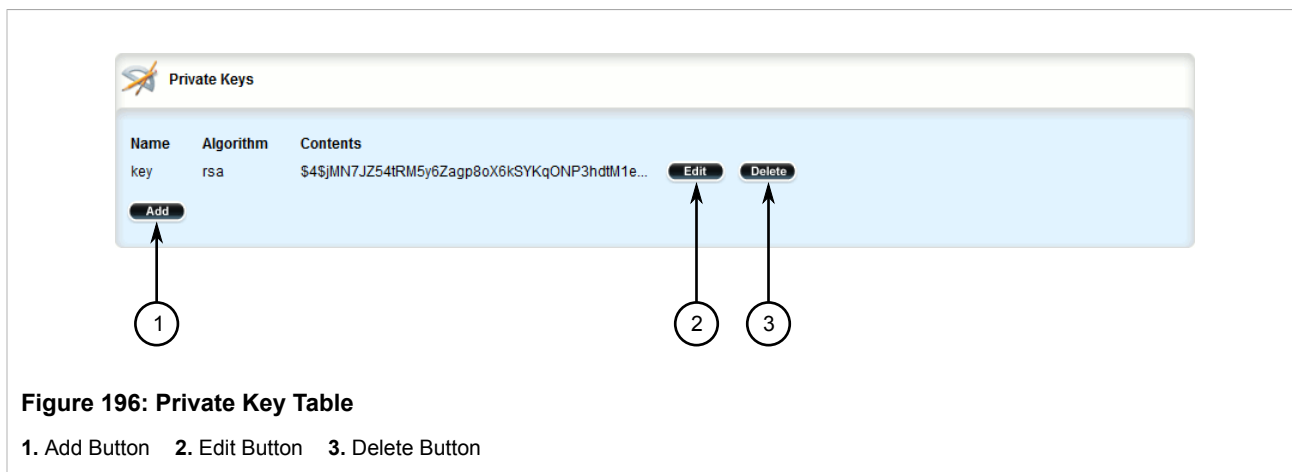
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 4.7.2.3

### Deleting a Private Key

To delete an unsigned private key, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » crpto » private-key**. The **Private Key** table appears.



**Figure 196: Private Key Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen private key.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 4.7.3

## Managing Public Keys

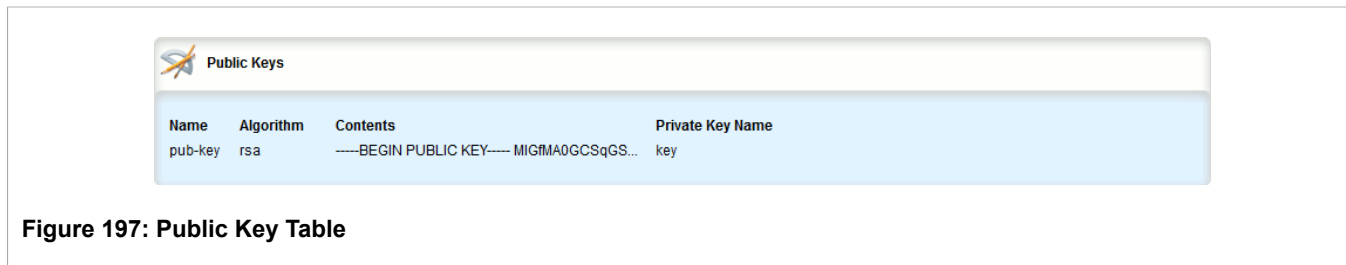
The following sections describe how to configure and manage unsigned public keys on the device:

- [Section 4.7.3.1, “Viewing a List of Public Keys”](#)
- [Section 4.7.3.2, “Adding a Public Key”](#)
- [Section 4.7.3.3, “Adding an IPSec-Formatted Public Key”](#)
- [Section 4.7.3.4, “Deleting a Public Key”](#)

#### Section 4.7.3.1

### Viewing a List of Public Keys

To view a list of unsigned public keys, navigate to **security » crypto » public-key**. If public keys have been configured, the **Public Key** table appears.



**Figure 197: Public Key Table**

If no public keys have been configured, add keys as needed. For more information, refer to [Section 4.7.3.2, “Adding a Public Key”](#).

### Section 4.7.3.2

## Adding a Public Key

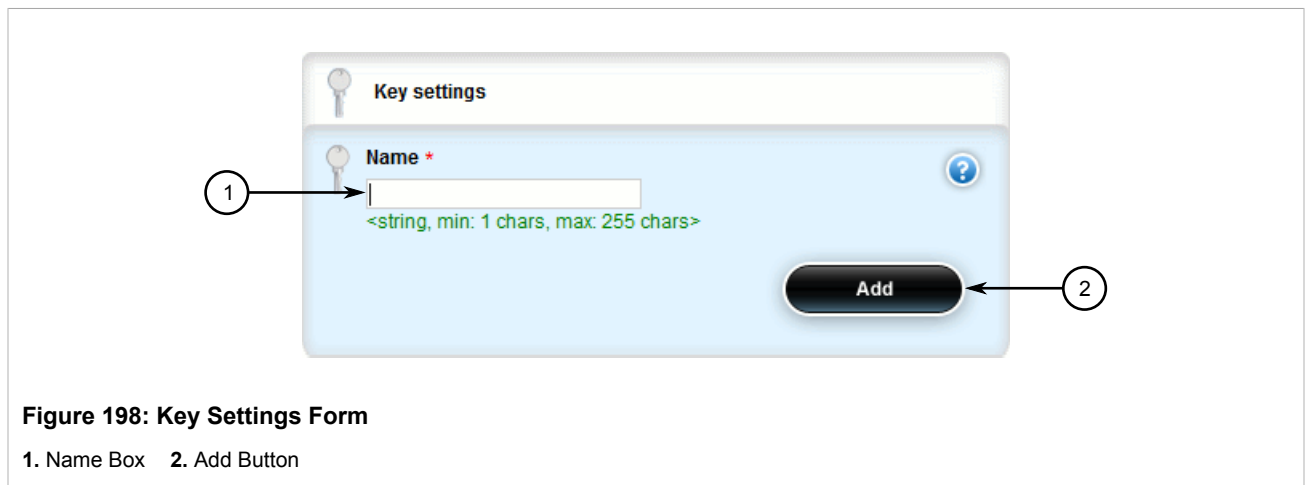
To add an unsigned public key, do the following:



#### NOTE

*Do not associate the public key with the private key if the public key belongs to another device.*

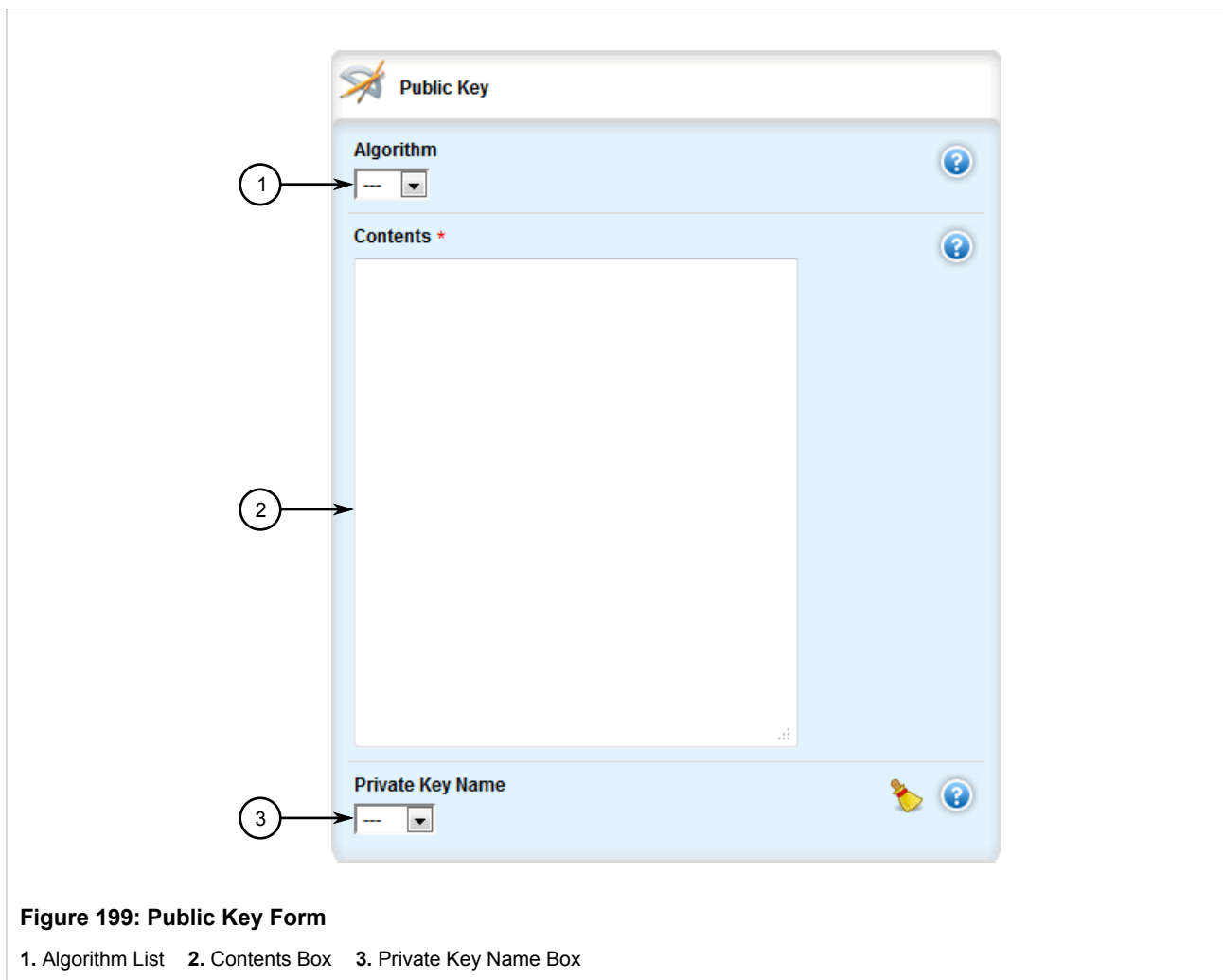
1. Make sure the private key associated with the public key has been added. For more information, refer to [Section 4.7.2.2, “Adding a Private Key”](#).
2. Change the mode to **Edit Public** or **Edit Exclusive**.
3. Navigate to **security » crypto » public-key** and click **<Add public-key>**. The **Key Settings** form appears.



4. In the **Key Settings** form, configure the following parameters as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 255 characters long The name of the key.

5. Click **Add** to create the new public key. The **Public Key** form appears.



6. In the **Public Key** form, configure the following parameters as required:



**NOTE**

*For added security, consider adding an IPSec-formatted public key. For more information, refer to [Section 4.7.3.3, “Adding an IPSec-Formatted Public Key”](#).*

Parameter	Description
algorithm	<b>Synopsis:</b> { rsa, dsa } The algorithm of the key.
Contents	<b>Synopsis:</b> A string 1 to 8192 characters long The contents of the key.
Private Key Name	The private key name associated with this public key.

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

## Section 4.7.3.3

## Adding an IPSec-Formatted Public Key

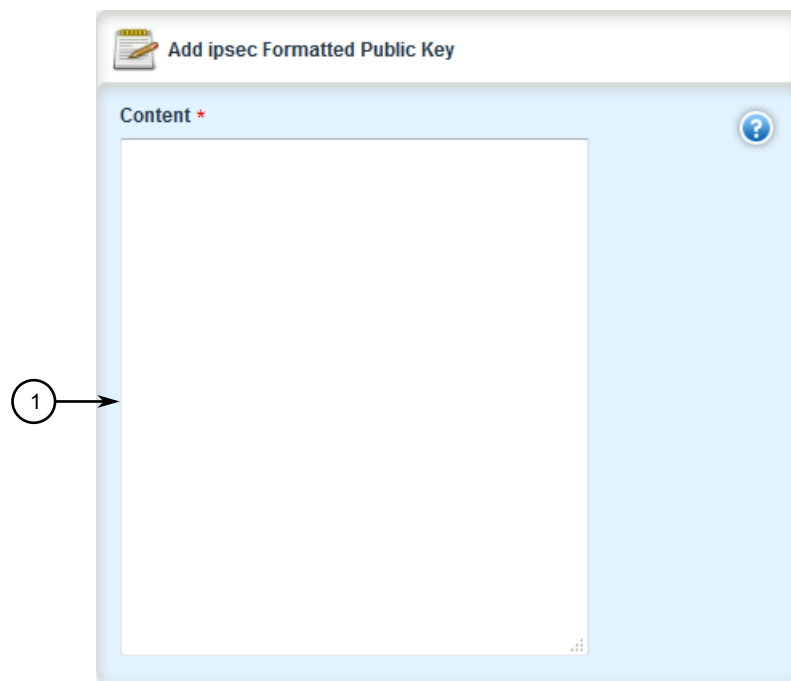
IPSec-formatted public keys from systems that do not support the Privacy-Enhanced Mail (PEM) format, such as RUGGEDCOM ROX devices, can be imported into RUGGEDCOM ROX II and automatically converted.

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 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.

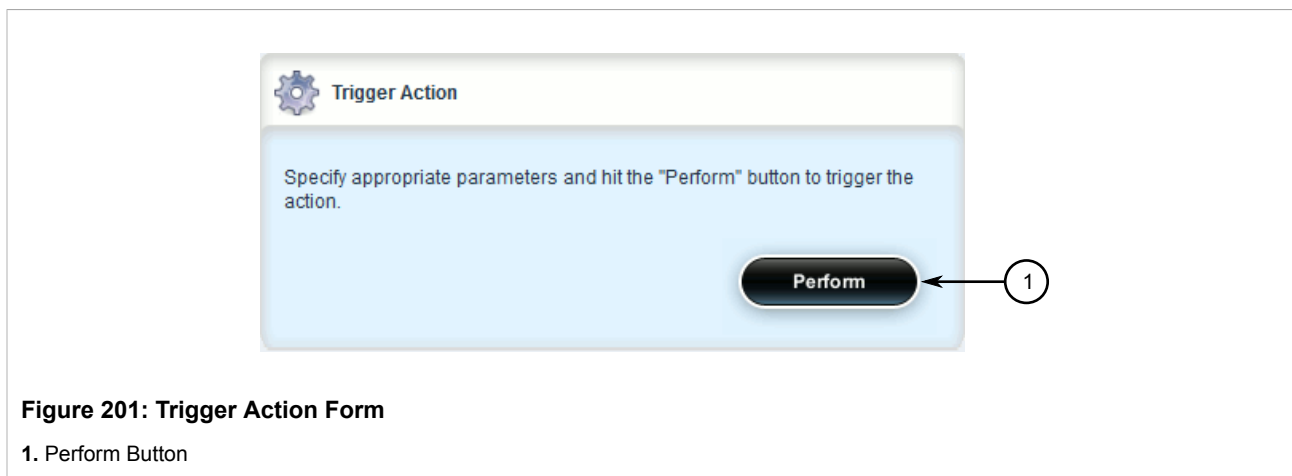
To add an IPSec-formatted public key and have it converted into PEM format, do the following:

1. Change the mode to **Edit Public** or **Edit Exclusive**.
2. Navigate to *security » crypto » public-key* and either select a public key. If the desired key is not available, add it. For more information about adding a public key, refer to [Section 4.7.3.2, “Adding a Public Key”](#).
3. Click **add-ipsec-formatted-public-key** in the menu. The **Add IPSec-Formatted Public Key** and **Trigger Action** forms appear:



**Figure 200: Add IPSec-Formatted Public Key Form**

1. Content Box



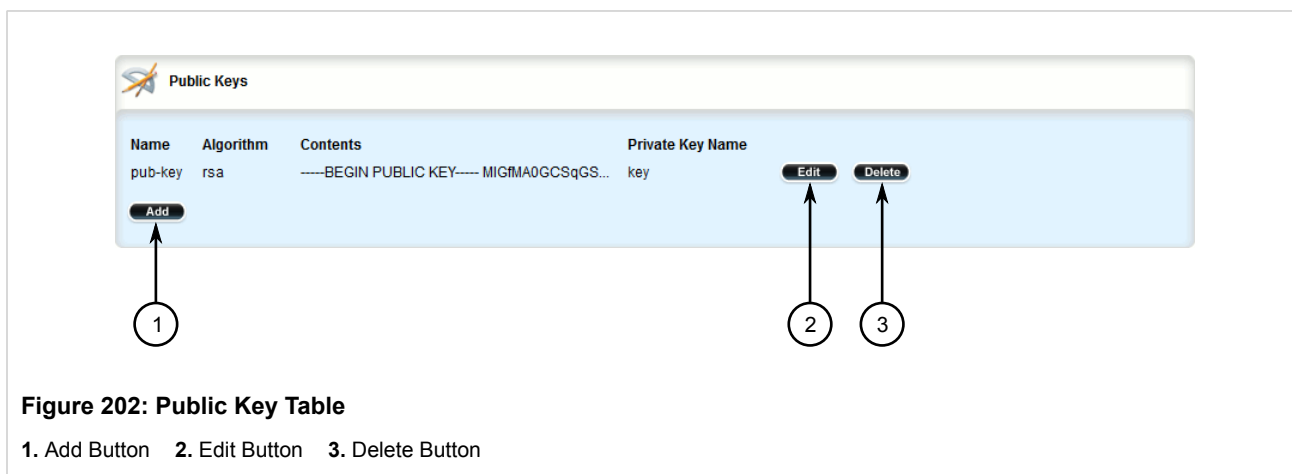
4. In the **Add IPSec-Formatted Public Key** form, in the **Content** box, enter the contents of the public key.
5. Click **Perform** to convert the public key to PEM format and add it to RUGGEDCOM ROX II.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 4.7.3.4

### Deleting a Public Key

To delete an unsigned public key, do the following:

1. Change the mode to **Edit Public** or **Edit Exclusive**.
2. Navigate to **security » crpto » public-key**. The **Public Key** table appears.



3. Click **Delete** next to the chosen public key.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 4.7.4

# Managing Certificates

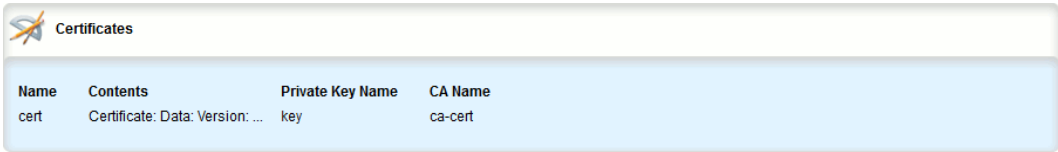
The following sections describe how to configure and manage certificates on the device:

- [Section 4.7.4.1, “Viewing a List of Certificates”](#)
- [Section 4.7.4.2, “Viewing the Status of a Certificate”](#)
- [Section 4.7.4.3, “Adding a Certificate”](#)
- [Section 4.7.4.4, “Deleting a Certificate”](#)

Section 4.7.4.1

## Viewing a List of Certificates

To view a list of certificates, navigate to **security » crypto » certificate**. If certificates have been configured, the **Certificates** table appears.



The screenshot shows a web interface titled "Certificates" with a table containing one row of certificate data.

Name	Contents	Private Key Name	CA Name
cert	Certificate: Data: Version: ...	key	ca-cert

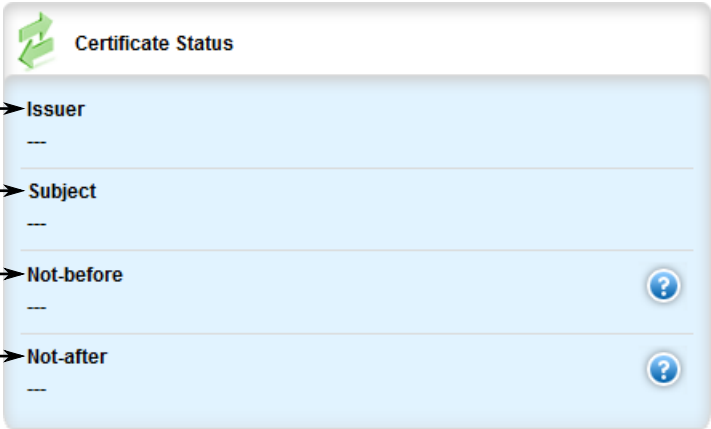
Figure 203: Certificates Table

If no certificates have been configured, add certificates as needed. For more information, refer to [Section 4.7.4.3, “Adding a Certificate”](#).

Section 4.7.4.2

## Viewing the Status of a Certificate

To view the status of a certificate, navigate to **security » crypto » certificate » {name}**, where {name} is the name of the certificate. The **Certificate Status** form appears.

The image shows a 'Certificate Status' form with a green double-checkmark icon at the top left. The form has four input fields, each with a label and a placeholder '---'. The labels are 'Issuer', 'Subject', 'Not-before', and 'Not-after'. To the left of the form, four numbered circles (1, 2, 3, 4) have arrows pointing to their respective labels. To the right of the 'Not-before' and 'Not-after' fields, there are blue circular icons with a white question mark.

1 Issuer  
---  
2 Subject  
---  
3 Not-before  
---  
4 Not-after  
---

**Figure 204: Certificate Status Form**

1. Issuer   2. Subject   3. Not Before   4. Not After

This table provides the following information:

Parameter	Description
issuer	<b>Synopsis:</b> A string
subject	<b>Synopsis:</b> A string
Not Before	<b>Synopsis:</b> A string This certificate is not valid before this date.
Not After	<b>Synopsis:</b> A string This certificate is not valid after this date.

Section 4.7.4.3

## 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, public keys and/or private keys have been added to the device.
  - For more information about adding CA Certificates, refer to [Section 4.7.1.3, “Adding a CA Certificate and CRL”](#)
  - For more information about adding public keys, refer to [Section 4.7.3.2, “Adding a Public Key”](#)
  - For more information about adding private keys, refer to [Section 4.7.2.2, “Adding a Private Key”](#)
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to **security » crypto » certificate** and click **<Add certificate>**. The **Key Settings** form appears.



A screenshot of the 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a light blue panel. Inside this panel, there is a label 'Name \*' with a key icon to its left and a question mark icon to its right. Below the label is a text input field. Underneath the input field, the text '<string, min: 1 chars, max: 255 chars>' is displayed in green. At the bottom right of the light blue panel is a dark blue button labeled 'Add'. A circled number '1' with an arrow points to the text input field. A circled number '2' with an arrow points to the 'Add' button.

**Figure 205: Key Settings Form**

1. Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 255 characters long The name of the certificate.

5. Click **Add**. The **Certificate** form appears.

A screenshot of the 'Certificate' form. It has a title bar with a key icon and the text 'Certificate'. Below the title bar is a light blue panel. Inside this panel, there is a label 'Contents \*' with a question mark icon to its right. Below the label is a large text area. Below the text area are two dropdown menus. The first dropdown menu is labeled 'Private Key Name' and has a question mark icon to its right. The second dropdown menu is labeled 'CA Name' and has a question mark icon to its right. A circled number '1' with an arrow points to the text area. A circled number '2' with an arrow points to the 'Private Key Name' dropdown menu. A circled number '3' with an arrow points to the 'CA Name' dropdown menu.

**Figure 206: Certificate Form**

1. Contents Box    2. Private Key Name List    3. CA Certificate Name List

6. Configure the following parameter(s) as required:

Parameter	Description
Contents	<b>Synopsis:</b> A string 1 to 8192 characters long The contents of the certificate.
Private Key Name	The private key associated with this certificate.
CA Name	The optional CA certificate for this certificate.

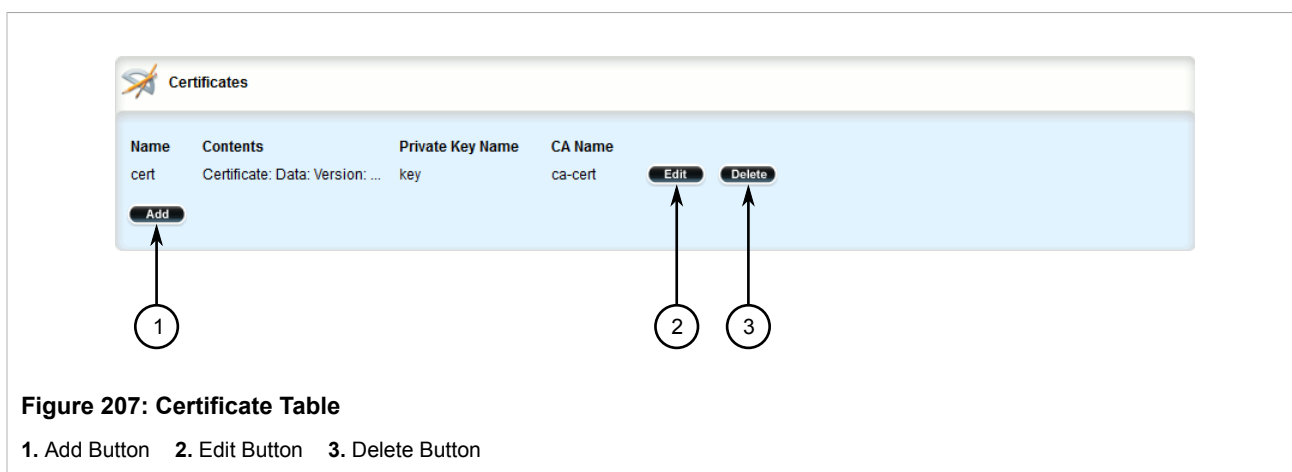
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 4.7.4.4

### Deleting a Certificate

To delete a certificate, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » crypto » certificate**. The **Certificate** table appears.



- Click **Delete** next to the chosen certificate.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 4.8

## Managing RADIUS Authentication

RADIUS is a UDP-based protocol used for carrying authentication, authorization and configuration information between a Network Access Server (NAS) that desires to authenticate its links and a shared authentication server. It provides centralized authentication and authorization for network access.

RADIUS is also widely used in conjunction with the IEEE 802.1x standard for port security using the Extensible Authentication Protocol (EAP).

**NOTE**

For more information about the RADIUS protocol, refer to [RFC 2865](http://tools.ietf.org/html/rfc2865) [<http://tools.ietf.org/html/rfc2865>].

For more information about the Extensible Authentication Protocol (EAP), refer to [RFC 3748](http://tools.ietf.org/html/rfc3748) [<http://tools.ietf.org/html/rfc3748>].

**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 4.4, “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 802.1X security support. When this is required, the following attributes are sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ The username as derived from the client's EAP identity response }
NAS-IP-Address	{ The Network Access Server IP address }
Service-Type	2
Frame-MTU	1500
EAP-Message <sup>a</sup>	{ A message(s) received from the authenticating peer }

<sup>a</sup> EAP-Message is an extension attribute for RADIUS, as defined by [RFC 2869](#).

Primary and secondary RADIUS servers, typically operating from a common database, can be configured for redundancy. If the first server does not respond to an authentication request, the request will be forwarded to the second server until a positive/negative acknowledgment is received.

**NOTE**

RADIUS authentication activity is logged to the authentication log file `var/log/auth.log`. Details of each authentication including the time of occurrence, source and result are included. For more information about the authentication log file, refer to [Section 3.9.1, “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.

The following sections describe how to configure and manage RADIUS authentication:

- [Section 4.8.1, “Configuring RADIUS Authentication for LOGIN Services”](#)
- [Section 4.8.2, “Configuring RADIUS Authentication for PPP Services”](#)
- [Section 4.8.3, “Configuring RADIUS Authentication for Switched Ethernet Ports”](#)

#### Section 4.8.1

## Configuring RADIUS Authentication for LOGIN Services

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



### IMPORTANT!

*Passwords are case-sensitive.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » authentication » radius**. The **Primary Radius Server** and **Secondary Radius Server** forms appear.

The image shows a web form titled "Primary Radius Server". It contains three main input fields, each with a callout number: 1. "Address" field with a callout "1" pointing to it. 2. "Port-udp" field with a callout "2" pointing to it. 3. "Password" field with a callout "3" pointing to it. Each field has a help icon (question mark in a circle) to its right. The "Address" field contains a placeholder icon and "--". The "Port-udp" field contains "1812" and "(1812)". The "Password" field is empty.

Figure 208: Primary Radius Server Form

1. Address Box    2. Port UDP Box    3. Password Box

The image shows a web form titled "Secondary Radius Server". It contains three main input fields, each with a callout number: 1. "Address" field with a callout "1" pointing to it. 2. "Port-udp" field with a callout "2" pointing to it. 3. "Password" field with a callout "3" pointing to it. Each field has a help icon (question mark in a circle) to its right. The "Address" field contains a placeholder icon and "--". The "Port-udp" field contains "1812" and "(1812)". The "Password" field is empty.

Figure 209: Secondary Radius Server Form

1. Address Box    2. Port UDP Box    3. Password Box

3. In both forms, configure the following parameters as required:

Parameter	Description
address	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the server.

Parameter	Description
port-udp	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812 The network port of the server.
password	<b>Synopsis:</b> A string The password of the RADIUS server.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 4.8.2

## Configuring RADIUS Authentication for PPP Services

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



### IMPORTANT!

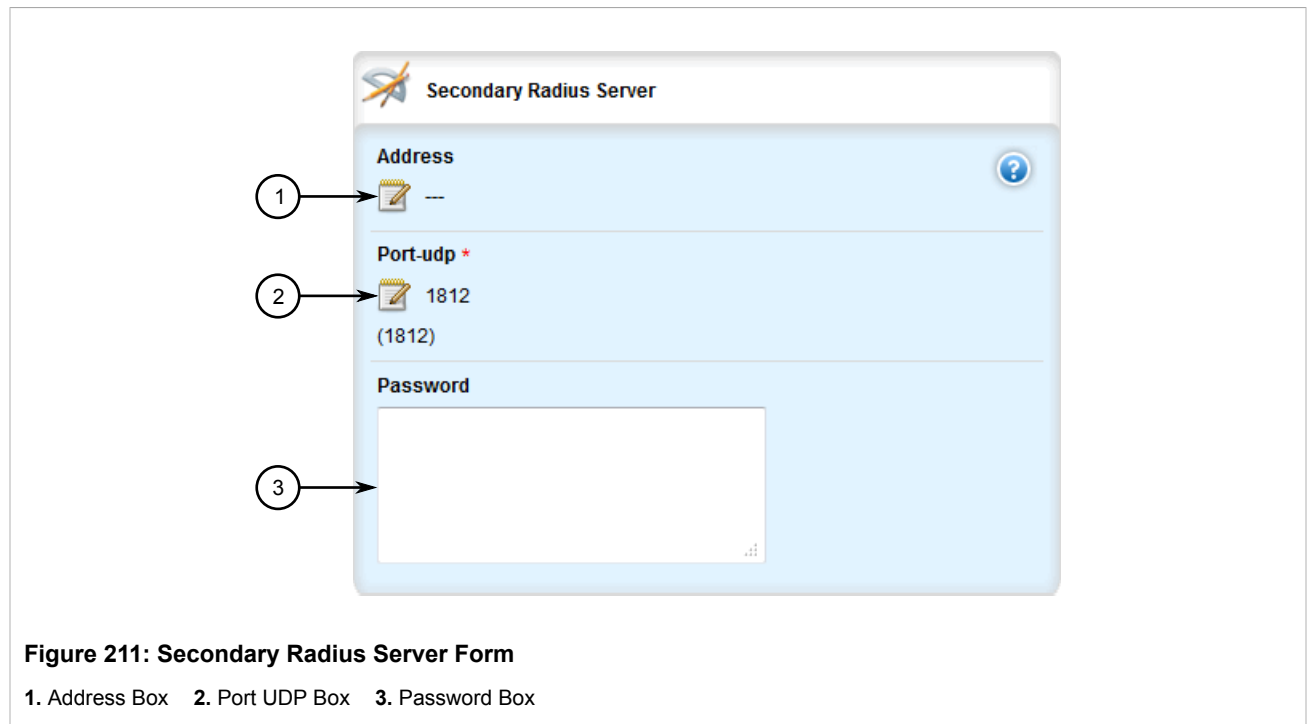
*Passwords are case-sensitive.*

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **global » ppp » radius**. The **Primary Radius Server** and **Secondary Radius Server** forms appear.

The screenshot shows the 'Primary Radius Server' configuration window. It contains three input fields: 'Address' (empty), 'Port-udp' (set to 1812), and 'Password' (empty). Numbered arrows point to each field: 1 to Address, 2 to Port-udp, and 3 to Password.

**Figure 210: Primary Radius Server Form**

1. Address Box    2. Port UDP Box    3. Password Box



3. In both forms, configure the following parameters as required:

Parameter	Description
address	<b>Synopsis:</b> A string 7 to 15 characters long The IPv4 address of the server.
UDP Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812
password	<b>Synopsis:</b> A string

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 4.8.3

## Configuring RADIUS Authentication for Switched Ethernet Ports

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



### IMPORTANT!

*Passwords are case-sensitive.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **switch » port-security » radius**. The **Primary Radius Server** and **Secondary Radius Server** forms appear.

**Primary Radius Server**

**Address** ?

1 →

**Port-udp \***

2 →   
(1812)

**Password**

3 →

**Figure 212: Primary Radius Server Form**

1. Address Box   2. Port UDP Box   3. Password Box

**Secondary Radius Server**

**Address** ?

1 →

**Port-udp \***

2 →   
(1812)

**Password**

3 →

**Figure 213: Secondary Radius Server Form**

1. Address Box   2. Port UDP Box   3. Password Box

3. In both forms, configure the following parameters as required:

Parameter	Description
address	<b>Synopsis:</b> A string 7 to 15 characters long



Parameter	Description
	The IPv4 address of the server.
UDP Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1812 The IPv4 port of the server.
password	<b>Synopsis:</b> A string The password of the server

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 4.9

## 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 4.10.2, “Setting a User Password/Passphrase”](#).*

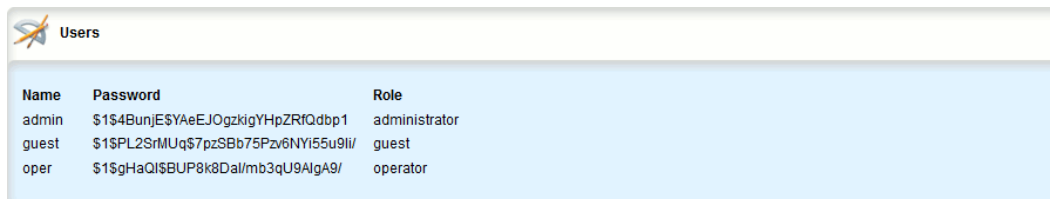
The following sections describe how to configure and manage users:

- [Section 4.9.1, “Viewing a List of Users”](#)
- [Section 4.9.2, “Adding a User”](#)
- [Section 4.9.3, “Deleting a User”](#)
- [Section 4.9.4, “Monitoring Users”](#)

### Section 4.9.1

## Viewing a List of Users

To view a list of user accounts, navigate to **admin » users**. If user accounts have been configured, the **Users** table appears.



Name	Password	Role
admin	\$1\$4BunjESYAeEJOgzkigYHpZRfQdbp1	administrator
guest	\$1\$PL2SrfMUq\$7pzSBb75Pzv6NYI55u9li/	guest
oper	\$1\$gHaQl\$BUP8k8Dal/mb3qU9AlgA9/	operator

**Figure 214: Users Table**

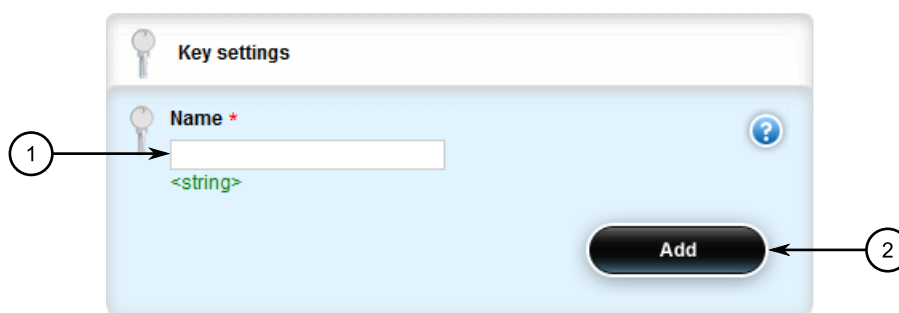
If no user accounts have been configured, add user accounts as needed. For more information, refer to [Section 4.9.2, “Adding a User”](#).

### Section 4.9.2

## Adding a User

To add a new user account, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » users** and click **<Add userid>** in the menu. The **Key Settings** form appears.



**Figure 215: Key Settings Form**

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 128 characters long The name of the user.

4. Click **Add** to create the new user account. The **Users** form appears.

**Figure 216: Users Form**

1. Password Box   2. Role List

5. Under **Role**, select the user's role (i.e. administrator, operator or guest).



**NOTE**

The **Password** box displays a hashed version of the user's current password/passphrase. If a password/passphrase is not configured, the box is blank. Setting the user password/passphrase is done elsewhere in RUGGEDCOM ROX II.

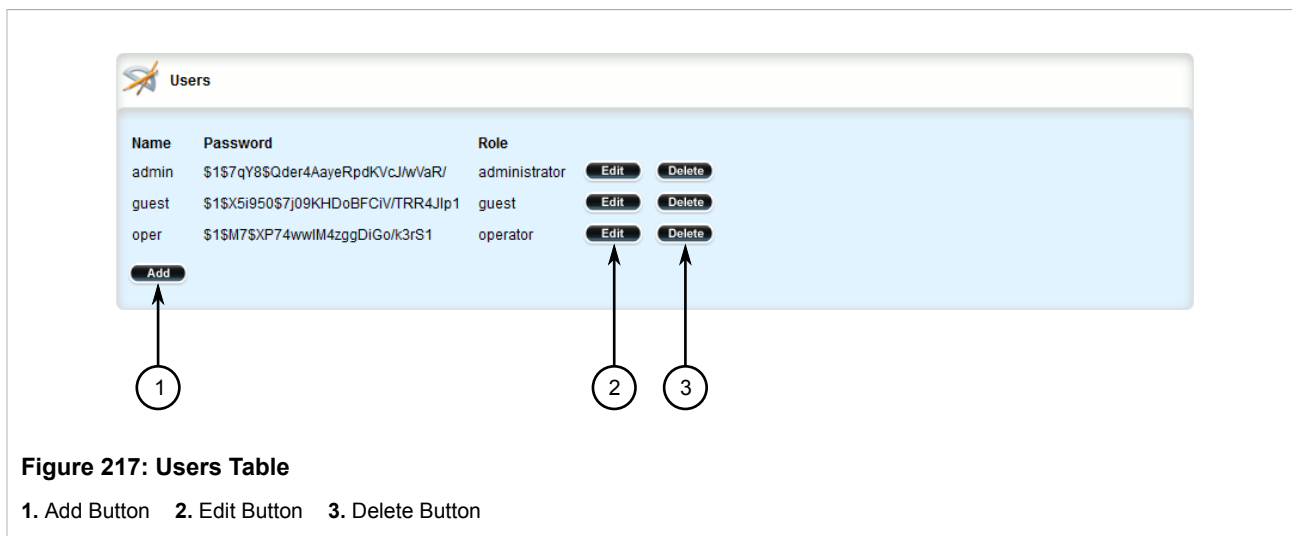
6. Set the user's password. For more information, refer to [Section 4.10.2, "Setting a User Password/Passphrase"](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 4.9.3

## Deleting a User

To delete a user account, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » users**. The **Users** table appears.



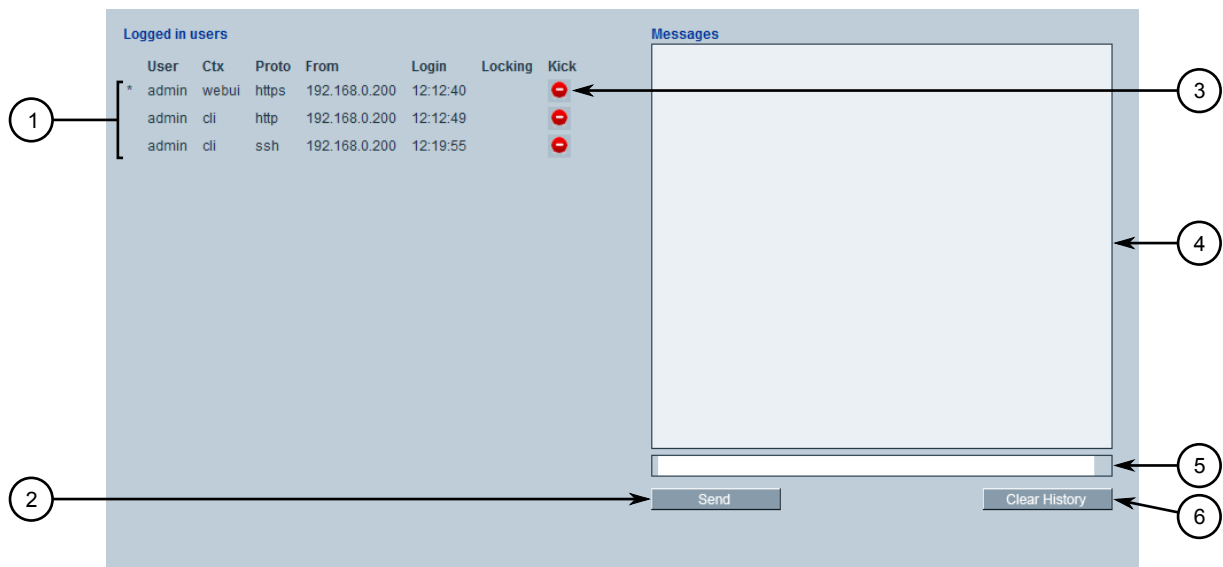
3. Click **Delete** next to the chosen user account.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 4.9.4

## Monitoring Users

Users currently logged in to the device are monitored by RUGGEDCOM ROX II and can be viewed on the **Users** screen. RUGGEDCOM ROX II allows administrators to monitor users, log users out, and broadcast message to all users.

To view a list of users currently logged in to the device, select the **Tools** menu and click **Users**. The **Users** screen appears.



**Figure 218: Users Screen**

1. List of Users   2. Send Button   3. Kick Icon   4. Messages Window   5. Message Box   6. Clear History Button

The following sections describe other actions that can be used to manage users logged in to the device:

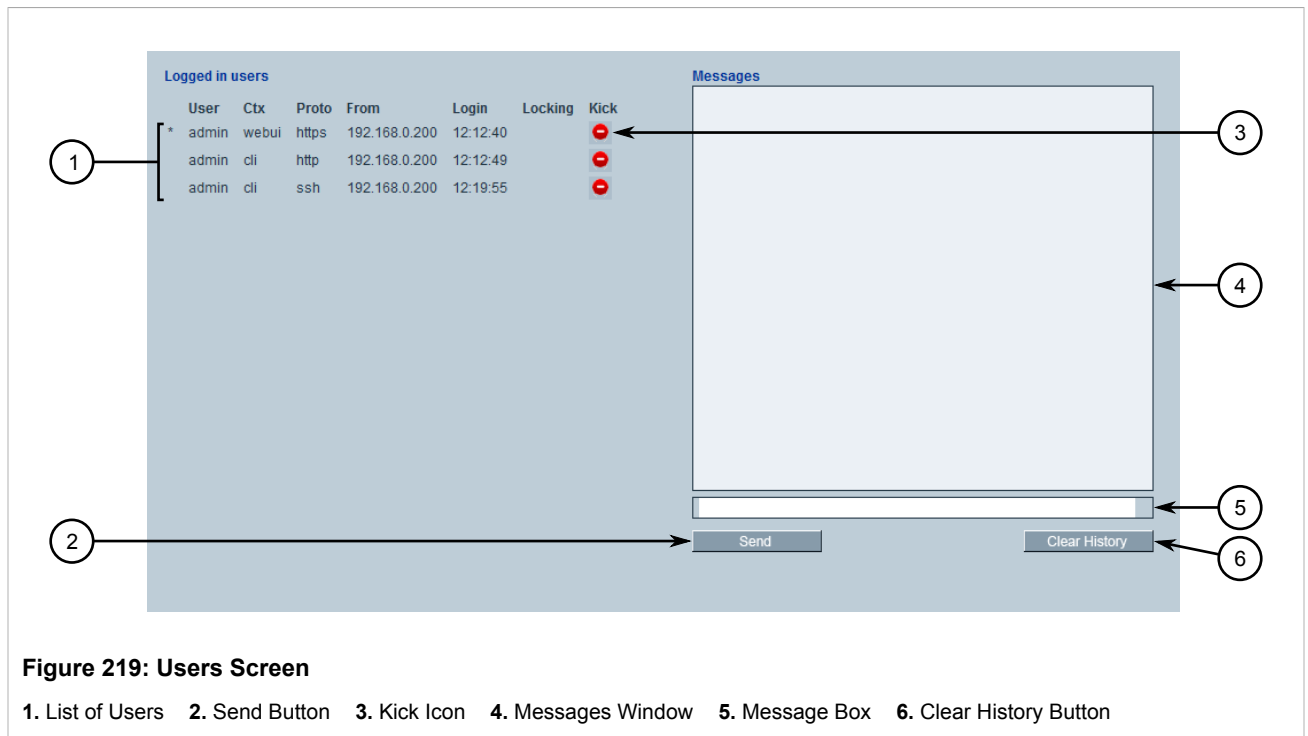
- [Section 4.9.4.1, “Kicking Users from the Network”](#)
- [Section 4.9.4.2, “Sending Messages to Users”](#)

#### Section 4.9.4.1

### Kicking Users from the Network

To log a user out of the device, do the following:

1. Select the **Tools** menu and click **Users**. The **Users** screen appears.



2. Click the **Kick** icon next to the user profile.

#### Section 4.9.4.2

### Sending Messages to Users

To broadcast a message to all users or a specific user, do the following:

1. Select the **Tools** menu and click **Users**. The **Users** screen appears.

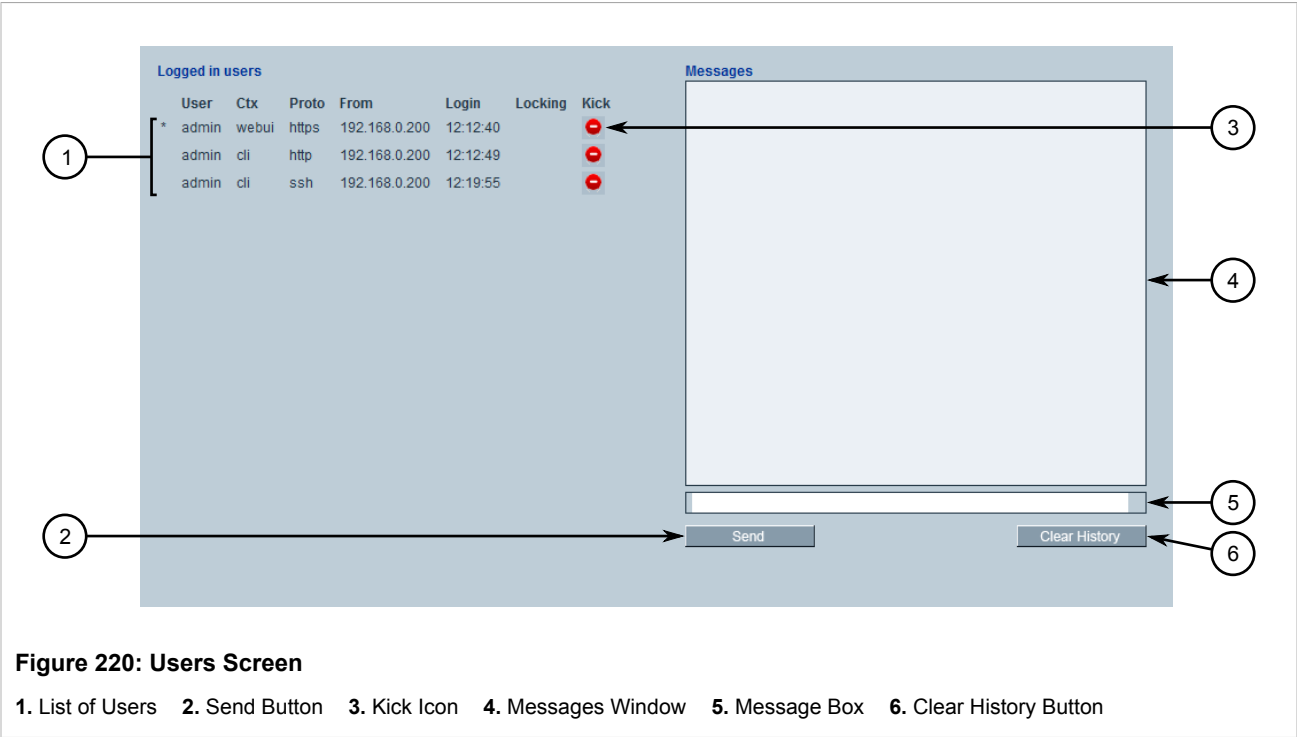


Figure 220: Users Screen

1. List of Users   2. Send Button   3. Kick Icon   4. Messages Window   5. Message Box   6. Clear History Button

2. Type a message in the **Message** box and click **Send**.

Section 4.10

# 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.

For a list of default passwords, refer to [Section 2.2, “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.

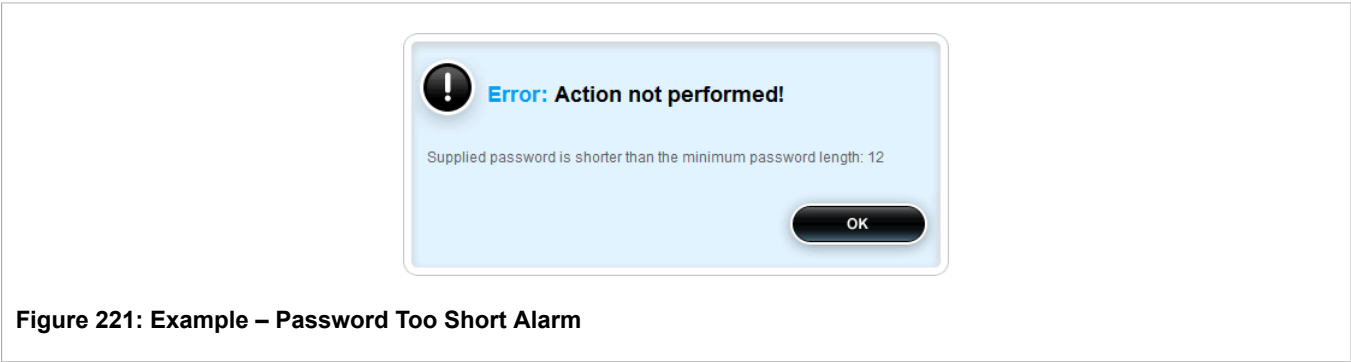


Figure 221: Example – Password Too Short Alarm



#### NOTE

User authentication can also be verified through a RADIUS server. When enabled for authentication and authorization, the RADIUS server will be used in the absence of any local settings. For more information about configuring a RADIUS server, refer to [Section 4.8, “Managing RADIUS 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.

The following sections describe how to configure and manage passwords and passphrases:

- [Section 4.10.1, “Configuring Password/Passphrase Complexity Rules”](#)
- [Section 4.10.2, “Setting a User Password/Passphrase”](#)
- [Section 4.10.3, “Setting the Boot Password/Passphrase”](#)
- [Section 4.10.4, “Setting the Maintenance Password/Passphrase”](#)
- [Section 4.10.5, “Resetting Passwords and Passphrases”](#)

#### Section 4.10.1

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » authentication**. The **Password Complexity** form appears.



**Password Complexity**

1. Minimum Length \* 12 (12)

2. Maximum Length \* 128 (128)

3. Uppercase Characters Required \* Enabled (true)

4. Lowercase Characters Required \* Enabled (true)

5. Digits Required \* Enabled (true)

6. Special Characters Required \* Enabled (true)

**Figure 222: Password Complexity Form**

1. Minimum Length Box   2. Maximum Length Box   3. Uppercase Characters Required Check Box   4. Lowercase Characters Required Check Box   5. Digits Required Check Box   6. Special Characters Required Check Box

3. Configure the following parameter(s):

Parameter	Description
Minimum Length	<b>Synopsis:</b> An integer between 1 and 128 <b>Default:</b> 12 Minimum password length.
Maximum Length	<b>Synopsis:</b> An integer between 1 and 128 <b>Default:</b> 128 Maximum password length.
Uppercase Characters Required	<b>Synopsis:</b> true or false <b>Default:</b> true Requires the password to have at least one uppercase letter.
Lowercase Characters Required	<b>Synopsis:</b> true or false <b>Default:</b> true Requires the password to have at least one lowercase letter.
Digits Required	<b>Synopsis:</b> true or false <b>Default:</b> true

Parameter	Description
	Requires the password to have at least one numerical digit.
Special Characters Required	<b>Synopsis:</b> true or false <b>Default:</b> true Requires the password to have at least one non-alphanumeric character. Allowed characters include "!@#\$\$%^&*()_+~{}[];':<.>/?\ `~".

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 4.10.2

## Setting a User Password/Passphrase

To set the password/passphrase for a user profile, do the following:

- Navigate to **admin » users » {user} » set-password**, where {user} is the user ID. The **Set User Password** and **Trigger Action** forms appear.

**Figure 223: Set User Password Form**

1. New Password Box    2. New Password Repeat Box

**Figure 224: Trigger Action Form**

1. Perform Button

2. On the **Set User Password** form, configure the following parameters:

Parameter	Description
new-password	<b>Synopsis:</b> A string 1 to 128 characters long The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
new-password-repeat	<b>Synopsis:</b> A string 1 to 128 characters long The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.

3. On the **Trigger Action** form, click **Perform**.

## Section 4.10.3

## Setting the Boot Password/Passphrase

The boot password/passphrase grants access to BIST mode and service mode, which are only accessible through the Command Line Interface (CLI). For more information about these modes, refer to the *RUGGEDCOM ROX II v2.9 CLI User Guide*.

**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.*

**IMPORTANT!**

*The boot password/passphrase is only supported by version 2010.09RR16 or later of the uboot binary. For information about determining and/or upgrading the uboot version installed on the device, refer to the application note *Upgrading Uboot on ROX Devices* available on [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom).*

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

**NOTE**

*A passphrase must consist of four separate words and each word must be 4 to 20 characters long.*

1. Navigate to **admin » authentication » set-boot-password**. The **Set Boot Password** and **Trigger Action** forms appear.

The image shows a web form titled "Set Boot Password". It contains three input fields, each with a help icon (question mark in a circle) to its right. The first field is labeled "New Password \*" and has a green text hint below it: "<string, min: 0 chars, max: 128 chars>". The second field is labeled "New Password Repeat \*" and also has the same green text hint. The third field is labeled "Old Password" and has a password icon (key with a dot) and three asterisks "\*\*\*" next to it. Three numbered circles with arrows point to each of these fields: 1 points to the first field, 2 points to the second field, and 3 points to the third field.

**Figure 225: Set Boot Password Form**

1. New Password Box    2. New Password Repeat Box    3. Old Password Box

The image shows a web form titled "Trigger Action" with a gear icon to the left of the title. Below the title, there is a text instruction: "Specify appropriate parameters and hit the 'Perform' button to trigger the action." At the bottom right of the form is a dark, rounded button labeled "Perform". A numbered circle with the number "1" and an arrow points to this button.

**Figure 226: Trigger Action Form**

1. Perform Button

- On the **Set Boot Password** form, configure the following parameters:

Parameter	Description
new-password	<b>Synopsis:</b> A string 0 to 128 characters long The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
new-password-repeat	<b>Synopsis:</b> A string 0 to 128 characters long The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
old-password	<b>Synopsis:</b> A string 0 to 128 characters long Specify the old password if there is currently a boot password set.

- On the **Trigger Action** form, click **Perform**.

Section 4.10.4

## Setting the Maintenance Password/Passphrase

The maintenance password/passphrase grants access to the maintenance mode, which is only accessible through the Command Line Interface (CLI). For more information about this mode, refer to the *RUGGEDCOM ROX II v2.9 CLI User Guide*.



### 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:



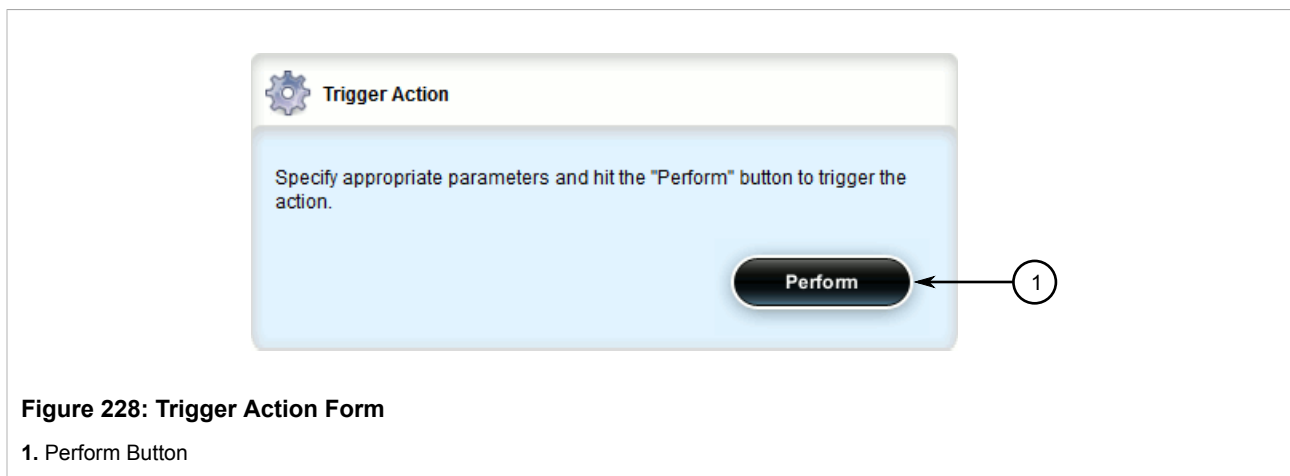
### NOTE

*A passphrase must consist of four separate words and each word must be 4 to 20 characters long.*

1. Navigate to **admin » authentication » set-maint-password**. The **Set Maint Password** and **Trigger Action** forms appear.

**Figure 227: Set Maint Password Form**

1. New Password Box    2. New Password Repeat Box    3. Old Password Box



- On the **Set Maint Password** form, configure the following parameters:

Parameter	Description
new-password	<b>Synopsis:</b> A string 1 to 128 characters long The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
new-password-repeat	<b>Synopsis:</b> A string 1 to 128 characters long The new password or passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
old-password	<b>Synopsis:</b> A string 1 to 128 characters long Specify the old password.

- On the **Trigger Action** form, click **Perform**.

#### Section 4.10.5

## Resetting Passwords and Passphrases

If either the admin, boot or maintenance password/passphrase is lost, the only method for resetting the password/passphrase is to physically connect to the device and reset the password/passphrase through the Command Line Interface (CLI). For information about resetting passwords/passphrases, refer to the *RUGGEDCOM ROX II v2.9 CLI User Guide*.

#### Section 4.11

## 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.

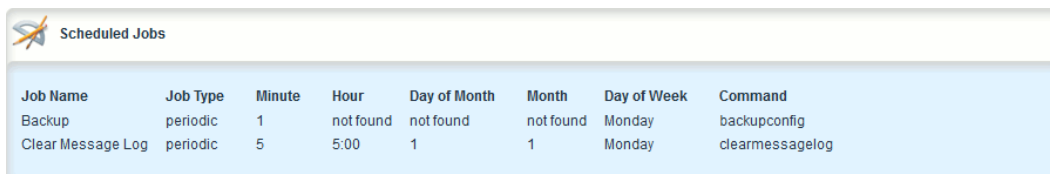
The following sections describe how to configure and manage scheduled jobs:

- [Section 4.11.1, “Viewing a List of Scheduled Jobs”](#)
- [Section 4.11.2, “Adding Scheduled Jobs”](#)
- [Section 4.11.3, “Deleting a Scheduled Job”](#)

#### Section 4.11.1

## Viewing a List of Scheduled Jobs

To view a list of scheduled jobs, navigate to **admin » scheduler**. If jobs have been configured, the **Scheduled Jobs** table appears.



The screenshot shows a web interface titled "Scheduled Jobs" with a table containing two rows of job data. The table has columns for Job Name, Job Type, Minute, Hour, Day of Month, Month, Day of Week, and Command.

Job Name	Job Type	Minute	Hour	Day of Month	Month	Day of Week	Command
Backup	periodic	1	not found	not found	not found	Monday	backupconfig
Clear Message Log	periodic	5	5:00	1	1	Monday	clearmessagelog

**Figure 229: Scheduled Jobs Table**

If no jobs have been configured, add jobs as needed. For more information, refer to [Section 4.11.2, “Adding Scheduled Jobs”](#).

#### Section 4.11.2

## Adding Scheduled Jobs

To add a scheduled job, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » scheduler** and click **<Add scheduled-jobs>**. The **Key Settings** form appears.

**Figure 230: Key Settings Form**

1. Job Name Box    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
Job Name	<p><b>Synopsis:</b> A string 1 to 64 characters long</p> <p>The name of the scheduled job. The name can be up to 64 characters in length.</p>

- Click **Add**. The **Scheduled Jobs** form appears.



**Figure 231: Key Settings Form**

**1. Job Type List   2. Minute Box   3. Hour Box   4. Day of Month Box   5. Month Box   6. Day of Week Box   7. Command Box**

5. Configure the following parameter(s) as required:

Parameter	Description
Job Type	<p><b>Synopsis:</b> { configchange, periodic }</p> <p><b>Default:</b> periodic</p> <p>Determines when to launch the scheduled job:</p> <ul style="list-style-type: none"> <li>periodic: The job launches at a set date and time.</li> <li>configchange: The job launches when the configuration changes.</li> </ul>
Minute	<p><b>Synopsis:</b> A string 1 to 128 characters long</p> <p><b>Default:</b> 0</p> <p>For periodic jobs, sets the minutes portion of the job launch time. Valid values are in the range of 0 to 59. If no value is set, the scheduler uses the default value of 0 and launches the job every hour on the the hour.</p> <ul style="list-style-type: none"> <li>To specify a single value, enter the value in the field. For example, to launch the job 10 minutes past the hour, enter 10.</li> <li>To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 15, 30, and 45 minutes past the hour, enter 15,30,45.</li> <li>To specify a range of values, enter the range as comma-separated values. For example, to launch the job every minute between 30 and 45</li> </ul>

Parameter	Description
	minutes past the hour, enter 30-45.</listitem></itemizedlist> This parameter is not required for configchange jobs.
Hour	<p><b>Synopsis:</b> A string 1 to 64 characters long</p> <p>For periodic jobs, sets the hour portion of the job launch time, in the 24-hour clock format. Valid values are in the range of 0 to 23. If no value is set, the job launches every hour at the time set in the Minute field. &lt;itemizedlist&gt;&lt;listitem&gt;To specify a single value, enter the value in the field. For example, to launch the job at 5:00 pm, enter 17.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt;&lt;/itemizedlist&gt; This parameter is not required for configchange jobs.</p>
Day of Month	<p><b>Synopsis:</b> A string 1 to 64 characters long</p> <p>For periodic jobs, sets the day of the month on which to run the scheduled job. Valid values are in the range of 1 to 31. If no value is set, the job launches every day. &lt;itemizedlist&gt;&lt;listitem&gt;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.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt;&lt;/itemizedlist&gt; This parameter is not required for configchange jobs.</p>
Month	<p><b>Synopsis:</b> A string 1 to 32 characters long</p> <p>For periodic jobs, sets the month in which to run the scheduled job. Valid values are in the range of 1 to 12. If no value is set, the job launches every day. &lt;itemizedlist&gt;&lt;listitem&gt;To specify a single value, enter the value in the field. For example, to set the month to February, enter 2.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt;&lt;/itemizedlist&gt; This parameter is not required for configchange jobs.</p>
Day of Week	<p><b>Synopsis:</b> A string 1 to 16 characters long</p> <p>For periodic jobs, sets the day of the week on which to run the scheduled job. Valid entries are in the range of 0 to 6, where 0 represents Sunday, 1 represents Monday, and so on. If no value is set, the job launches every day. &lt;itemizedlist&gt;&lt;listitem&gt;To specify a single value, enter the value in the field. For example, to set the day to Monday, enter 1.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt; &lt;listitem&gt;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.&lt;/listitem&gt;&lt;/itemizedlist&gt; This parameter is not required for configchange jobs.</p>
Command	<p><b>Synopsis:</b> A string 1 to 1024 characters long</p> <p>One or more commands to execute at the scheduled time. For example, this command saves the running configuration to a file name 'myconfig': show running-config   save myconfig. Do not</p>

Parameter	Description
	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.

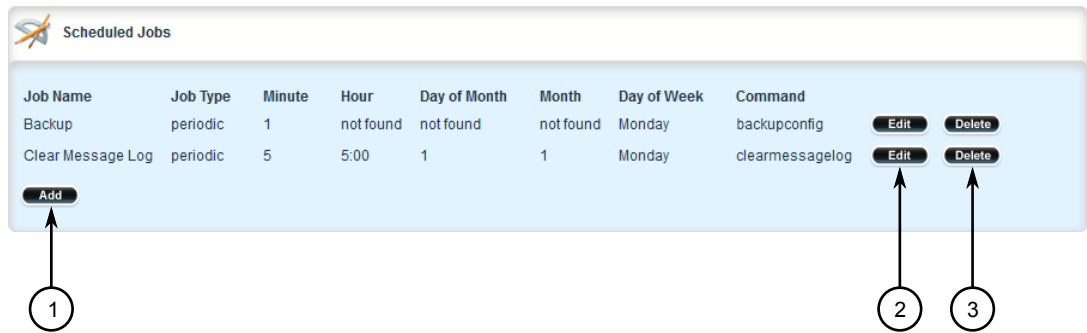
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 4.11.3

## Deleting a Scheduled Job

To delete a scheduled Job, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin » scheduler**. The **Scheduled Jobs** table appears.



**Figure 232: Scheduled Jobs Table**

1. Add Button    2. Edit Button    3. Delete Button

- Click **Delete** next to the chosen job.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.



# 5 Setup and Configuration

This chapter describes how to setup and configure the device for use on a network using the various features available in RUGGEDCOM ROX II. It describes the following tasks:

- [Section 5.1, “Configuring a Basic Network”](#)
- [Section 5.2, “Configuring ICMP Control”](#)
- [Section 5.3, “Enabling and Configuring CLI Sessions”](#)
- [Section 5.4, “Enabling and Configuring SFTP Sessions”](#)
- [Section 5.5, “Enabling and Configuring WWW Interface Sessions”](#)
- [Section 5.6, “Enabling/Disabling Brute Force Attack Protection”](#)
- [Section 5.7, “Viewing the Status of IPv4 Routes”](#)
- [Section 5.8, “Viewing the Status of IPv6 Routes”](#)
- [Section 5.9, “Viewing the Memory Statistics”](#)
- [Section 5.10, “Managing NETCONF”](#)
- [Section 5.11, “Managing SNMP”](#)
- [Section 5.12, “Managing Time Synchronization Functions”](#)
- [Section 5.13, “Managing the DHCP Relay Agent”](#)
- [Section 5.14, “Managing the DHCP Server”](#)
- [Section 5.15, “Managing Port Mirroring”](#)
- [Section 5.16, “Managing Firewalls”](#)
- [Section 5.17, “Managing IS-IS”](#)
- [Section 5.18, “Managing BGP”](#)
- [Section 5.19, “Managing RIP”](#)
- [Section 5.20, “Managing OSPF”](#)
- [Section 5.21, “Managing Virtual Routing and Forwarding \(VRF\)”](#)
- [Section 5.22, “Managing Static Routing”](#)
- [Section 5.23, “Managing Static Multicast Routing”](#)
- [Section 5.24, “Managing Dynamic Multicast Routing”](#)
- [Section 5.25, “Managing Multicast Filtering”](#)
- [Section 5.26, “Managing VRRP”](#)
- [Section 5.27, “Managing Link Failover Protection”](#)
- [Section 5.28, “Managing IPsec Tunnels”](#)
- [Section 5.29, “Managing 6in4 and 4in6 Tunnels”](#)
- [Section 5.30, “Managing Layer 2 Tunnels”](#)
- [Section 5.31, “Managing Generic Routing Encapsulation Tunnels”](#)
- [Section 5.32, “Managing Layer 3 Switching”](#)

- [Section 5.33, “Managing Classes of Service”](#)
- [Section 5.34, “Managing MAC Addresses”](#)
- [Section 5.35, “Managing Spanning Tree Protocol”](#)
- [Section 5.36, “Managing VLANs”](#)
- [Section 5.37, “Managing Network Discovery and LLDP”](#)
- [Section 5.38, “Managing Traffic Control”](#)
- [Section 5.39, “Managing IP Addresses for Routable Interfaces”](#)
- [Section 5.40, “Managing MPLS”](#)

## Section 5.1

## Configuring a Basic Network

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

The following table lists the default IP addresses.

**Table: Default IP Addresses**

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

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

The following sections describe how to configure a basic network:

- [Section 5.1.1, “Configuring a Basic IPv4 Network”](#)
- [Section 5.1.2, “Configuring a Basic IPv6 Network”](#)

## Section 5.1.1

### Configuring a Basic IPv4 Network

To configure a basic IPv4 network, do the following:

1. Connect a computer to the Fast Ethernet (fe-cm-1) of the device and configure the computer to be on the same subnet as the port.
2. Configure the computer to use the IPv4 address of the Fast Ethernet port as the default gateway.
3. Connect one of the switched ports from any available line module to a switch that is connected to a LAN.
4. Make sure the computer connected to the switch is on the same subnet as the switch.
5. Enable the Brute Force Attack (BFA) protection system on the device. For more information, refer to [Section 5.6, “Enabling/Disabling Brute Force Attack Protection”](#).

6. Configure the switch and all the computers behind it to use switch.0001's IP address as the default gateway. The default IP address is 192.168.0.2.
7. Make sure all computers connected to the device can ping one another.

### Section 5.1.2

## Configuring a Basic IPv6 Network

To configure a basic IPv6 network, do the following:

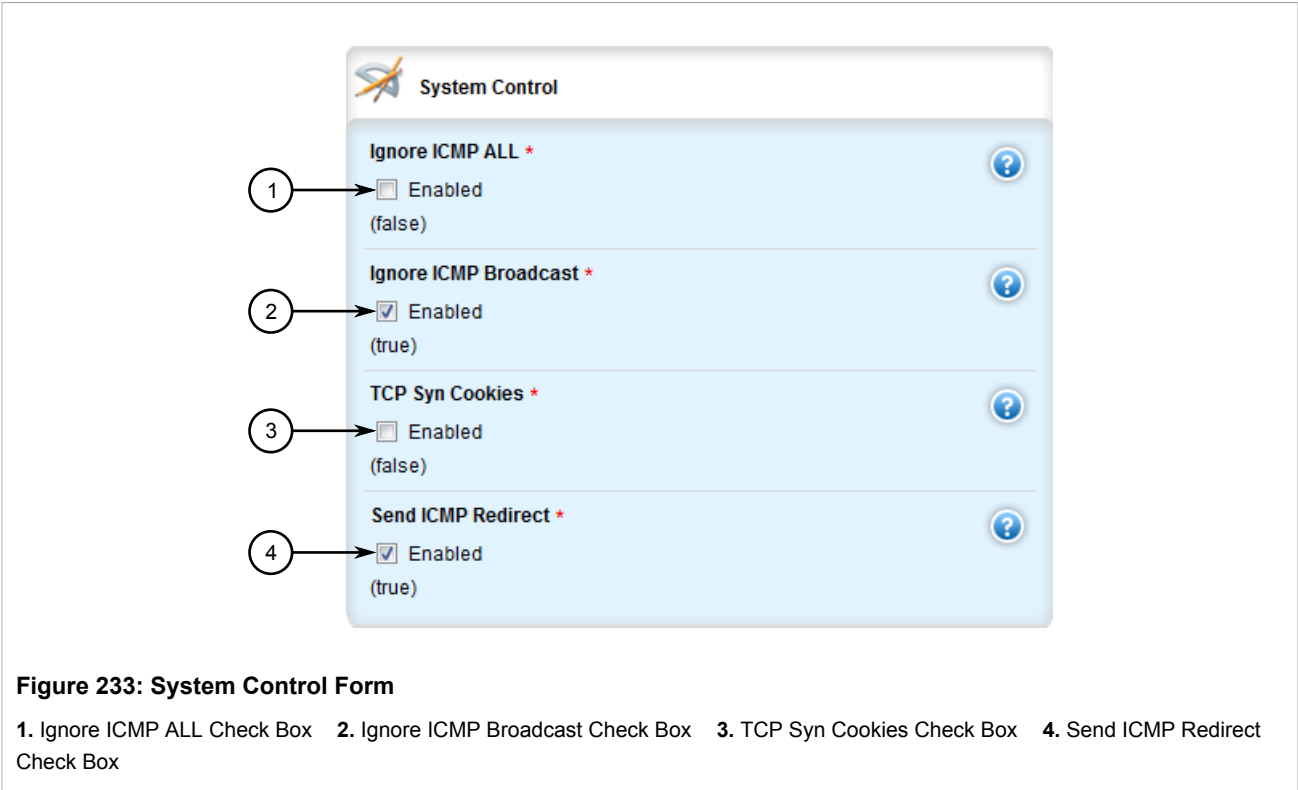
1. Connect a computer to the Fast Ethernet port (fe-cm-1) of the device and configure the computer to be on the same subnet as the port.
2. Configure an IPv6 address and default gateway for the computer (e.g. FDD1:9AEF:3DE4::1/24 and FDD1:9AEF:3DE4::2).
3. Configure the fe-cm-1 and switch.0001 interfaces on the device with IPv6 addresses.
4. Connect one of the switched ports from any available line module to an IPv6 capable network.
5. Configure the computers on the IPv6 network to be on the same IP subnet as switch.0001 and configure the default gateway address.
6. Enable the Brute Force Attack (BFA) protection system on the device. For more information, refer to [Section 5.6, "Enabling/Disabling Brute Force Attack Protection"](#).
7. Enable IPv6 Neighbor Discovery. For more information, refer to [Section 5.39.4, "Configuring IPv6 Neighbor Discovery"](#).
8. Make sure all computers connected to the device can ping one another.

### Section 5.2

## Configuring ICMP Control

To configure how RUGGEDCOM ROX II manages ICMP redirect messages, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin**. The **System Control** form appears.



3. Configure the following parameter(s) as required:



**NOTE**  
*ICMP redirect messages are sent by routers to hosts to inform them when a better route is available for a particular destination. However, before enabling RUGGEDCOM ROX II to send ICMP messages, be aware that ICMP redirects are simple to forge, allowing attackers to control the path by which packets are forwarded, and are sometimes considered a security risk. Send ICMP redirect messages only when appropriate.*

Parameter	Description
Ignore ICMP ALL	<b>Synopsis:</b> true or false <b>Default:</b> false Ignores all ICMP echo requests sent to it.
Ignore ICMP Broadcast	<b>Synopsis:</b> true or false <b>Default:</b> true Ignores all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast.
TCP Syn Cookies	<b>Synopsis:</b> true or false <b>Default:</b> false Sends out syncookies when the syn backlog queue of a socket overflows. This is to prevent against the common 'SYN flood attack'.
Send ICMP Redirect	<b>Synopsis:</b> true or false <b>Default:</b> true Sends the ICMP redirect.



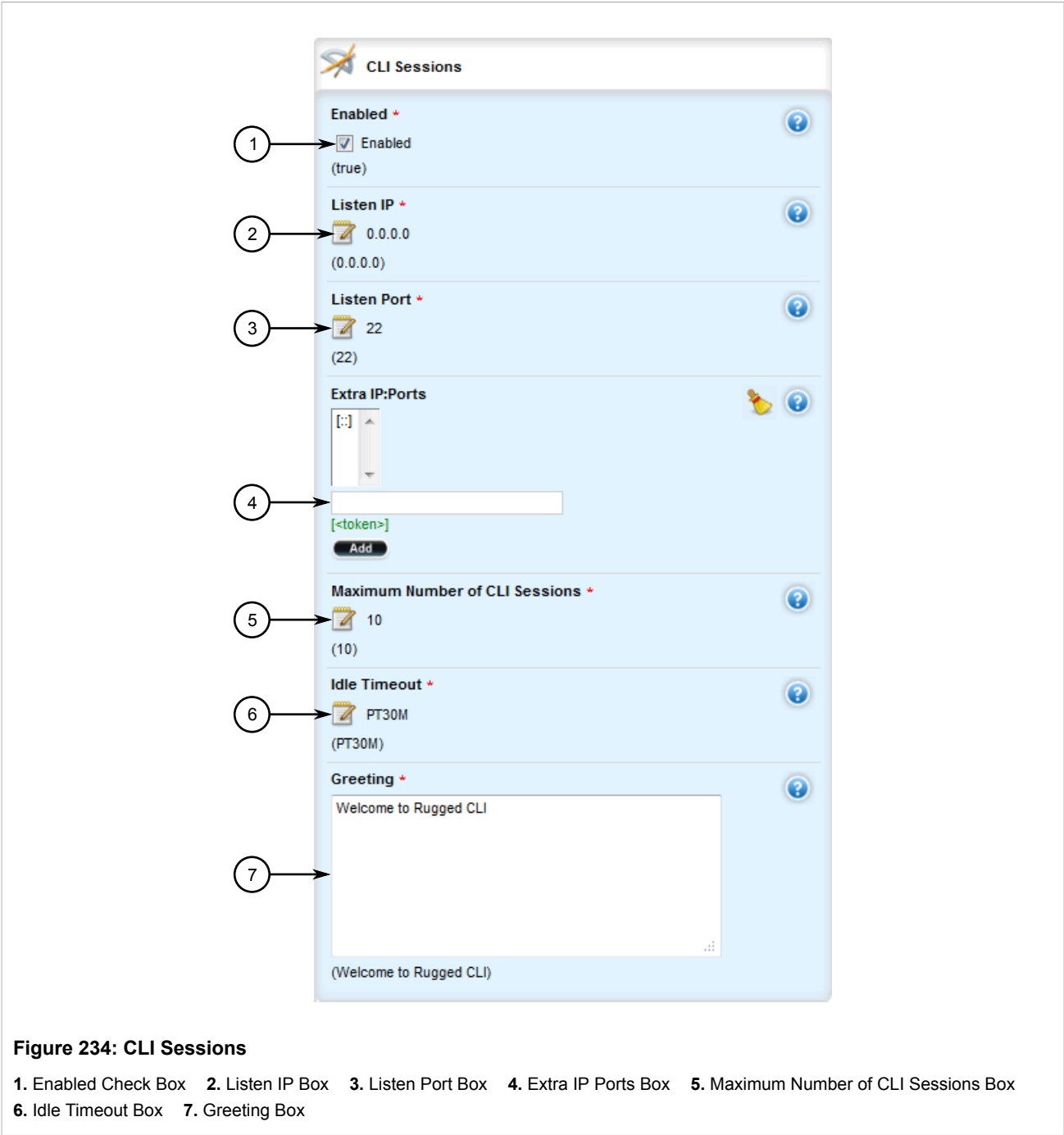
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.3

## Enabling and Configuring CLI Sessions

To enable and configure CLI sessions, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin**. The **CLI Sessions** form appears.



3. Configure the following parameter(s):

Parameter	Description
enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Provides the ability to configure the device via CLI over ssh and serial console.
Listen IP	<b>Synopsis:</b> A string <b>Default:</b> 0.0.0.0

Parameter	Description
	The IP Address the CLI will listen on for CLI requests.
Listen Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 22 The port on which the CLI listens for CLI requests.
Extra IP:Ports	<b>Synopsis:</b> A string The CLI 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.
Maximum Number of CLI Sessions	<b>Synopsis:</b> { unbounded } <b>Default:</b> 10 The maximum number of concurrent CLI sessions.
Idle Timeout	<b>Synopsis:</b> A string <b>Default:</b> PT30M The maximum time before an idle CLI session is terminated. The default time is 30 minutes, or PT30M. A timeout period of 1 year, 1 month, 2 hours and 30 seconds would be translated as P1Y1MT2H30S. The countdown will not begin if the system is waiting for notifications or if commits are pending. Changes will not take effect until the next CLI session.
Greeting	<b>Synopsis:</b> A string 1 to 8192 characters long Sets the greeting presented when the user logs in to the CLI. <phrase userlevel="CLI">The string must be enclosed in quotation marks.</phrase> Sets the greeting presented when the user logs in to the CLI.

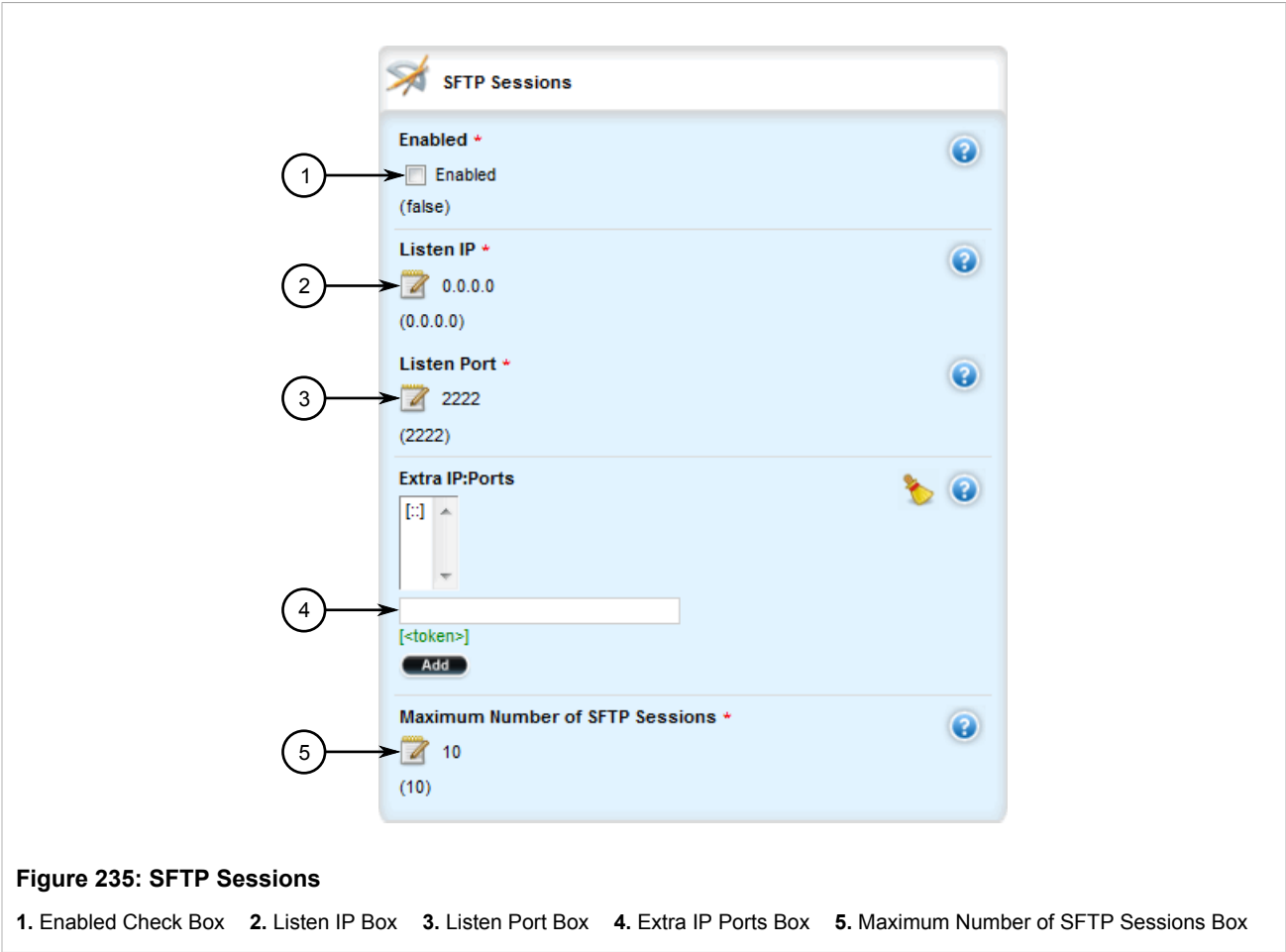
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.4

## Enabling and Configuring SFTP Sessions

To enable and configure SFTP sessions, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin**. The **SFTP Sessions** form appears.



3. Configure the following parameter(s):

Parameter	Description
enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/Disables the SFTP user interface.
Listen IP	<b>Synopsis:</b> A string <b>Default:</b> 0.0.0.0 The IP Address the SFTP will listen on for SFTP requests.
Listen Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 2222 The port the SFTP will listen on for SFTP requests.
Extra IP:Ports	<b>Synopsis:</b> A string The SFTP 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.
Maximum Number of SFTP Sessions	<b>Synopsis:</b> { unbounded } <b>Default:</b> 10

Parameter	Description
	This parameter is not supported and any value is ignored by the system.

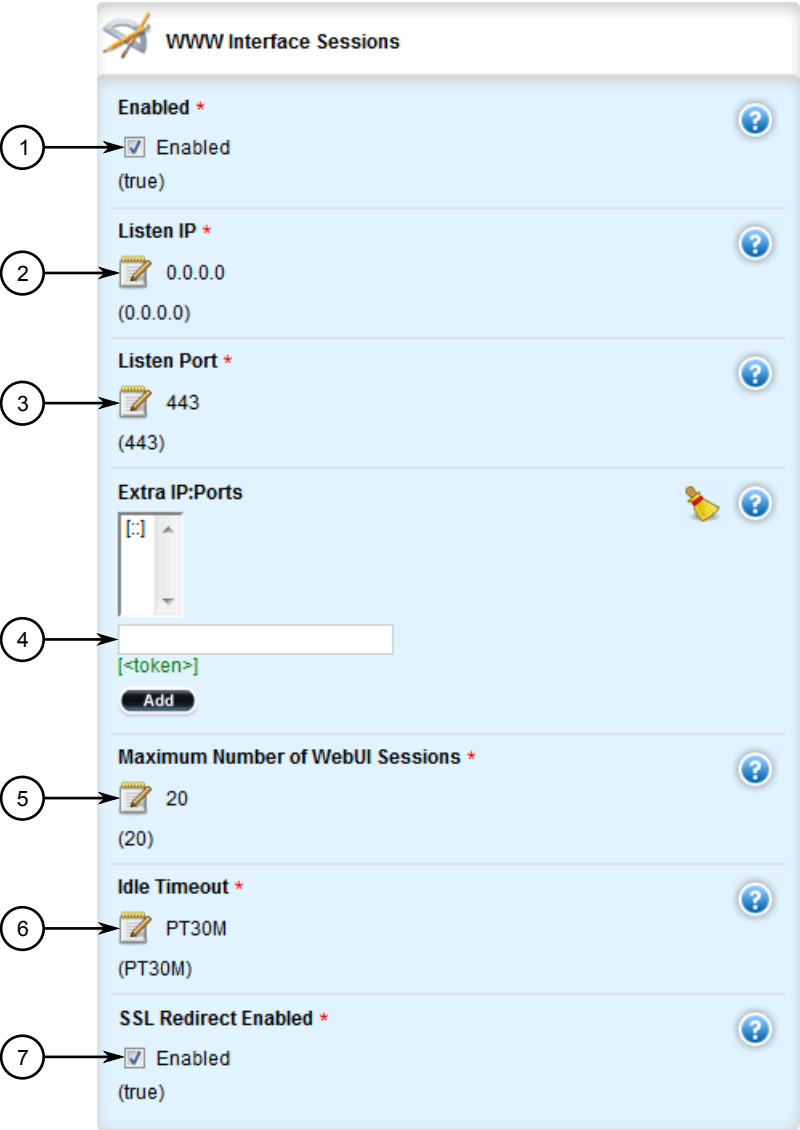
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.5

## Enabling and Configuring WWW Interface Sessions

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

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin**. The **WWW Interface Sessions** form appears.



**Figure 236: WWW Interface Sessions**

1. Enabled Check Box   2. Listen IP Box   3. Listen Port Box   4. Extra IP Ports Box   5. Maximum Number of WebUI Sessions Box   6. Idle Timeout Box   7. SSL Redirect Enabled Check Box

3. Configure the following parameter(s):

Parameter	Description
enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Provides the ability to configure WebUI features on the device.
Listen IP	<b>Synopsis:</b> A string <b>Default:</b> 0.0.0.0 The IP Address the CLI will listen on for WebUI requests.

Parameter	Description
Listen Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 443 The port on which the WebUI listens for WebUI requests.
Extra IP:Ports	<b>Synopsis:</b> 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.
Maximum Number of WebUI Sessions	<b>Synopsis:</b> { unbounded } <b>Default:</b> 20 The maximum number of concurrent WebUI sessions
Idle Timeout	<b>Synopsis:</b> A string <b>Default:</b> 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	<b>Synopsis:</b> true or false <b>Default:</b> true Redirects traffic from port 80 to port 443. If disabled, port 80 will be closed.
Client Certificate Verification	<b>Synopsis:</b> { none, peer, fail-if-no-peer-cert } <b>Default:</b> none Client certificate verification level Level of verification the server does on client certificates <itemizedlist><listitem>none - It does not do any verification.</listitem> <listitem>peer - The server will ask the client for a client-certificate but not fail if the client does not supply a client-certificate.</listitem> <listitem>fail-if-no-peer-cert - The server requires the client to supply a client certificate.</listitem></itemizedlist>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.6

# 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).
```

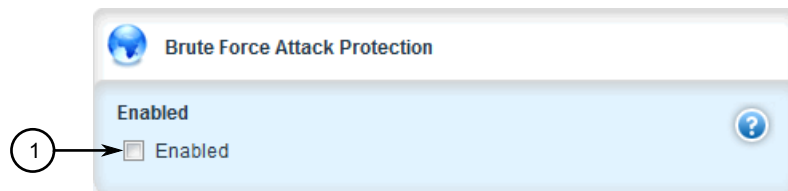


#### NOTE

*For information about how to view auth.log, refer to [Section 3.9.1, “Viewing Logs”](#).*

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security**. The **Brute Force Attack Protection** form appears.



**Figure 237: Brute Force Attack Protection Form**

1. Enable Check Box

3. Select the check box to enable the BFA protection mechanism, or clear it to disable the mechanism.



4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.7

# Viewing the Status of IPv4 Routes

To view the status of the IPv4 routes configured on the device, navigate to **routing » status » ipv4routes**. If IPv4 routes have been configured, the **IPv4 Kernel Active Routing** table appears.



**NOTE**  
*It is possible to create a route on a locally connected broadcast network (i.e. without a gateway) without also bringing up a corresponding IP address on that interface. For example, it would be possible to add 192.168.1.0/24 to switch.0001, which has an IP address of 10.0.1.1 but no corresponding alias address on the 192.168.1.0/24 subnet.*

IPv4 Kernel Active Routing Table					
Subnet	Gateway Address	Interface Name	Route Type	Route Weight	Metric
192.168.0.0/24		switch.0001	kernel		

Figure 238: IPv4 Kernel Active Routing Table

This table provides the following information:

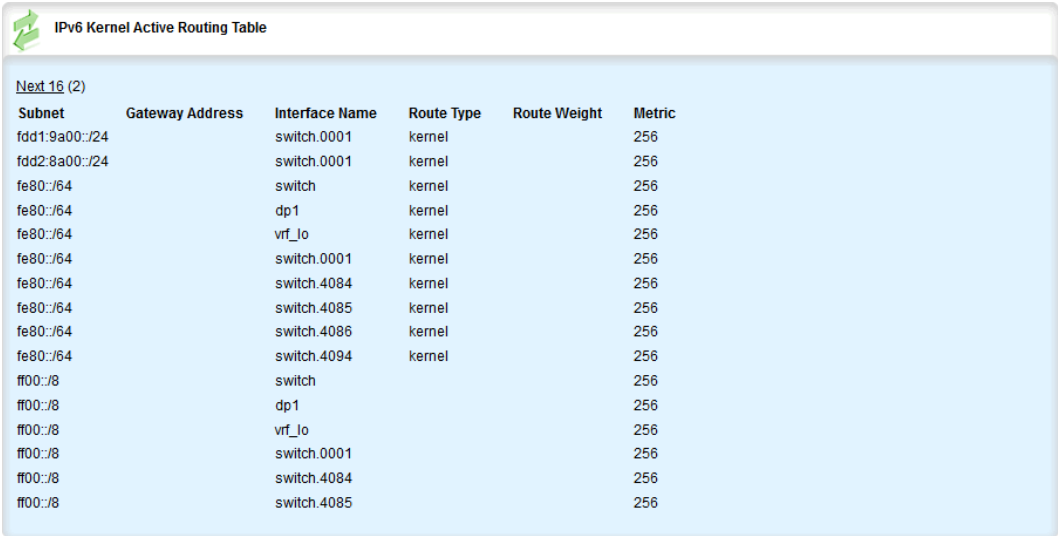
Parameter	Description
Subnet	<b>Synopsis:</b> A string The network/prefix.
Gateway Address	<b>Synopsis:</b> A string The gateway address.
Interface Name	<b>Synopsis:</b> A string The interface name.
Route Type	<b>Synopsis:</b> A string The route type.
Route Weight	<b>Synopsis:</b> A string The route weight.
Metric	<b>Synopsis:</b> A string The route metric value.

If no IPv4 routes have been configured, add routes as needed. For more information, refer to [Section 5.39.3.2, “Adding an IPv4 Address”](#).

Section 5.8

# Viewing the Status of IPv6 Routes

To view the status of the IPv6 routes configured on the device, navigate to **routing » status » ipv6routes**. If IPv6 routes have been configured, the **IPv6 Kernel Active Routing** table appears.



Subnet	Gateway Address	Interface Name	Route Type	Route Weight	Metric
Next 16 (2)					
fdd1:9a00::/24		switch.0001	kernel		256
fdd2:8a00::/24		switch.0001	kernel		256
fe80::/64		switch	kernel		256
fe80::/64		dp1	kernel		256
fe80::/64		vrf_lo	kernel		256
fe80::/64		switch.0001	kernel		256
fe80::/64		switch.4084	kernel		256
fe80::/64		switch.4085	kernel		256
fe80::/64		switch.4086	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		switch.4084			256
ff00::/8		switch.4085			256

Figure 239: IPv6 Kernel Active Routing Table

This table provides the following information:

Parameter	Description
Subnet	<b>Synopsis:</b> A string The network/prefix.
Gateway Address	<b>Synopsis:</b> A string The gateway address.
Interface Name	<b>Synopsis:</b> A string The interface name.
Route Type	<b>Synopsis:</b> A string The route type.
Route Weight	<b>Synopsis:</b> A string The route weight.
Metric	<b>Synopsis:</b> A string The metric value.

If no IPv6 routes have been configured, add routes as needed. For more information, refer to [Section 5.22.3, “Adding an IPv6 Static Route”](#).

Section 5.9

# Viewing the Memory Statistics

To view statistics related to the Core, RIP, OSPF and BGP daemons, navigate to **routing » status » memory**. The **Core Daemon Memory Statistics**, **RIP Daemon Memory Statistics**, **OSPF Daemon Memory Statistics** and **BGP Daemon Memory Statistics** forms appear.

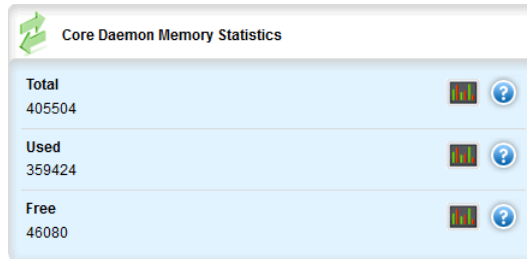


Figure 240: Core Daemon Memory Statistics Form

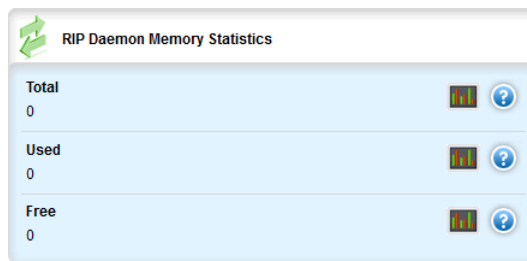


Figure 241: RIP Daemon Memory Statistics Form

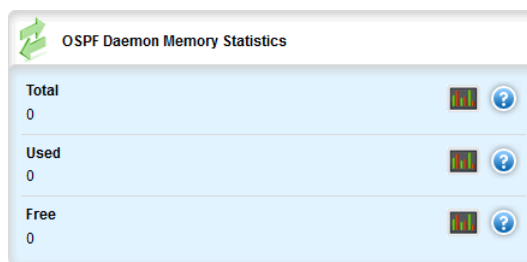
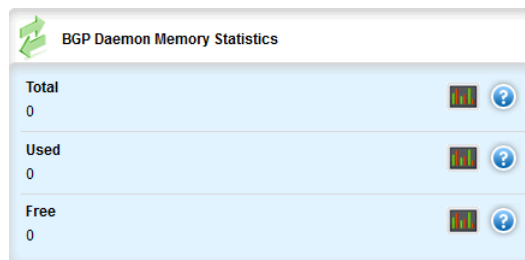


Figure 242: OSPF Daemon Memory Statistics Form



**Figure 243: BGP Daemon Memory Statistics Form**

These forms provides the following information:

Parameter	Description
total	The total heap allocated (in bytes).
used	The number of used ordinary blocks (in bytes).
free	The number of free ordinary blocks (in bytes).

#### Section 5.10

## 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 RUGGEDCOM ROX II NETCONF Reference Guide.*

The following sections describe how to configure and manage NETCONF:

- [Section 5.10.1, “Enabling and Configuring NETCONF Sessions”](#)
- [Section 5.10.2, “Viewing NETCONF Statistics”](#)

#### Section 5.10.1

## Enabling and Configuring NETCONF Sessions

To enable and configure NETCONF sessions, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » netconf**. The **NETCONF Sessions** form appears.

The screenshot shows the 'NETCONF Sessions' configuration page. It has a light blue background and a white header with the 'NETCONF Sessions' title and a logo. The configuration is divided into several sections, each with a title, a value, and a help icon (question mark in a circle). The sections are: 'Enabled \*' with a checked checkbox and the value '(true)'; 'Listen IP \*' with a text box containing '0.0.0.0' and the value '(0.0.0.0)'; 'Listen Port \*' with a text box containing '830' and the value '(830)'; 'Extra IP:Ports' with a text box containing '[:]' and a bell icon; 'Maximum Number of NETCONF Sessions \*' with a text box containing '10' and the value '(10)'; and 'Idle Timeout \*' with a text box containing 'PT0S' and the value '(PT0S)'. Numbered callouts point to specific elements: 1 points to the 'Enabled' checkbox, 2 points to the 'Listen IP' text box, 3 points to the 'Listen Port' text box, 4 points to the 'Extra IP:Ports' text box, 5 points to the 'Maximum Number of NETCONF Sessions' text box, and 6 points to the 'Idle Timeout' text box.

**Figure 244: NETCONF Sessions**

1. Enabled Check Box   2. Listen IP Box   3. Listen Port Box   4. Extra IP Ports Box   5. Maximum Number of NETCONF Sessions Box   6. Idle Timeout Box



**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.*

3. Configure the following parameter(s):

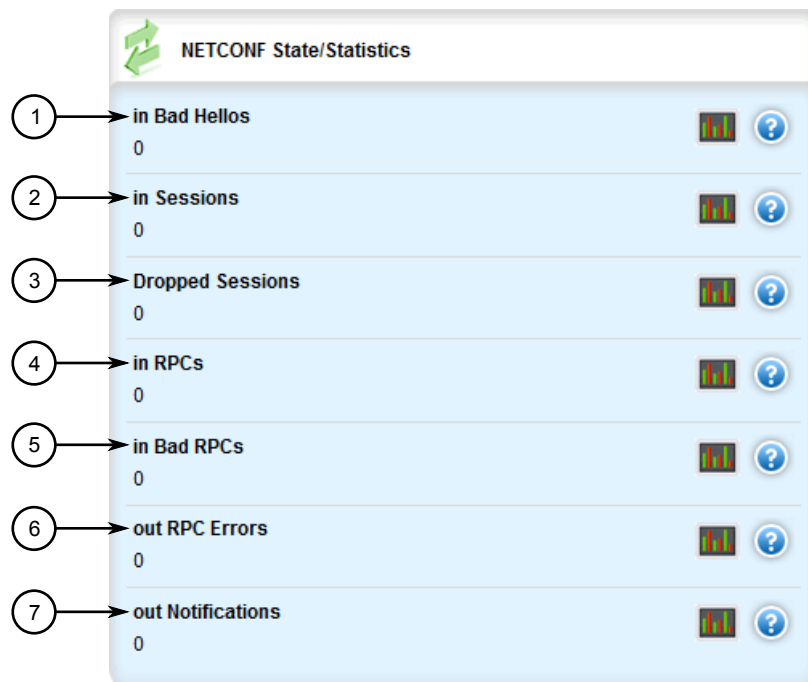
Parameter	Description
enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Provides the ability to configure NETCONF features on the device.
Listen IP	<b>Synopsis:</b> A string <b>Default:</b> 0.0.0.0 The IP Address the CLI will listen on for NETCONF requests.
Listen Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 830 The port on which NETCONF listens for NETCONF requests.
Extra IP:Ports	<b>Synopsis:</b> A string Additional IP addresses and ports on which NETCONF listens for NETCONF requests. You can specify IP addresses and ports in the following forms: <itemizedlist><listitem>nnn.nnn.nnn.nnn:port represents an IPv4 address followed by a colon and port number. For example, 192.168.10.12:19343</listitem> <listitem>0.0.0.0 represents the default IPv4 address and default port number. This is the default configuration.</listitem> <listitem>[:]:port represents an IPv6 address followed by a colon and port number. For example, [fe80::5eff:35ff]:16000</listitem> <listitem>If using the default address, do not specify another listen address with the same port.</listitem> </itemizedlist>
Maximum Number of NETCONF Sessions	<b>Synopsis:</b> { unbounded } <b>Default:</b> 10 The maximum number of concurrent NETCONF sessions.
Idle Timeout	<b>Synopsis:</b> A string <b>Default:</b> PT0S The maximum idle time before terminating a NETCONF 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.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.10.2

## Viewing NETCONF Statistics

To view NETCONF related statistics, navigate to **admin » netconf**. The **NETCONF State/Statistics** form appears.

**Figure 245: NETCONF State/StatisticsForm**

1. In Bad Hellos   2. In Sessions   3. Dropped Sessions   4. In RPCs   5. In Bad RPCs   6. Out RPC Errors   7. Out Notifications

This form provides the following information:

Parameter	Description
In Bad Hellos	The total number of sessions silently dropped because an invalid 'hello' message was received. This includes hello messages with a 'session-id' attribute, bad namespace, and bad capability declarations.
In Sessions	The total number of NETCONF sessions started towards the NETCONF peer. $\text{inSessions} - \text{inBadHellos} = \text{'The number of correctly started NETCONF sessions.'}$
Dropped Sessions	The total number of NETCONF sessions dropped. $\text{inSessions} - \text{inBadHellos} = \text{'The number of correctly started NETCONF sessions.'}$
In RPCs	The total number of RPC requests received.
In Bad RPCs	The total number of RPCs which were parsed correctly, but couldn't be serviced because they contained non-conformant XML.
Out RPC Errors	The total number of 'rpc-reply' messages with 'rpc-error' sent.
Out Notifications	The total number of 'notification' messages sent.

Section 5.11

## 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

The following sections describe how to configure and manage SNMP:

- [Section 5.11.1, “MIB Files and SNMP Traps”](#)
- [Section 5.11.2, “Enabling and Configuring SNMP Sessions”](#)
- [Section 5.11.3, “Viewing Statistics for SNMP”](#)
- [Section 5.11.4, “Discovering SNMP Engine IDs”](#)
- [Section 5.11.5, “Managing SNMP Communities”](#)
- [Section 5.11.6, “Managing SNMP Target Addresses”](#)
- [Section 5.11.7, “Managing SNMP Users”](#)
- [Section 5.11.8, “Managing SNMP Security Model Mapping”](#)
- [Section 5.11.9, “Managing SNMP Group Access”](#)

Section 5.11.1

### MIB Files and SNMP Traps

The current MIB files supported by RUGGEDCOM ROX II can be downloaded from the [www.siemens.com/ruggedcom](http://www.siemens.com/ruggedcom).



**NOTE**

SNMP traps are not configurable in RUGGEDCOM ROX II.

The MIB files support the following SNMP traps:

**Table: SNMP Traps**

Standard	MIB	Trap and Description
RFC 3418	SNMPv2-MIB	<b>authenticationFailure</b> An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
		<b>coldStart</b> A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
		<b>warmStart</b> 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	<b>newRoot</b> The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree. The trap is sent by a bridge soon after its election as the new root (e.g. upon expiration of the Topology Change Timer) immediately subsequent to its election. Implementation of this trap is optional.
		<b>topologyChange</b> A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
IEEE Std 802.1AB-2005	LLDP-MIB	<b>IldpRemTablesChange</b> An IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. It can be utilized by a Network Management System (NMS) to trigger LLDP remote systems table maintenance polls. Note that transmission of IldpRemTablesChange notifications are throttled by the agent, as specified by the IldpNotificationInterval object.
RFC 1229, 2863, 2233, 1573	IF-MIB	<b>linkUp</b> A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
		<b>linkDown</b> A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
RuggedCom	RUGGEDCOM-TRAPS-MIB	<b>trapGenericTrap</b> The main subtree for RUGGEDCOM generic traps. Used for <i>User Authentication Events</i> only.
		<b>trapPowerSupplyTrap</b> The main subtree for the RUGGEDCOM power supply trap.
		<b>trapSwUpgradeTrap</b> The main subtree for the RUGGEDCOM software upgrade trap.
		<b>trapCfgChangeTrap</b> The main subtree for the RUGGEDCOM configuration change trap.

Standard	MIB	Trap and Description
		<b>trapFanBankTrap</b> The main subtree for the RUGGEDCOM fan bank trap.
		<b>trapHotswapModuleStateChangeTrap</b> The main subtree for the RUGGEDCOM fan hot-swap module state change trap.
RFC 3895	DS1-MIB	<b>ds1LineStatusChange</b> 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: <ul style="list-style-type: none"> <li>• <b>dsx1RcvFarEndLOF</b> – Far end Loss of Frames (i.e. yellow alarm or RAI)</li> <li>• <b>dsx1RcvAIS</b> – Far end sending AIS</li> <li>• <b>dsx1LossOfFrame</b> – Near end Loss of Frame (i.e. red alarm)</li> <li>• <b>dsx1LossofSignal</b> – Near end Loss of Signal</li> <li>• <b>dsx1OtherFailure</b> – Out of Frame</li> <li>• <b>dsx1NoAlarm</b></li> </ul>

#### Section 5.11.2

## Enabling and Configuring SNMP Sessions

To enable and configure SNMP sessions, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp**. The **SNMP Sessions** form appears.

The image shows the 'SNMP Sessions' configuration page in a web interface. It features a light blue background with various configuration options. Numbered callouts (1-11) point to specific elements:

- 1:** Points to the 'Enable' checkbox, which is currently unchecked. The text 'Enabled (false)' is displayed below it.
- 2:** Points to the 'Listen IP' text box, which contains '0.0.0.0'. The text '(0.0.0.0)' is displayed below it.
- 3:** Points to the 'Listen Port' text box, which contains '161'. The text '(161)' is displayed below it.
- 4:** Points to the 'Extra IP:Ports' section, which includes a text box containing '[::]', a vertical scrollbar, and an 'Add' button below it. The text '<token>' is displayed below the text box.
- 5:** Points to the 'Maximum Number of SNMP Sessions' text box, which contains '30'. The text '(30)' is displayed below it.
- 6:** Points to the 'SNMP Local Engine ID' text box, which contains '80:00:3a:9c:03:00:0a:dc:ff:44:00'.
- 7:** Points to the 'Source IP for Traps' text box, which contains '--'.
- 8:** Points to the 'Authentication Failure Notify Name' dropdown menu, which is set to 'none'. The text '(none)' is displayed below it.
- 10:** Points to the 'Enable Authentication Traps' checkbox, which is currently unchecked. The text 'Enabled (false)' is displayed below it.
- 11:** Points to the 'DSCP Value for SNMP Traffic' text box, which contains '0'. The text '(0)' is displayed below it.

Other visible elements include a title bar 'SNMP Sessions' with a logo, question mark icons for help, and a bell icon for notifications.

**Figure 246: SNMP Sessions**

1. Enabled Check Box   2. Listen IP Box   3. Listen Port Box   4. Extra IP Ports Box   5. Maximum Number of SNMP Sessions Box   6. SNMP Local Engine ID Box   7. Source ID for Traps Box   8. Authentication Failure Notify Name Box   9. Enable Authentication Box   10. DSCP Value for SNMP Traffic Box

3. Configure the following parameter(s):

Parameter	Description
Enable	<p><b>Synopsis:</b> true or false  <b>Default:</b> false</p> <p>Provides the ability to configure SNMP features on the device.</p>
Listen IP	<p><b>Synopsis:</b> A string  <b>Default:</b> 0.0.0.0</p> <p>The IP Address the SNMP agent will listen on for SNMP requests.</p>
Listen Port	<p><b>Synopsis:</b> An integer between 0 and 65535  <b>Default:</b> 161</p> <p>The port the SNMP agent will listen on for SNMP requests.</p>
Extra IP:Ports	<p><b>Synopsis:</b> A string</p> <p>The SNMP agent 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.</p>
Maximum Number of SNMP Sessions	<p><b>Synopsis:</b> { unbounded }  <b>Default:</b> 30</p> <p>The maximum number of concurrent SNMP sessions.</p>
SNMP Local Engine ID	<p><b>Synopsis:</b> A string</p> <p>Provides specific identification for the engine/device. By default, this value is set to use the base MAC address within the Engine ID value. When using SNMPv3: If you change this value, you must also change the User SNMP Engine ID value for SNMP users.</p>
Source IP for Traps	<p><b>Synopsis:</b> A string</p> <p>If set, all traffic/traps originating from this device shall use the configured IP Address for the Source IP.</p>
Authentication Failure Notify Name	<p><b>Synopsis:</b> { none, snmpv1_trap, snmpv2_trap, snmpv2_inform, snmpv3_trap, snmpv3_inform }  <b>Default:</b> none</p> <p>When the SNMP agent sends the standard authenticationFailure notification, it is delivered to the management targets defined for the snmpNotifyName in the snmpNotifyTable in SNMP-NOTIFICATION-MIB (RFC3413). If authenticationFailureNotifyName is the empty string (default), the notification is delivered to all management targets.</p>
Enable Authentication Traps	<p><b>Synopsis:</b> true or false  <b>Default:</b> false</p> <p>Enables authentication traps to be sent from the SNMP agent.</p>
DSCP Value for SNMP Traffic	<p><b>Synopsis:</b> An integer between 0 and 63  <b>Default:</b> 0</p> <p>Support for setting the Differentiated Services Code Point (6 bits) for traffic originating from the SNMP agent.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.11.3

# Viewing Statistics for SNMP

To view the statistics collected for SNMP, navigate to **admin » snmp**. The **SNMP USM** form appears.

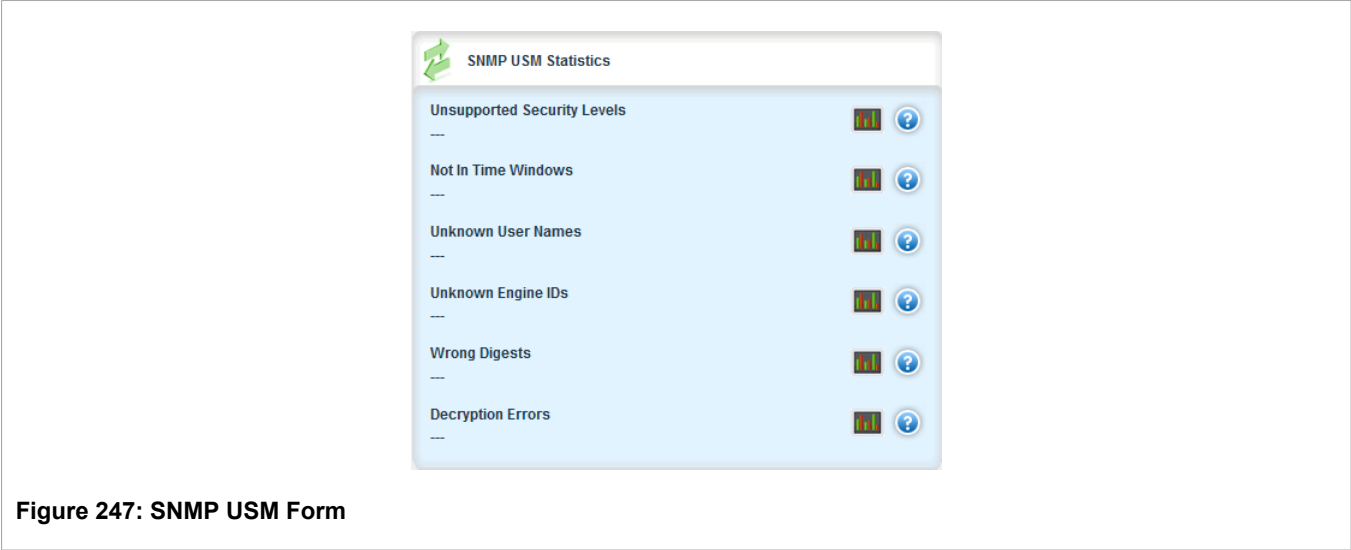


Figure 247: SNMP USM Form

This table provides the following information:

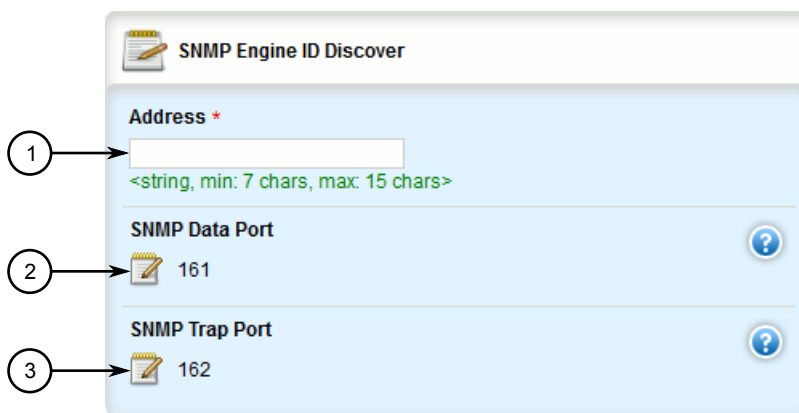
Parameter	Description
Unsupported Security Levels	The total number of packets received by the SNMP engine which were dropped because they requested a securityLevel that was unknown to the SNMP engine or otherwise unavailable.
Not In Time Windows	The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.
Unknown Engine IDs	The total number of packets received by the SNMP engine which were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value.
Decryption Errors	The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.

Section 5.11.4

# Discovering SNMP Engine IDs

To discover an SNMP engine ID on a device, do the following:

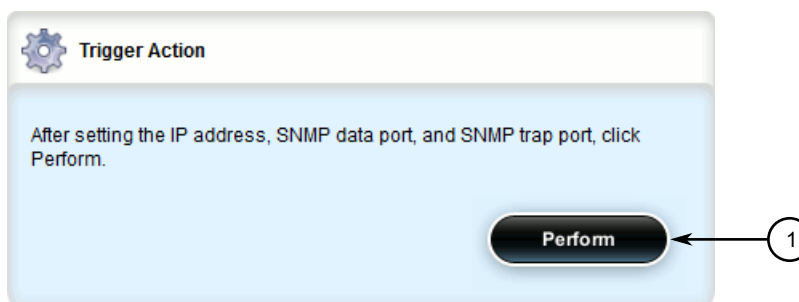
1. Navigate to **admin » snmp** and click **snmp-discover** in the menu. The **SNMP Engine ID Discover** and **Trigger Action** forms appear.



The image shows a web form titled "SNMP Engine ID Discover". It contains three input fields, each with a numbered callout: 1. "Address \*" with a text input box and a hint "<string, min: 7 chars, max: 15 chars>". 2. "SNMP Data Port" with a dropdown menu showing "161" and a help icon. 3. "SNMP Trap Port" with a dropdown menu showing "162" and a help icon.

**Figure 248: SNMP Engine ID Discover Form**

1. Address Box   2. SNMP Data Port Box   3. SNMP Trap Port Box



The image shows a web form titled "Trigger Action" with a gear icon. It contains a text instruction: "After setting the IP address, SNMP data port, and SNMP trap port, click Perform." Below the instruction is a "Perform" button, which is pointed to by a numbered callout 1.

**Figure 249: Trigger Action Form**

1. Perform Button

2. Click **Perform**.

#### Section 5.11.5

## Managing SNMP Communities

The following sections describe how to configure and manage SNMP communities:

- [Section 5.11.5.1, "Viewing a List of SNMP Communities"](#)
- [Section 5.11.5.2, "Adding an SNMP Community"](#)
- [Section 5.11.5.3, "Deleting an SNMP Community"](#)

## Section 5.11.5.1

## Viewing a List of SNMP Communities

To view a list of SNMP communities configured on the device, navigate to **admin » snmp » snmp-community**. The **SNMPv1/v2c Community Configuration** table appears.



The image shows a screenshot of the 'SNMPv1/v2c Community Configuration' table. The table has two columns: 'Community Name' and 'User Name'. It lists two pre-configured communities: 'private' with user 'oper' and 'public' with user 'guest'.

Community Name	User Name
private	oper
public	guest

**Figure 250: SNMPv1/v2c Community Configuration Table**

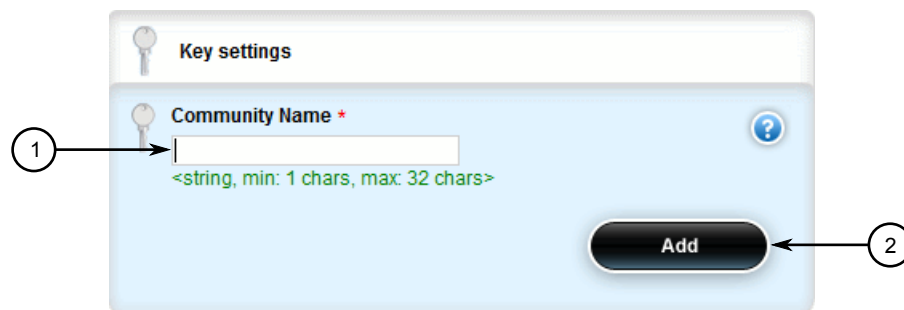
By default, private and public communities are pre-configured. If additional communities are required, add them as needed. For more information, refer to [Section 5.11.5.2, “Adding an SNMP Community”](#).

## Section 5.11.5.2

## Adding an SNMP Community

To add an SNMP community, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-community** and click **<Add snmp-community>**. The **Key Settings** form appears.



The image shows the 'Key settings' form for adding an SNMP community. It features a 'Community Name' input field with a red asterisk, a help icon, and a character count '<string, min: 1 chars, max: 32 chars>'. An 'Add' button is located at the bottom right. Numbered callouts indicate: 1. Community Name Box and 2. Add Button.

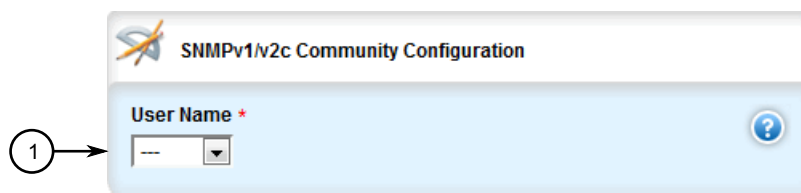
**Figure 251: Key Settings Form**

1. Community Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Community Name	<b>Synopsis:</b> A string 1 to 32 characters long The SNMP community name.

4. Click **Add** to create the protocol. The **SNMPv1/v2c Community Configuration** screen appears.



**Figure 252: SNMPv1/v2c Community Configuration Form**

1. User Name List

5. Configure the following parameter(s) as required:

Parameter	Description
User Name	The SNMP community security name.

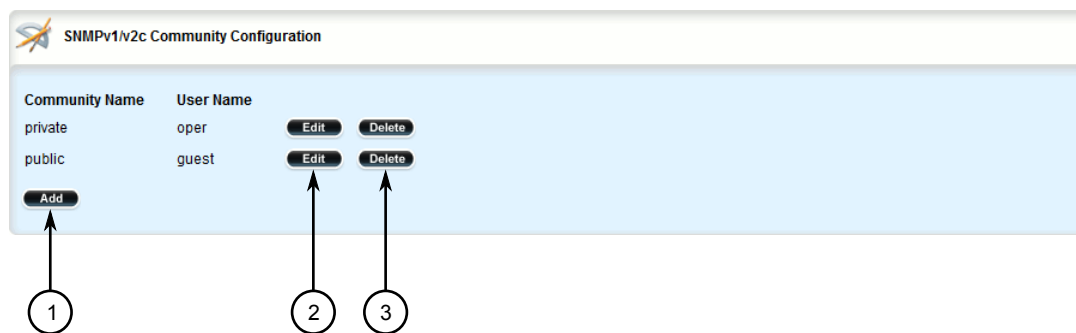
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.11.5.3

### Deleting an SNMP Community

To delete an SNMP community, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-community**. The **SNMPv1/v2c Community Configuration** table appears.



**Figure 253: SNMPv1/v2c Community Configuration Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen community.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.



## Section 5.11.6

## Managing SNMP Target Addresses

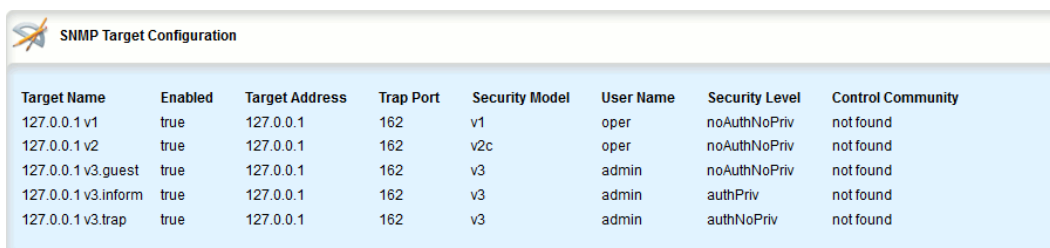
The following sections describe how to configure and manage SNMP target addresses:

- [Section 5.11.6.1, “Viewing a List of SNMP Target Addresses”](#)
- [Section 5.11.6.2, “Adding an SNMP Target Address”](#)
- [Section 5.11.6.3, “Deleting an SNMP Target Address”](#)

## Section 5.11.6.1

### Viewing a List of SNMP Target Addresses

To view a list of SNMP target addresses configured on the device, navigate to **admin » snmp » snmp-target-address**. If target addresses have been configured, the **SNMPv3 Target Configuration** table appears.



Target Name	Enabled	Target Address	Trap Port	Security Model	User Name	Security Level	Control Community
127.0.0.1 v1	true	127.0.0.1	162	v1	oper	noAuthNoPriv	not found
127.0.0.1 v2	true	127.0.0.1	162	v2c	oper	noAuthNoPriv	not found
127.0.0.1 v3.guest	true	127.0.0.1	162	v3	admin	noAuthNoPriv	not found
127.0.0.1 v3.inform	true	127.0.0.1	162	v3	admin	authPriv	not found
127.0.0.1 v3.trap	true	127.0.0.1	162	v3	admin	authNoPriv	not found

**Figure 254: SNMPv3 Target Configuration Table**

If no SNMP target addresses have been configured, add target addresses as needed. For more information, refer to [Section 5.11.6.2, “Adding an SNMP Target Address”](#).

## Section 5.11.6.2

### Adding an SNMP Target Address

To add an SNMP target address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-target-address** and click **<Add snmp-target-address>**. The **Key Settings** form appears.

**Figure 255: Key Settings Form**

1. Target Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Target Name	<b>Synopsis:</b> A string 1 to 32 characters long A descriptive name for the target (ie. 'Corportate NMS').

4. Click **Add** to create the protocol. The **SNMPv3 Target Configuration** screen appears.

The image shows the 'SNMPv3 Target Configuration' form with the following fields and their corresponding numbered callouts:

- 1:** Enabled \* (checked)
- 2:** Target Address \* (<IP address>)
- 3:** Trap Port \* (162)
- 4:** Security Model \* (v2c)
- 5:** User Name (---)
- 6:** Security Level \* (noAuthNoPriv)
- 7:** Control Community (---)
- 8:** Trap Type List \* (snmpv2\_trap selected)
- 9:** Inform Timeout \* (6000)
- 10:** Inform Retries \* (3)
- 11:** Target Engine ID \* (0)

**Figure 256: SNMPv3 Target Configuration Form**

1. Enabled Check Box   2. Target Address Box   3. Trap Port Box   4. Security Model List   5. User Name List   6. Security Level List   7. Control Community Box   8. Trap Type List Check Boxes   9. Inform Timeout Box   10. Inform Retries Box   11. Target Engine ID Box

5. Configure the following parameter(s) as required:

Parameter	Description
enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables/disables this specific target.
Target Address	<b>Synopsis:</b> A string An IPv4 or IPv6 address for the remote target.
Trap Port	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 162 The UDP Port for the remote target to receive traps on.
Security Model	<b>Synopsis:</b> { v1, v2c, v3 } <b>Default:</b> v2c The SNMP security model to use: SNMPv1, SNMPv2c, or USM/ SNMPv3.
User Name	The user name to be used in communications with this target.
Security Level	<b>Synopsis:</b> { noAuthNoPriv, authNoPriv, authPriv } <b>Default:</b> noAuthNoPriv The SNMP security level: <itemizedlist><listitem>authPriv: Communication with authentication and privacy.</listitem><listitem>authNoPriv: Communication with authentication and without privacy.</listitem> <listitem>noAuthnoPriv: Communication without authentication and privacy.</listitem></itemizedlist>
Control Community	<b>Synopsis:</b> A string 1 to 32 characters long Restricts incoming SNMP requests from the IPv4 or IPv6 address associated with this community.
Trap Type List	<b>Default:</b> snmpv2_trap Selects the type of trap communications to be sent to this target.
Inform Timeout	<b>Synopsis:</b> An integer between 0 and 2147483647 <b>Default:</b> 6000 The timeout used for reliable inform transmissions (seconds*100).
Inform Retries	<b>Synopsis:</b> An integer between 0 and 255 <b>Default:</b> 3 The number of retries used for reliable inform transmissions.
Target Engine ID	<b>Synopsis:</b> A string <b>Default:</b> Empty string The target's SNMP local engine ID. This field may be left blank.

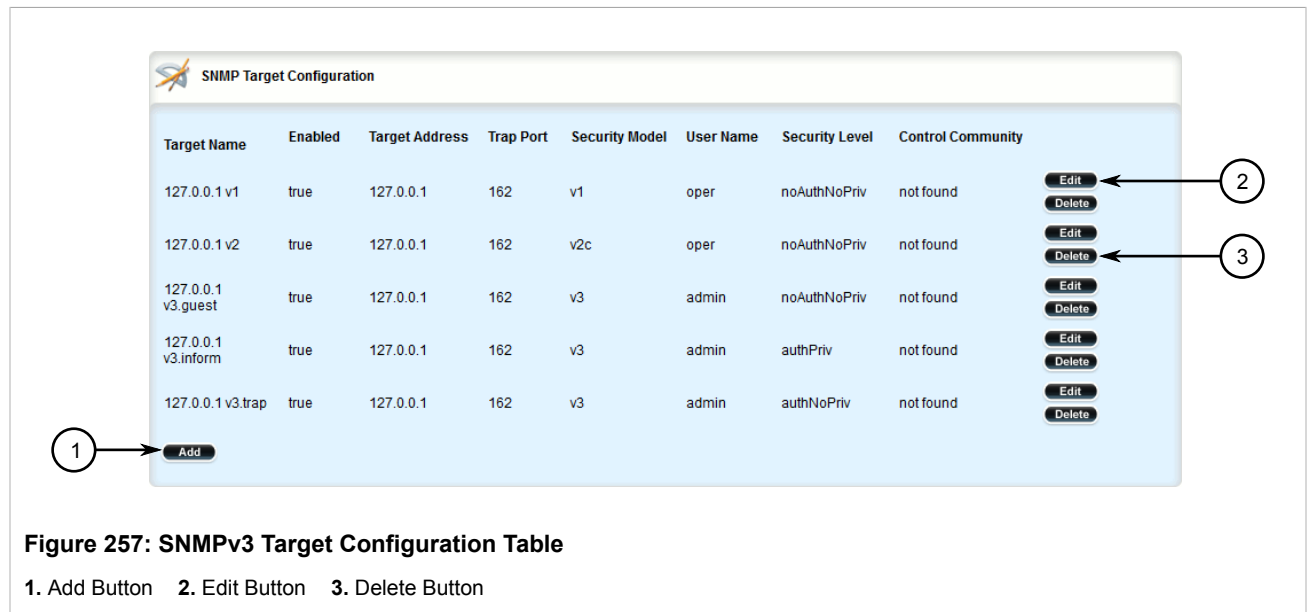
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.11.6.3

## Deleting an SNMP Target Address

To delete an SNMP target address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-target-address**. The **SNMPv3 Target Configuration** table appears.



3. Click **Delete** next to the chosen target address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.11.7

## Managing SNMP Users

The following sections describe how to configure and manage SNMP users:

- [Section 5.11.7.1, “Viewing a List of SNMP Users”](#)
- [Section 5.11.7.2, “Adding an SNMP User”](#)
- [Section 5.11.7.3, “Deleting an SNMP User”](#)

#### Section 5.11.7.1

### Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, navigate to **admin » snmp » snmp-user**. If security models have been configured, the **SNMP User Configuration** table appears.

SNMPv3 User Configuration					
User SNMP Engine ID	User Name	Authentication Protocol	Authentication Key	Privacy Protocol	Privacy Key
80:00:3a:9c:03:00:0a:dc:ff:cc:00	oper	md5	\$4\$k9pWCLM68FRwhYYI0d4IDw==	des3cbc	\$4\$ktpWCLM68FRwhYYI0d4IDw==
80:00:3a:9c:03:00:0a:dc:ff:cc:00	admin	md5	\$4\$ktpWCLM68FRwhYYI0d4IDw==	des3cbc	\$4\$ktWCLM68FRwhYYI0d4IDw==

Figure 258: SNMP User Configuration Table

If no SNMP users have been configured, add users as needed. For more information, refer to [Section 5.11.7.2, “Adding an SNMP User”](#).

Section 5.11.7.2

Adding an SNMP User

To add an SNMP user, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *admin » snmp » snmp-user* and click **<Add snmp-user>**. The **Key Settings** form appears.

The image shows a 'Key settings' form with a light blue background. At the top is a key icon and the title 'Key settings'. Below this are two fields: 'User SNMP Engine ID \*' with a text input box and a help icon, and 'User Name \*' with a dropdown menu showing 'admin' and a help icon. Below the dropdown is a small 'Add' button. Three numbered callouts are present: '1' points to the 'User SNMP Engine ID' input box, '2' points to the 'User Name' dropdown, and '3' points to the 'Add' button. Below the input box is a green text hint: '<hexList, min: 5 octets, max: 32 octets>'. The form is enclosed in a rounded rectangle.

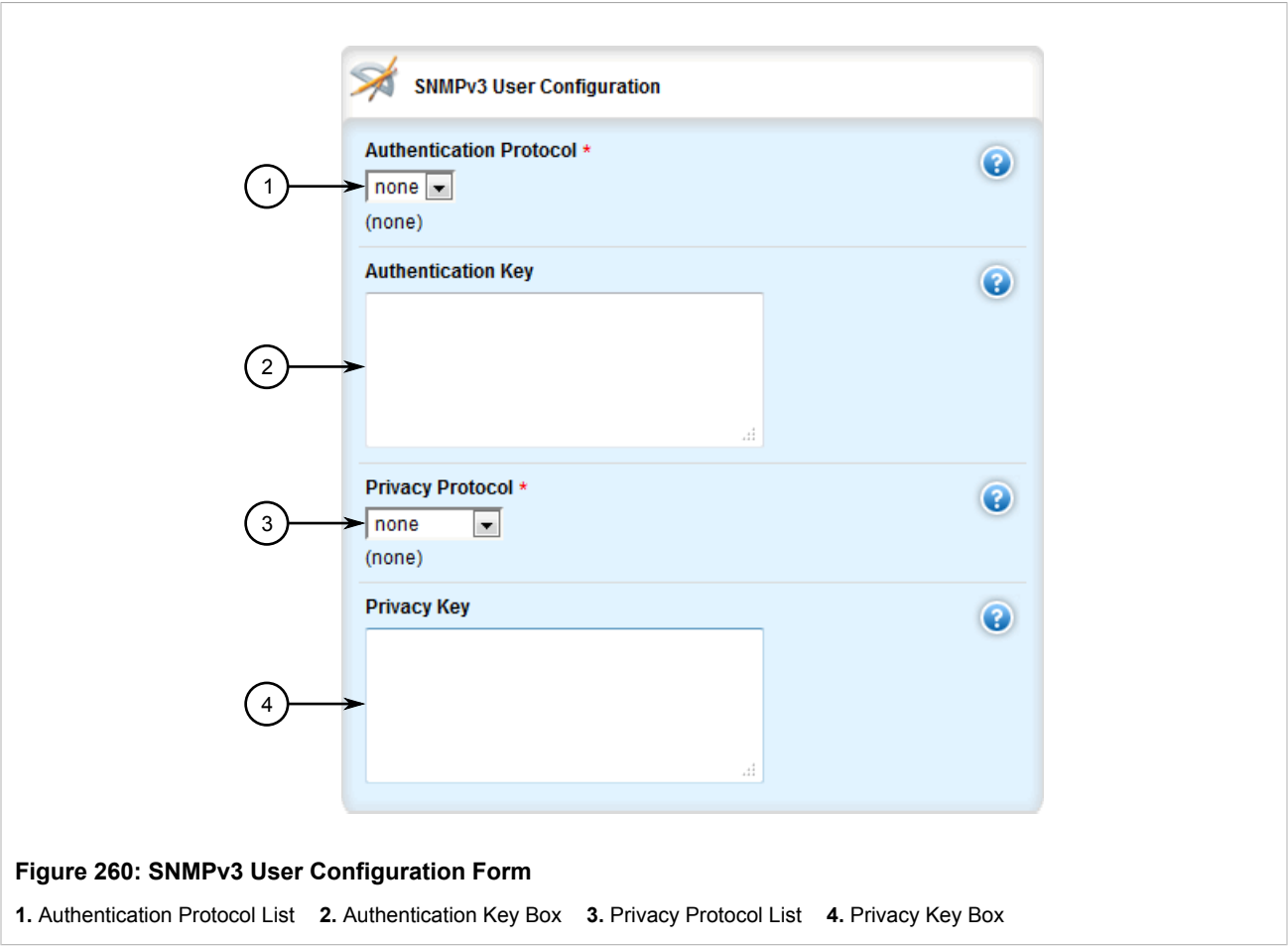
Figure 259: Key Settings Form

1. User SNMP Engine ID Box    2. User Name List    3. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
User SNMP Engine ID	<b>Synopsis:</b> A string The administratively-unique identifier for the SNMP engine; a value in the format nn:nn:nn:nn:nn:nn:nn:nn:nn:nn, where nn is a 2-digit hexadecimal number. The minimum length is 5 octets. The maximum length is 32 octets. Each octet must be separated by a colon (:).
User Name	The user for the SNMP key. Select a user name from the list.

- 4. Click **Add** to create the protocol. The **SNMPv3 User Configuration** screen appears.



5. Configure the following parameter(s) as required:

Parameter	Description
Authentication Protocol	<b>Synopsis:</b> { none, md5, sha1 } <b>Default:</b> none The authentication protocol providing data integrity and authentication for SNMP exchanges between the user and the SNMP engine.
Authentication Key	<b>Synopsis:</b> A string A free-text password in the format <code>&lt;code&gt;\$0\$&lt;your password&gt;&lt;/code&gt;</code> . passphrase must be minimum 8 characters long
Privacy Protocol	<b>Synopsis:</b> { none, des3cbc, aescfb128 } <b>Default:</b> none The symmetric privacy protocol providing data encryption and decryption for SNMP exchanges between the user and the SNMP engine.
Privacy Key	<b>Synopsis:</b> A string A free-text password in the format <code>&lt;code&gt;\$0\$&lt;your password&gt;&lt;/code&gt;</code> . passphrase must be minimum 8 characters long

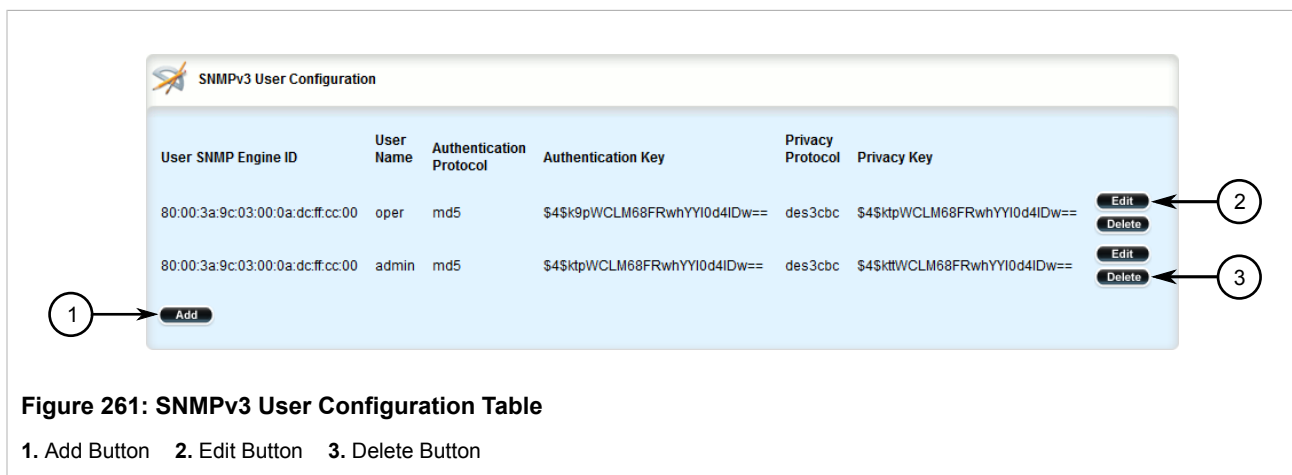
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.11.7.3

## Deleting an SNMP User

To delete an SNMP user, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-user**. The **SNMPv3 User Configuration** table appears.



**SNMPv3 User Configuration**

User SNMP Engine ID	User Name	Authentication Protocol	Authentication Key	Privacy Protocol	Privacy Key	
80:00:3a:9c:03:00:0a:dc:ff:cc:00	oper	md5	\$4\$k9pWCLM68FRwhYYI0d4IDw==	des3cbc	\$4\$ktpWCLM68FRwhYYI0d4IDw==	<div>1 → Add</div> <div>Edit</div> <div>Delete</div> <div>2</div>
80:00:3a:9c:03:00:0a:dc:ff:cc:00	admin	md5	\$4\$ktpWCLM68FRwhYYI0d4IDw==	des3cbc	\$4\$kttWCLM68FRwhYYI0d4IDw==	<div>Edit</div> <div>Delete</div> <div>3</div>

**Figure 261: SNMPv3 User Configuration Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen user.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.11.8

## Managing SNMP Security Model Mapping

The following sections describe how to configure and manage SNMP security models:

- [Section 5.11.8.1, “Viewing a List of SNMP Security Models”](#)
- [Section 5.11.8.2, “Adding an SNMP Security Model”](#)
- [Section 5.11.8.3, “Deleting an SNMP Security Model”](#)

### Section 5.11.8.1

## Viewing a List of SNMP Security Models

To view a list of SNMP security models configured on the device, navigate to **admin » snmp » snmp-security-to-group**. If security models have been configured, the **SNMP Security Model to Group Mapping** table appears.



SNMP Security Model to Group Mapping		
Security Model	User Name	Group
v1	oper	all-rights
v1	guest	all-rights
v2c	oper	all-rights
v2c	guest	all-rights
v3	admin	initial

Figure 262: SNMP Security Model to Group Mapping Table

If no SNMP security models have been configured, add security models as needed. For more information, refer to [Section 5.11.8.2, “Adding an SNMP Security Model”](#).

Section 5.11.8.2

Adding an SNMP Security Model

To add an SNMP security model, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *admin » snmp » snmp-security-to-group* and click **<Add snmp-security-to-group>**. The **Key Settings** form appears.

Key settings

1

Security Model \*

v3

2

User Name \*

admin

3

Add

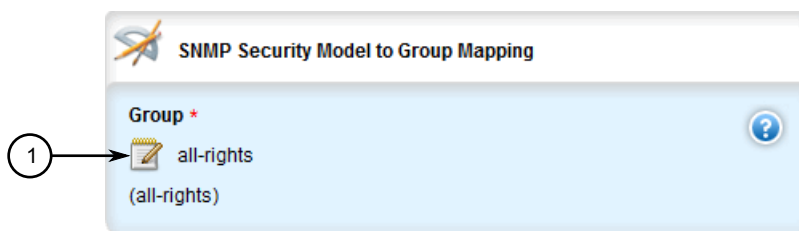
Figure 263: Key Settings Form

1. Security Model List    2. User Name List    3. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
Security Model	<b>Synopsis:</b> { v1, v2c, v3 } The SNMP security model to use: SNMPv1, SNMPv2c, or USM/ SNMPv3.
User Name	The security name (a ROX user name) for the SNMP group.

- 4. Click **Add** to create the protocol. The **SNMP Security Model to Group Mapping** screen appears.



**Figure 264: SNMP Security Model to Group Mapping Form**

1. Group Box

5. Configure the following parameter(s) as required:

Parameter	Description
Group	<b>Synopsis:</b> A string 1 to 32 characters long <b>Default:</b> all-rights The name of the SNMP group.

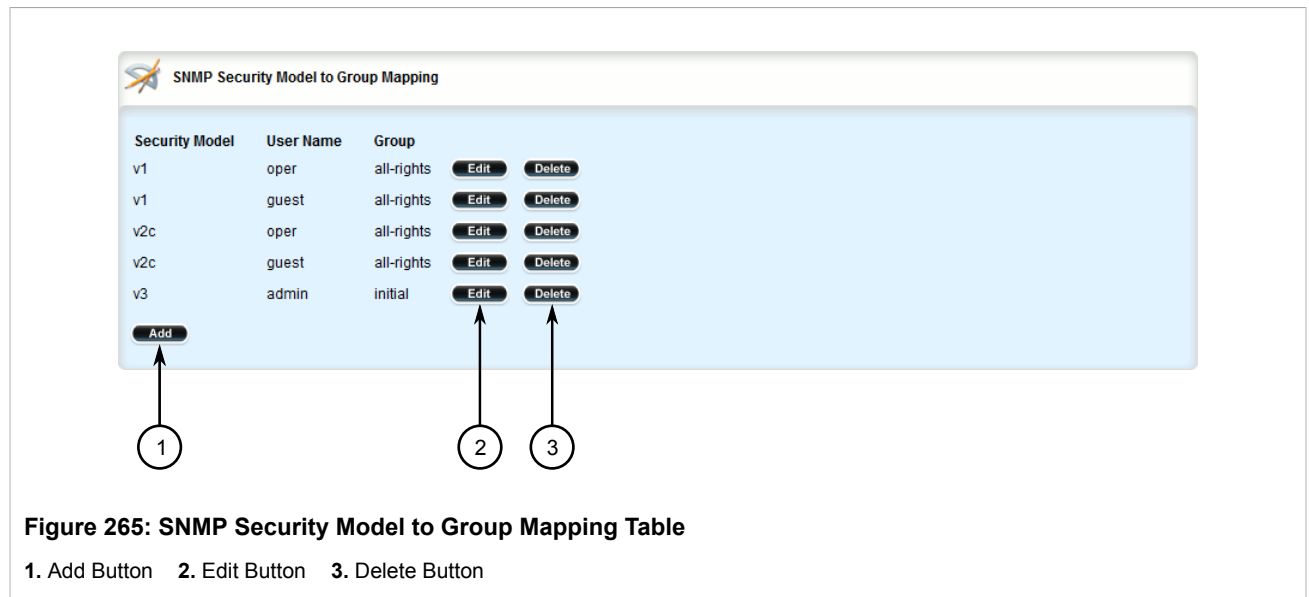
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.11.8.3

## Deleting an SNMP Security Model

To delete an SNMP security model, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-security-to-group**. The **SNMP Security Model to Group Mapping** table appears.



3. Click **Delete** next to the chosen security model.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.11.9

## Managing SNMP Group Access

The following sections describe how to configure and manage SNMP group access:

- [Section 5.11.9.1, “Viewing a List of SNMP Groups”](#)
- [Section 5.11.9.2, “Adding an SNMP Group”](#)
- [Section 5.11.9.3, “Deleting an SNMP Group”](#)

#### Section 5.11.9.1

### Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, navigate to **admin » snmp » snmp-access**. If groups have been configured, the **SNMP Group Access Configuration** table appears.

Group	Security Model	Security Level	Read View Name	Write View Name	Notify 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
all-rights	any	noAuthNoPriv	all-of-mib	all-of-mib	all-of-mib

**Figure 266: SNMP Group Access Configuration Table**

If no SNMP groups have been configured, add groups as needed. For more information, refer to [Section 5.11.9.2, “Adding an SNMP Group”](#).

### Section 5.11.9.2

## Adding an SNMP Group

To add an SNMP group, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-access** and click **<Add snmp-access>**. The **Key Settings** form appears.

**Key settings**

1. **Group \***  <string, min: 1 chars, max: 32 chars> (all-rights)

2. **Security Model \*** v3 (any)

3. **Security Level \*** authPriv (noAuthNoPriv)

4. **Add**

**Figure 267: Key Settings Form**

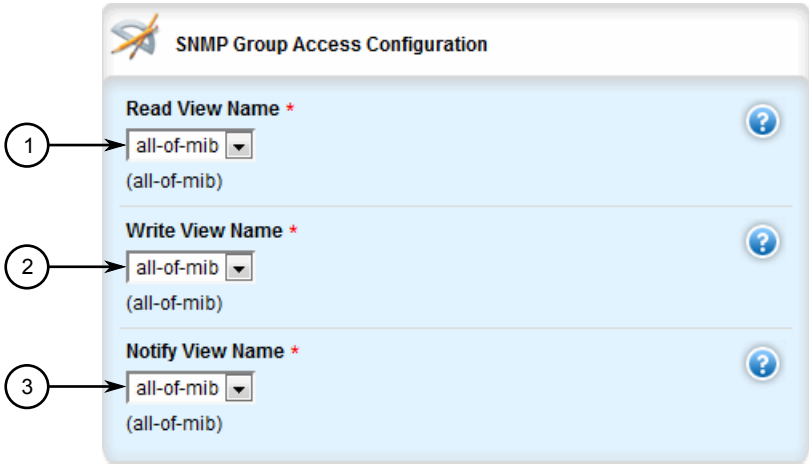
1. Group Box   2. Security Model List   3. Security Level List   4. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Group	<b>Synopsis:</b> A string 1 to 32 characters long

Parameter	Description
	The name of the SNMP group.
Security Model	<b>Synopsis:</b> { any, v1, v2c, v3 } The SNMP security model to use: SNMPv1, SNMPv2c, or USM/ SNMPv3.
Security Level	<b>Synopsis:</b> { noAuthNoPriv, authNoPriv, authPriv } The SNMP security level: <itemizedlist><listitem>authPriv: Communication with authentication and privacy.</listitem><listitem>authNoPriv: Communication with authentication and without privacy.</listitem><listitem>noAuthnoPriv: Communication without authentication and privacy.</listitem></itemizedlist>

- Click **Add** to create the protocol. The **SNMP Group Access Configuration** screen appears.



The image shows the 'SNMP Group Access Configuration' form. It has three sections, each with a dropdown menu and a help icon (blue circle with a question mark). The sections are: 'Read View Name \*' with a dropdown showing 'all-of-mib' and '(all-of-mib)' below it; 'Write View Name \*' with a dropdown showing 'all-of-mib' and '(all-of-mib)' below it; and 'Notify View Name \*' with a dropdown showing 'all-of-mib' and '(all-of-mib)' below it. Three numbered circles (1, 2, 3) are on the left, with arrows pointing to the first, second, and third dropdown menus respectively.

**Figure 268: SNMP Group Access Configuration Form**

1. Read View Name List    2. Write View Name List    3. Notify View Name List

- Configure the following parameter(s) as required:

Parameter	Description
Read View Name	<b>Synopsis:</b> { no-view, v1-mib, restricted, all-of-mib } <b>Default:</b> all-of-mib The name of the read view to which the SNMP group has access: all-of-mib, restricted, v1-mib, or no-view.
Write View Name	<b>Synopsis:</b> { no-view, v1-mib, restricted, all-of-mib } <b>Default:</b> all-of-mib The name of the write view to which the SNMP group has access: all-of-mib, restricted, v1-mib, or no-view.
Notify View Name	<b>Synopsis:</b> { no-view, v1-mib, restricted, all-of-mib } <b>Default:</b> all-of-mib The name of the notification view to which the SNMP group has access: all-of-mib, restricted, v1-mib, or no-view.

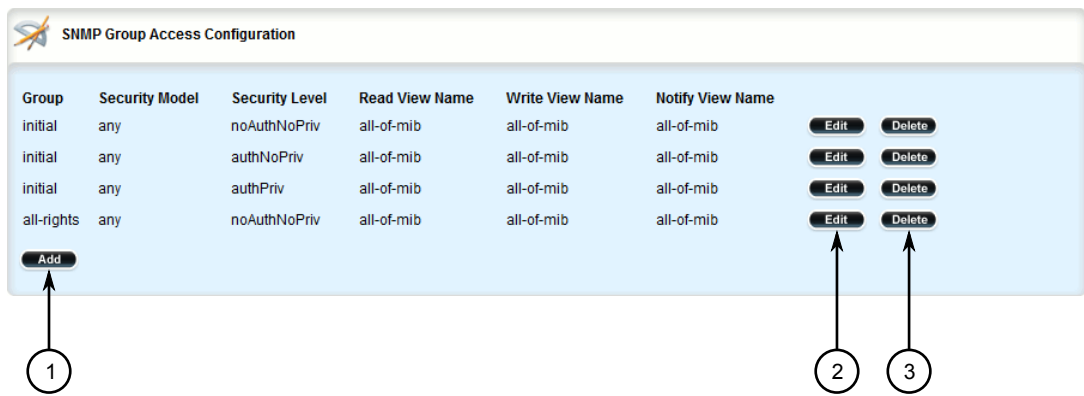
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.11.9.3

## Deleting an SNMP Group

To delete an SNMP group, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » snmp » snmp-group**. The **SNMP Group Access Configuration** table appears.



Group	Security Model	Security Level	Read View Name	Write View Name	Notify View Name		
initial	any	noAuthNoPriv	all-of-mib	all-of-mib	all-of-mib	Edit	Delete
initial	any	authNoPriv	all-of-mib	all-of-mib	all-of-mib	Edit	Delete
initial	any	authPriv	all-of-mib	all-of-mib	all-of-mib	Edit	Delete
all-rights	any	noAuthNoPriv	all-of-mib	all-of-mib	all-of-mib	Edit	Delete

**Figure 269: SNMP Group Access Configuration Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen group.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.12

## Managing Time Synchronization Functions

RUGGEDCOM ROX II uses version 4 of the Network Time Protocol (NTP) to synchronize the internal clock with a time source.



#### NOTE

For more information about version 4 of NTP, refer to [RFC 5905](http://tools.ietf.org/html/rfc5905) [<http://tools.ietf.org/html/rfc5905>].

NTP is a fault-tolerant protocol that allows an NTP daemon to automatically select the best of several available reference clocks to synchronize with. Multiple candidates can be combined to minimize the accumulated error. The NTP daemon can also detect and avoid reference clocks that are temporarily or permanently advertising the wrong time.

The NTP daemon achieves synchronization by making small and frequent changes to the internal clock. It operates in a *client-server* mode, which allows it to synchronize the internal clock with NTP servers and act as an NTP server for peer devices.

If multiple NTP servers are available to choose from, the NTP daemon will synchronize with the server that has the lowest stratum. The stratum is a rating of the server compared to the server with the reference clock. The reference clock itself appears at stratum 0. A server synchronized with a stratum  $n$  server will be running at stratum  $n+1$ .

NTP hosts with a lower stratum are typically configured as NTP servers, while NTP hosts with higher stratum are configured at the same stratum as their peers. If each NTP server fails, a configured peer will help in providing the NTP time. It is recommended that at least one server and one peer be configured.

The NTP daemon knows which NTP servers and peers to use in three ways:

- The daemon is configured manually with list of servers to poll
- The daemon is configured manually with a list of peers to send to
- NTP servers issue advertisements to the daemon on broadcast or multicast address

**NOTE**

*If a firewall is enabled, make sure UDP port 123 is open to send (if the router is an NTP client) or receive (if the router is an NTP server).*

NTP uses UDP/IP packets for data transfer, as UDP offers fast connections and response times, and transfers them through UDP port 123.

The following sections describe how to configure and manage time synchronization functions:

- [Section 5.12.1, “Configuring the Time Synchronization Settings”](#)
- [Section 5.12.2, “Configuring the System Time and Date”](#)
- [Section 5.12.3, “Configuring the System Time Zone”](#)
- [Section 5.12.4, “Configuring the Local Time Settings”](#)
- [Section 5.12.5, “Configuring NTP Multicast Clients”](#)
- [Section 5.12.6, “Configuring NTP Broadcast Clients”](#)
- [Section 5.12.7, “Enabling/Disabling the NTP Service”](#)
- [Section 5.12.8, “Viewing the NTP Service Status”](#)
- [Section 5.12.9, “Viewing the Status of Reference Clocks”](#)
- [Section 5.12.10, “Monitoring Subscribers”](#)
- [Section 5.12.11, “Managing NTP Servers”](#)
- [Section 5.12.12, “Managing NTP Broadcast/Multicast Addresses”](#)
- [Section 5.12.13, “Managing Server Keys”](#)
- [Section 5.12.14, “Managing Server Restrictions”](#)

## Section 5.12.1

## 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 5.12.2, “Configuring the System Time and Date”](#).

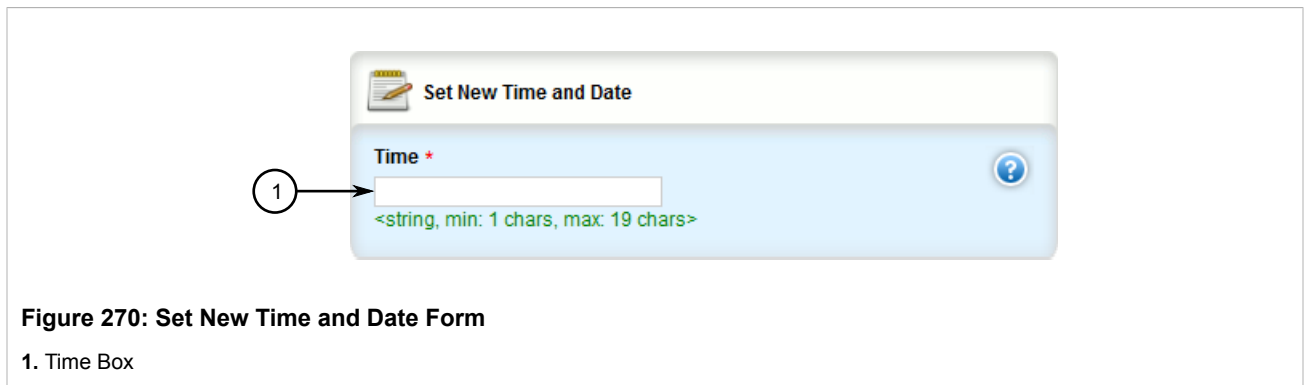
2. Configure the system time zone. For more information, refer to [Section 5.12.3, “Configuring the System Time Zone”](#).
3. Configure the local time settings. For more information, refer to [Section 5.12.4, “Configuring the Local Time Settings”](#).
4. If multicast addresses will be configured for the NTP server, configure the NTP multicast client. For more information, refer to [Section 5.12.5, “Configuring NTP Multicast Clients”](#).
5. If broadcast addresses will be configured for the NTP server, configure the NTP broadcast client. For more information, refer to [Section 5.12.6, “Configuring NTP Broadcast Clients”](#).
6. Add remote NTP servers. For more information, refer to [Section 5.12.11.2, “Adding an NTP Server”](#).
7. Add broadcast/multicast addresses for the NTP server. For more information, refer to [Section 5.12.12.2, “Adding a Broadcast/Multicast Address”](#).
8. If required, add server authentication keys. For more information, refer to [Section 5.12.13.2, “Adding a Server Key”](#).
9. Add restrictions for the remote NTP servers. For more information, refer to [Section 5.12.14.2, “Adding a Server Restriction”](#).
10. Enable the NTP service. For more information, refer to [Section 5.12.7, “Enabling/Disabling the NTP Service”](#).
11. View the status of the NTP service. For more information, refer to [Section 5.12.8, “Viewing the NTP Service Status”](#).

#### Section 5.12.2

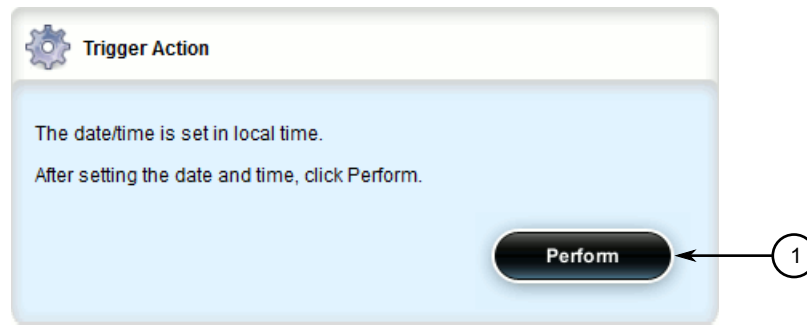
## Configuring the System Time and Date

To configure the system time and date, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin** and click **set-system-clock** in the menu. The **Set New Time and Date** and **Trigger Action** forms appear.







**Figure 271: Trigger Action Form**

1. Perform Button

- On the **Set New Time and Date** form, configure the following parameter(s) as required:

Parameter	Description
time	<p><b>Synopsis:</b> A string 1 to 19 characters long</p> <p>Enter the date and time in the format &lt;phrase userlevel="CLI"&gt;"&lt;/phrase&gt;YYYY-MM-DD HH:MM:SS&lt;phrase userlevel="CLI"&gt;"&lt;/phrase&gt;.</p>

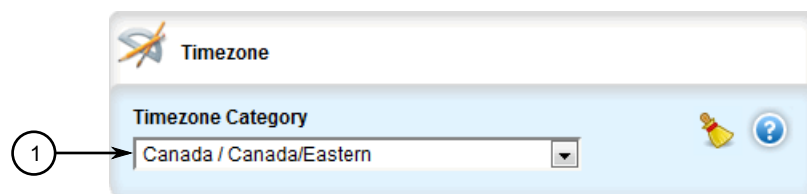
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.12.3

## Configuring the System Time Zone

To configure the system time zone, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **admin**. The **Timezone** form appears.



**Figure 272: Timezone Form**

1. Timezone Category Box

- Configure the following parameter(s) as required:

Parameter	Description
Timezone Category	Selects the time zone. Note that the Etc/GMT time zones conform to the POSIX style and have their signs reversed from common usage. In POSIX style, zones west of GMT have a positive sign; zones east of GMT have a negative sign.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

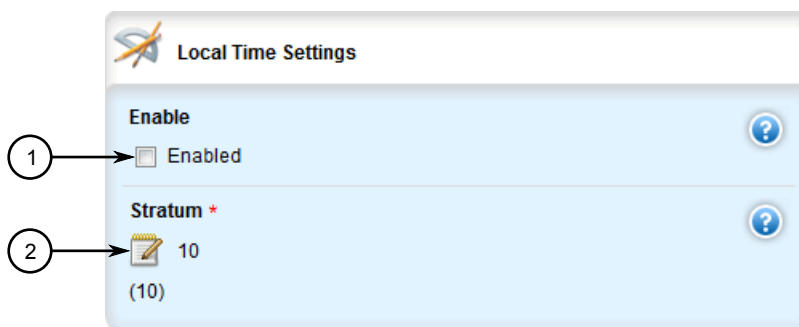
## Section 5.12.4

## 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:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » time » ntp**. The **Local Time Settings** form appears.



**Figure 273: Local Time Settings Form**

1. Enable Check Box    2. Stratum Box

- Configure the following parameter(s) as required:

Parameter	Description
Enable	<b>Synopsis:</b> typeless Enables the local clock. The NTP daemon will use the local clock as the NTP source. The stratum number (of 10) indicates the priority relative to other sources.
Stratum	<b>Synopsis:</b> An integer between 0 and 15 <b>Default:</b> 10 The stratum number of the local clock.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.12.5

## Configuring NTP Multicast Clients

The NTP multicast client enables the NTP server to receive advertisements from other NTP servers.

To configure the NTP multicast client, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp**. The **NTP Multicast Clients** form appears.

The screenshot shows the 'NTP Multicast Clients' configuration form. It features a title bar with an icon and the text 'NTP Multicast Clients'. Below the title bar, there is a section 'Enable Multicast Client' with a checkbox labeled 'Enabled'. A circled number '1' points to this checkbox. Below this, there is a section 'Address \*' with a text input field containing '224.0.1.1' and '(224.0.1.1)' below it. A circled number '2' points to the input field. There are help icons (question marks in circles) next to both sections.

**Figure 274: NTP Multicast Clients Form**

1. Enable Multicast Client Check Box    2. Address Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable Multicast Client	<b>Synopsis:</b> typeless Enables the multicast message mode.
Address	<b>Synopsis:</b> A string <b>Default:</b> 224.0.1.1 The multicast address on which the NTP client listens for NTP messages.

4. Add a multicast address for a known NTP server. For more information, refer to [Section 5.12.12.2, “Adding a Broadcast/Multicast Address”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

## Section 5.12.6

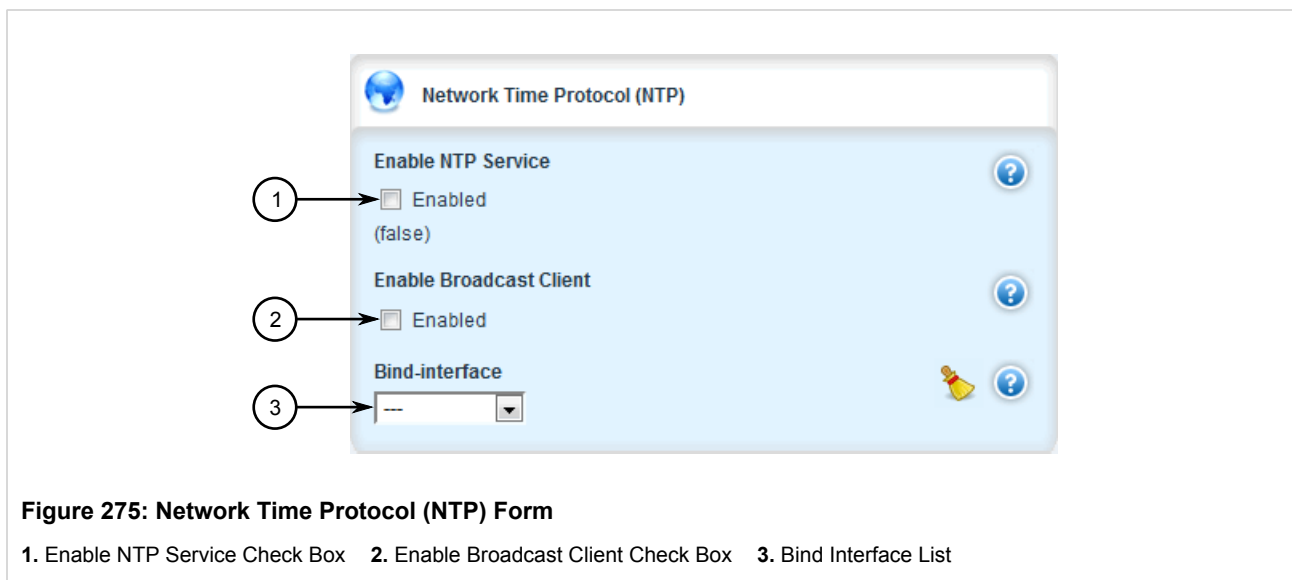
## Configuring NTP Broadcast Clients

The NTP broadcast client enables the NTP server to receive advertisements from other NTP servers and send advertisements of its own.

To configure the NTP broadcast client, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

- Navigate to **services » time » ntp**. The **Network Time Protocol (NTP)** form appears.



- Configure the following parameters as required:

Parameter	Description
Enable Broadcast Client	<b>Synopsis:</b> typeless Enables/disables the broadcast client.
Bind Interface	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.

- Add a broadcast address for a known NTP server. For more information, refer to [Section 5.12.12.2, “Adding a Broadcast/Multicast Address”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.12.7

## Enabling/Disabling the NTP Service

To enable/disable the NTP service, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » time » ntp**. The **Network Time Protocol (NTP)** form appears.

**Figure 276: Network Time Protocol (NTP) Form**

1. Enable NTP Service Check Box    2. Enable Broadcast Client Check Box

3. Select the **Enable NTP Service** check box to enable the NTP service, or clear the check box to disable the service.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.12.8

## Viewing the NTP Service Status

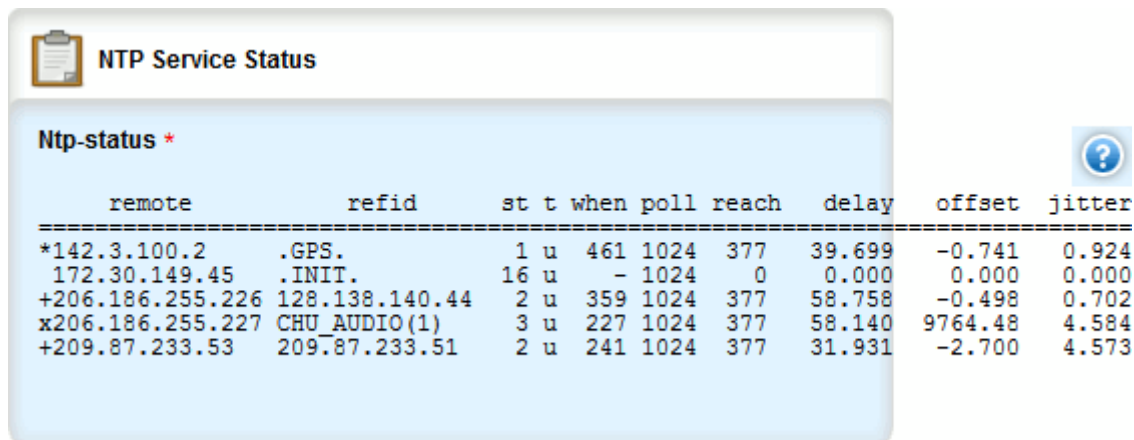
To view the status of the NTP service, do the following:

1. Make sure the NTP service is enabled. For more information, refer to [Section 5.12.7, “Enabling/Disabling the NTP Service”](#).
2. Navigate to **services » time » ntp** and click **ntp-status** in the menu. The **Trigger Action** form appears.

**Figure 277: Trigger Action Form**

1. Perform Button

3. Click **Perform**. The **NTP Service Status** form appears.



The image shows a screenshot of the 'NTP Service Status' form in a web interface. At the top, there is a clipboard icon and the title 'NTP Service Status'. Below the title, the text 'Ntp-status \*' is displayed. A table of NTP service status data is shown, with columns for remote, refid, st, t, when, poll, reach, delay, offset, and jitter. The data rows are as follows:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*142.3.100.2	.GPS.	1	u	461	1024	377	39.699	-0.741	0.924
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	359	1024	377	58.758	-0.498	0.702
x206.186.255.227	CHU_AUDIO(1)	3	u	227	1024	377	58.140	9764.48	4.584
+209.87.233.53	209.87.233.51	2	u	241	1024	377	31.931	-2.700	4.573

Figure 278: NTP Service Status Form

This form provides the following information:

Parameter	Description
NTP Service Status	Use this action to get the current NTP running status.


A character before an address is referred to as a tally code. Tally codes indicate the fate of the peer in the clock selection process. The following describes the meaning of each tally code:

Tally Code	Description
blank	A blank tally code indicates the peer has been discarded either because it is unreachable, it is synchronized to the same server (synch loop) or the synchronization distance is too far.
x	This tally code indicates the peer has been discarded because its clock is not correct. This is referred to as a <i>false-ticker</i> .
.	This tally code indicates the peer has been discarded because its synchronization distance is too poor to be considered a candidate.
-	This tally code indicates the peer has been discarded because its offset is too significant compared to the other peers. This is referred to as an <i>outlier</i> .
+	This tally code indicates the peer is considered a candidate.
#	This tally code indicates the peer is considered a candidate, but it is not among the top six sorted by synchronization distance. If the association is short-lived, it may be demobilized to conserve resources.
*	This tally code indicates the peer is the system peer.
o	This tally code indicates the peer is the system peer, but the synchronization distance is derived from a Pulse-Per-Second (PPS) signal.

#### Section 5.12.9

## Viewing the Status of Reference Clocks

To view the status of reference clocks, navigate to **services » time » ntp » status » reference-clocks**. The **Reference Clock** table appears.



Remote IP	State	RefId	Stratum	Address type	When	Poll	Reach
127.127.1.0	System peer	.LOCL.	10	I	54	64	377
206.186.255.227	Not synchronized	.INIT.	16	-	-	1024	0
206.186.255.226	Not synchronized	.INIT.	16	-	-	1024	0
142.3.100.2	Not synchronized	.INIT.	16	-	-	1024	0

**Figure 279: Reference Clock Table**

This table provides the following information:

Parameter	Description
Remote IP	<b>Synopsis:</b> A string 1 to 40 characters long The IP address of the reference clock.
State	<b>Synopsis:</b> A string 1 to 32 characters long The state of the clock.
RefId	<b>Synopsis:</b> A string 1 to 40 characters long The identification of the reference clock.
Stratum	<b>Synopsis:</b> A string 1 to 32 characters long The stratum number of the reference clock.
Address type	<b>Synopsis:</b> A string 1 to 32 characters long The address type of the remote machine.
When	<b>Synopsis:</b> A string 1 to 32 characters long The number of seconds since the last poll of the reference clock.
Poll	<b>Synopsis:</b> A string 1 to 32 characters long The polling interval in seconds.
Reach	<b>Synopsis:</b> A string 1 to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
Delay	<b>Synopsis:</b> A string 1 to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
Offset	<b>Synopsis:</b> A string 1 to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
Jitter	<b>Synopsis:</b> A string 1 to 32 characters long The observed jitter (in milliseconds).

#### Section 5.12.10

## 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. However, the command used to display the list is only available in the CLI. For more information about how to monitor hosts that have subscribed to the NTP service, refer to the *RUGGEDCOM ROX II v2.9 User Guide*.

Section 5.12.11

# 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 5.12.13.2, “Adding a Server Key”](#).

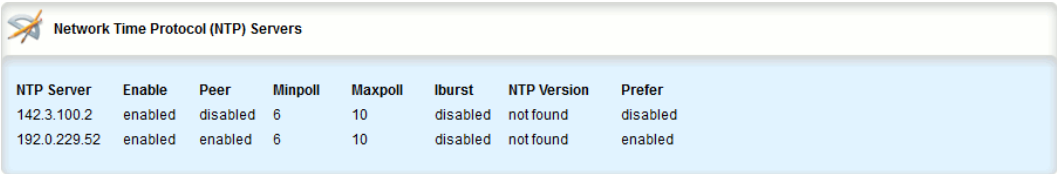
The following sections describe how to configure and manage NTP servers:

- [Section 5.12.11.1, “Viewing a List of NTP Servers”](#)
- [Section 5.12.11.2, “Adding an NTP Server”](#)
- [Section 5.12.11.3, “Deleting an NTP Server”](#)

Section 5.12.11.1

## Viewing a List of NTP Servers

To view a list of NTP servers configured on the device, navigate to **services » time » ntp » server**. If servers have been configured, the **Network Time Protocol (NTP) Servers** table appears.



NTP Server	Enable	Peer	Minpoll	Maxpoll	Iburst	NTP Version	Prefer
142.3.100.2	enabled	disabled	6	10	disabled	not found	disabled
192.0.229.52	enabled	enabled	6	10	disabled	not found	enabled

Figure 280: Network Time Protocol (NTP) Servers Table

If no servers have been configured, add servers as needed. For more information, refer to [Section 5.12.11.2, “Adding an NTP Server”](#).

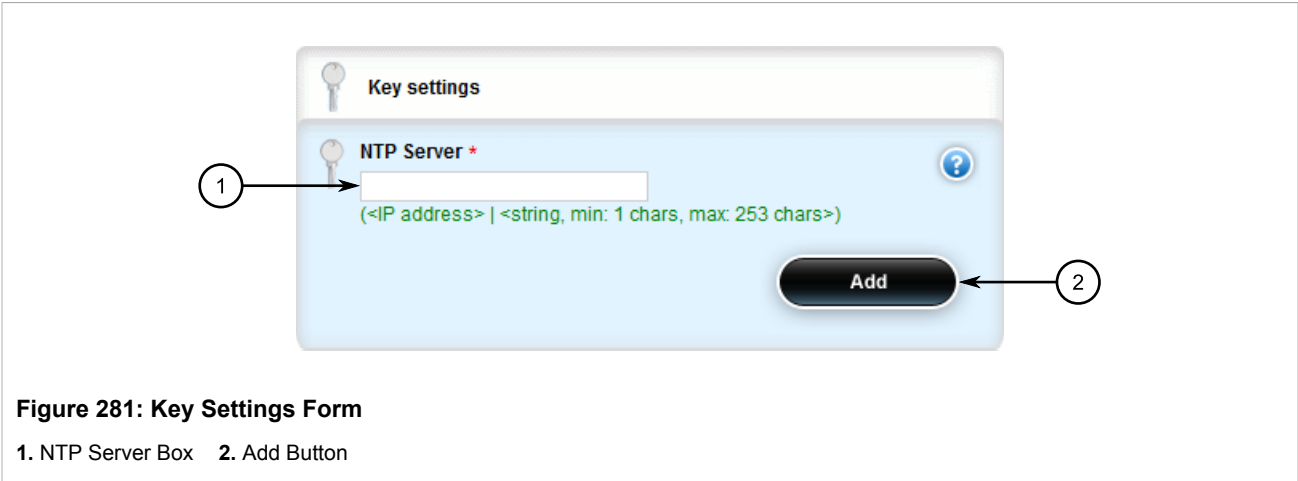
Section 5.12.11.2

## Adding an NTP Server

To configure an NTP server on the device, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp » server** and click **<Add server>**. The **Key Settings** form appears.





3. Configure the following parameter(s) as required:

Parameter	Description
NTP Server	<b>Synopsis:</b> A string The Internet address of the remote NTP server to be monitored.

4. Click **Add** to create the server configuration. The **Network Time Protocol (NTP) Servers** form appears.

**Figure 282: Network Time Protocol (NTP) Servers Form**

1. Enable Check Box   2. Peer Check Box   3. Mini Poll Box   4. Max Poll Box   5. IBurst Check Box   6. NTP Version Box  
7. Prefer Check Box   8. Key List

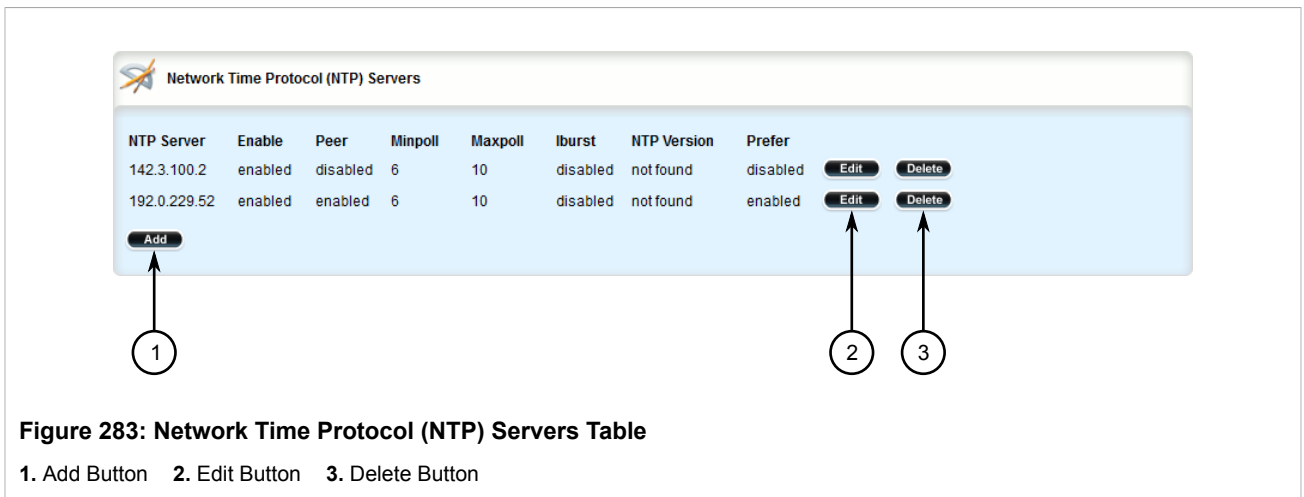
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 5.12.11.3

### Deleting an NTP Server

To delete an NTP server configured on the device, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp » server**. The **Network Time Protocol (NTP) Servers** table appears.



3. Click **Delete** next to the chosen server.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.12.12

## 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.

The following sections describe how to configure and manage broadcast and multicast addresses for an NTP server:

- [Section 5.12.12.1, “Viewing a List of Broadcast/Multicast Addresses”](#)
- [Section 5.12.12.2, “Adding a Broadcast/Multicast Address”](#)
- [Section 5.12.12.3, “Deleting a Broadcast/Multicast Address”](#)

## Section 5.12.12.1

### Viewing a List of Broadcast/Multicast Addresses

To view a list of broadcast/multicast addresses for an NTP server, navigate to **services » time » ntp » broadcast**. If addresses have been configured, the **NTP Broadcast/Multicast Servers** table appears.

Broadcast/Multicast IP Address	Enable	Key	NTP Version	Time To Live
224.0.0.1	disabled	not found	not found	1

Figure 284: NTP Broadcast/Multicast Servers Table

If no broadcast/multicast addresses have been configured, add addresses as needed. For more information, refer to [Section 5.12.12.2, “Adding a Broadcast/Multicast Address”](#).

## Section 5.12.12.2

# 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. If necessary, make sure a server authentication key has been configured with the broadcast/multicast setting to enable NTP authentication. For more information, refer to [Section 5.12.13.2, “Adding a Server Key”](#).
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to **services » time » ntp » broadcast** and click **<Add broadcast>**. The **Key Settings** form appears.

**Figure 285: Key Settings Form**

1. Broadcast/Multicast IP Address Box    2. Add Button

4. Configure the following parameter(s) as required:



### IMPORTANT!

*The broadcast/multicast address must be the same as the address for the NTP multicast client.*

Parameter	Description
Broadcast/Multicast IP Address	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long The broadcast or multicast address.

5. Click **Add** to create the new address. The **NTP Broadcast/Multicast Servers** form appears.

**Figure 286: NTP Broadcast/Multicast Servers Form**

1. Enable Check Box   2. Key List   3. NTP Version Box   4. Time to Live Box

6. Configure the following parameter(s) as required:

Parameter	Description
Enable	<b>Synopsis:</b> typeless Enables sending broadcast or multicast NTP messages to this address.
Key	Authentication key.
NTP Version	<b>Synopsis:</b> An integer between 1 and 4 The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
Time To Live	<b>Synopsis:</b> An integer between 1 and 127 <b>Default:</b> 1 Time to live.

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.12.12.3

## Deleting a Broadcast/Multicast Address

To delete a broadcast/multicast address for an NTP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp » broadcast**. The **NTP Broadcast/Multicast Servers** table appears.

Broadcast/Multicast IP Address	Enable	Key	NTP Version	Time To Live
224.0.0.1	disabled	not found	not found	1

Buttons: Add, Edit, Delete

Annotations: 1 points to Add, 2 points to Edit, 3 points to Delete

**Figure 287: NTP Broadcast/Multicast Servers Table**

1. Add Button   2. Edit Button   3. Delete Button

3. Click **Delete** next to the chosen address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.12.13

## 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.

The following sections describe how to configure and manage server keys:

- [Section 5.12.13.1, “Viewing a List of Server Keys”](#)
- [Section 5.12.13.2, “Adding a Server Key”](#)
- [Section 5.12.13.3, “Deleting a Server Key”](#)

#### Section 5.12.13.1

### Viewing a List of Server Keys

To view a list of server keys, navigate to **services » time » ntp » key**. If keys have been configured, the **Server Keys** table appears.

Key ID	Key	Trusted
1	\$4\$87sRTIZ+sxs9hYYI0d4IDw==	enabled

**Figure 288: Server Keys Table**

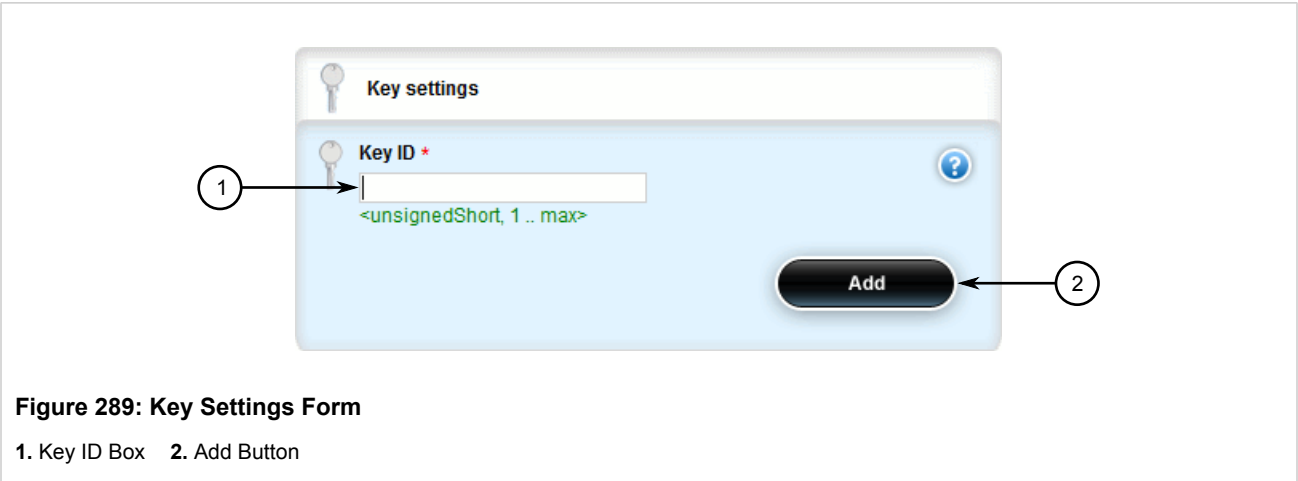
If no server keys have been configured, add keys as needed. For more information, refer to [Section 5.12.13.2, “Adding a Server Key”](#).

Section 5.12.13.2

Adding a Server Key

To add a server key, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to **services » time » ntp » key** and click **<Add key>**. The **Key Settings** form appears.



- 3. Configure the following parameter(s) as required:

Parameter	Description
Key ID	<b>Synopsis:</b> An integer The name of the key.

- 4. Click **Add** to create the new key. The **Server Keys** form appears.

**Figure 290: Server Keys Form**

1. Key Box 2. Trusted Check Box

5. Configure the following parameter(s) as required:

Parameter	Description
Key	<b>Synopsis:</b> A string The key.
Trusted	<b>Synopsis:</b> typeless 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.

6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

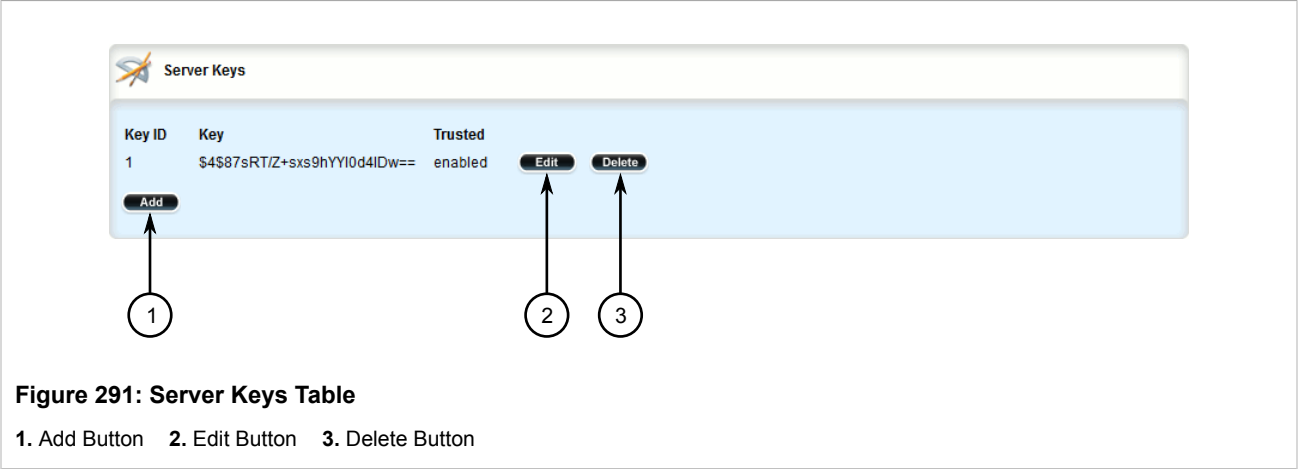
#### Section 5.12.13.3

### Deleting a Server Key

To delete a server key, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp » key**. The **Server Keys** table appears.





- 3. Click **Delete** next to the chosen key.
- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

Section 5.12.14

## Managing Server Restrictions

- Server restrictions control access to the NTP servers.
- The following sections describe how to configure and manage NTP server restrictions:
- [Section 5.12.14.1, “Viewing a List of Server Restrictions”](#)
  - [Section 5.12.14.2, “Adding a Server Restriction”](#)
  - [Section 5.12.14.3, “Deleting a Server Restriction”](#)

Section 5.12.14.1

### Viewing a List of Server Restrictions

To view a list of NTP server restrictions, navigate to **services » time » ntp » restrict**. If restrictions have been configured, the **Server Restrictions** table appears.

Address	Mask	Flags
127.0.0.1	default	not found

Figure 292: Server Restrictions Table

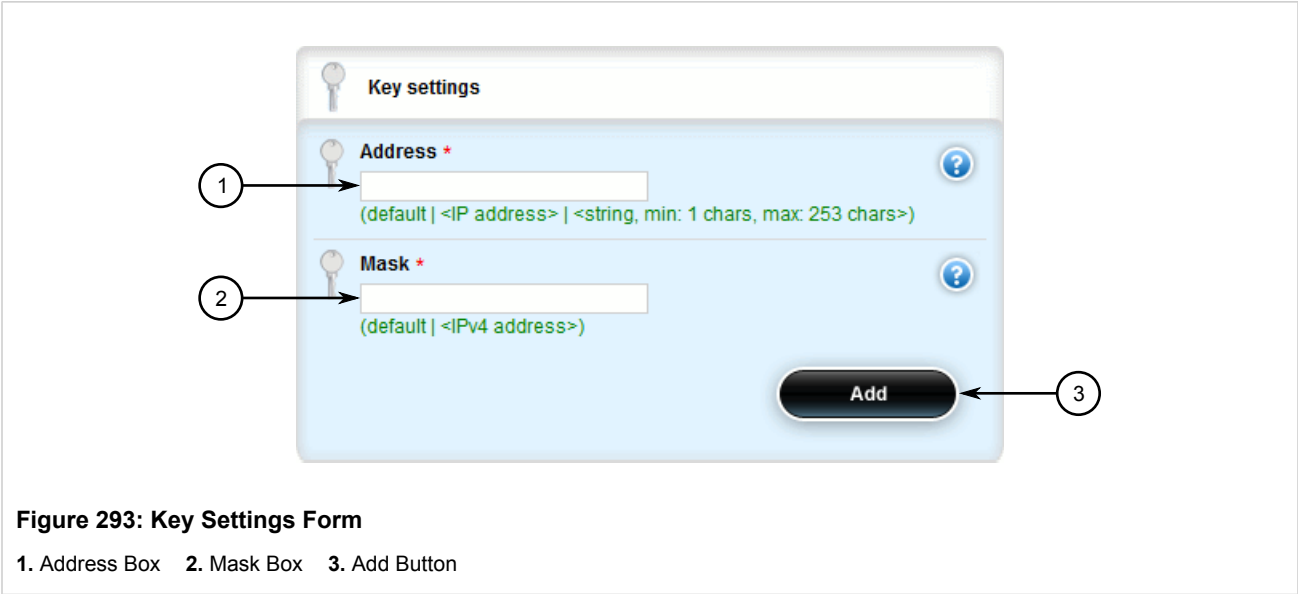
If no server restrictions have been configured, add restrictions as needed. For more information, refer to [Section 5.12.14.2, “Adding a Server Restriction”](#).

Section 5.12.14.2

# Adding a Server Restriction

To add an NTP server restriction, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp » restrict** and click **<Add restrict>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Address	<b>Synopsis:</b> { default } or a string The address to match. The address can be a host or network IP address or a valid host DNS name.
Mask	<b>Synopsis:</b> { default } or a string The mask used to match the address. Mask 255.255.255.255 means the address is treated as the address of an individual host.

4. Click **Add** to create the new restriction. The **Server Restrictions** form appears.

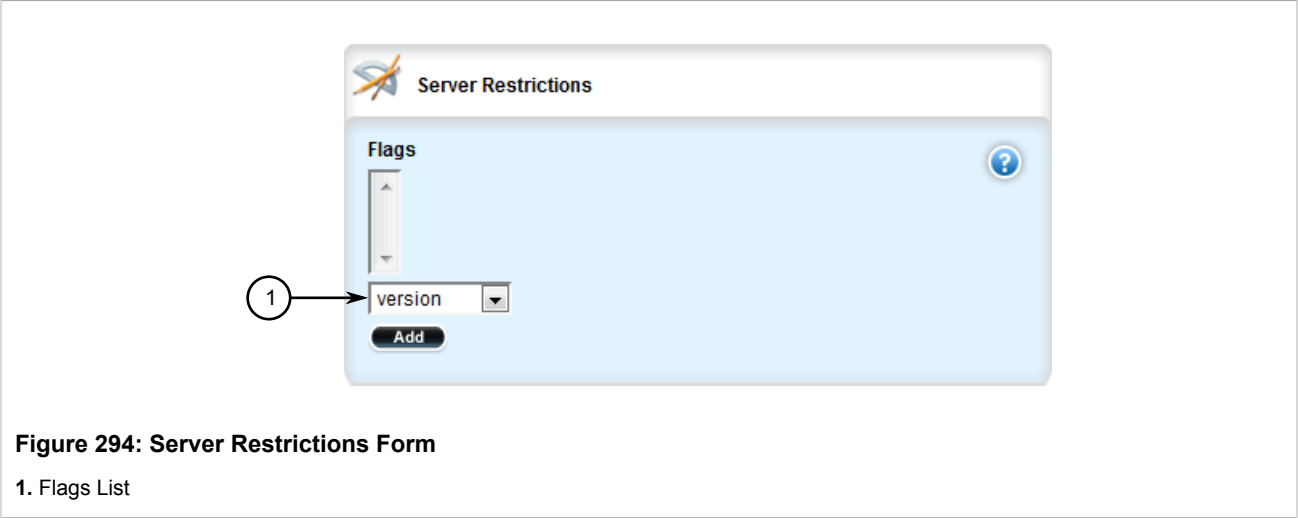


Figure 294: Server Restrictions Form

1. Flags List

5. Configure the following parameter(s) as required:



**CAUTION!**  
*Security hazard – risk of unauthorized access and/or exploitation. It is recommended to restrict queries via `ntpd` and `ntp`, unless the queries come from a local host, or to disable this feature entirely if not required. This prevents DDoS (Distributed Denial of Service) reflection/amplification attacks. Configure the following flags to the restrict default entry: `kod`, `nomodify`, `nopeer`, `noquery` and `notrap`.*

Parameter	Description
Flags	<p><b>Synopsis:</b> { ignore, kod, limited, lowpriortrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version }</p> <p>Flags restrict access to NTP services. An entry with no flags allows free access to the NTP server.</p> <p>&lt;itemizedlist&gt;&lt;listitem&gt;Version: Denies packets that do not match the current NTP version.&lt;/listitem&gt; &lt;listitem&gt;ntpport: Matches only if the source port in the packet is the standard NTP UDP port (123).&lt;/listitem&gt; &lt;listitem&gt;notrust: Denies service unless the packet is cryptographically authenticated.&lt;/listitem&gt; &lt;listitem&gt;notrap: Declines to provide mode 6 control message trap service to matching hosts.&lt;/listitem&gt; &lt;listitem&gt;noserve: Denies all packets except ntpq(8) and ntpdc(8) queries.&lt;/listitem&gt; &lt;listitem&gt;noquery: Denies ntpq(8) and ntpdc(8) queries.&lt;/listitem&gt; &lt;listitem&gt;nopeer: Denies packets which result in mobilizing a new association.&lt;/listitem&gt; &lt;listitem&gt;nomodify: Denies ntpq(8) and ntpdc(8) queries attempting to modify the state of the server; queries returning information are permitted.&lt;/listitem&gt; &lt;listitem&gt;lowpriortrap: Declares traps set by matching hosts to be low priority.&lt;/listitem&gt; &lt;listitem&gt;limited: Denies service if the packet spacing violates the lower limits specified in the NTP discard setting.&lt;/listitem&gt; &lt;listitem&gt;kod: Sends a Kiss-o'-Death (KoD) packet when an access violation occurs.&lt;/listitem&gt; &lt;listitem&gt;ignore: Denies all packets.&lt;/listitem&gt;&lt;/itemizedlist&gt;</p>

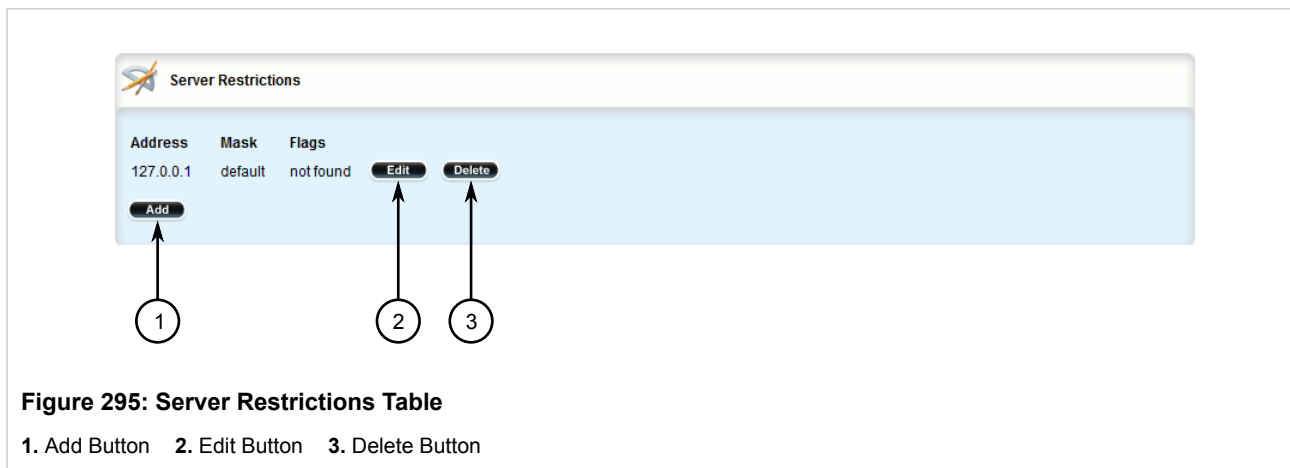
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.12.14.3

## Deleting a Server Restriction

To delete an NTP server restriction, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » time » ntp » restrict**. The **Server Restrictions** table appears.



3. Click **Delete** next to the chosen restriction.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.13

## 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.*

To configure the DHCP relay agent, do the following:

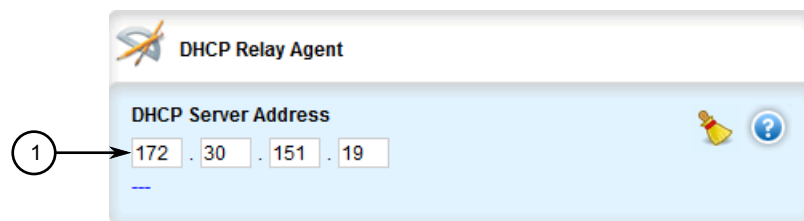
- [Section 5.13.1, “Configuring the DHCP Relay Agent”](#)
- [Section 5.13.2, “Viewing a List of DHCP Client Ports”](#)
- [Section 5.13.3, “Adding DHCP Client Ports”](#)
- [Section 5.13.4, “Deleting a DHCP Client Port”](#)

## Section 5.13.1

## Configuring the DHCP Relay Agent

To configure the DHCP relay agent, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » dhcp-relay-agent**. The **DHCP Relay Agent** form appears.



**Figure 296: DHCP Relay Agent Form**

1. DHCP Server Address Box

3. Configure the following parameter(s) as required:

Parameter	Description
DHCP Server Address	<b>Synopsis:</b> A string The IP address of the DHCP server to which DHCP queries will be forwarded from this relay agent.

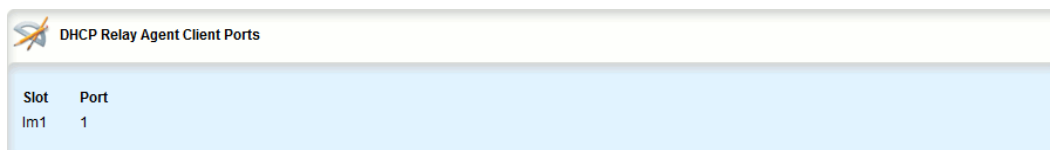
4. Add client ports. For more information, refer to [Section 5.13.3, “Adding DHCP Client Ports”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

6. Click **Exit Transaction** or continue making changes.

### Section 5.13.2

## Viewing a List of DHCP Client Ports

To view a list of DHCP relay agent client ports, navigate to **switch » dhcp-relay-agent » dhcp-client-ports**. If client ports have been configured, the **DHCP Relay Agent Client Ports** table appears.



Slot	Port
Im1	1

**Figure 297: DHCP Relay Agent Client Ports Table**

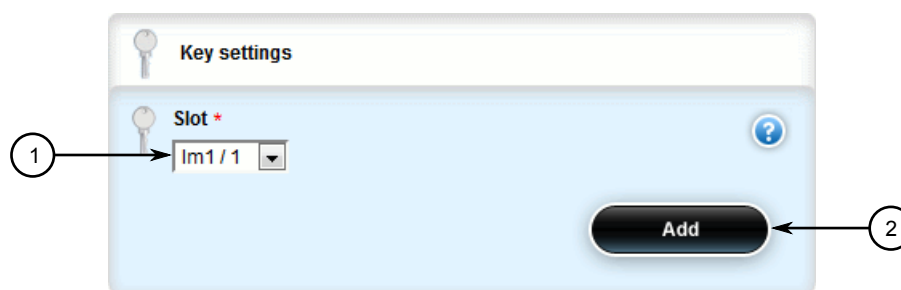
If no client ports have been configured, add client ports as needed. For more information, refer to [Section 5.13.3, “Adding DHCP Client Ports”](#).

### Section 5.13.3

## Adding DHCP Client Ports

To add a client port for the DHCP relay agent, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » dhcp-relay-agent » dhcp-client-ports** and click **<Add dhcp-client-ports>**. The **Key Settings** form appears.



**Figure 298: Key Settings Form**

1. Slot List    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Slot	The name of the module location provided on the silkscreen across the top of the device.

Parameter	Description
Port	The selected ports on the module installed in the indicated slot.

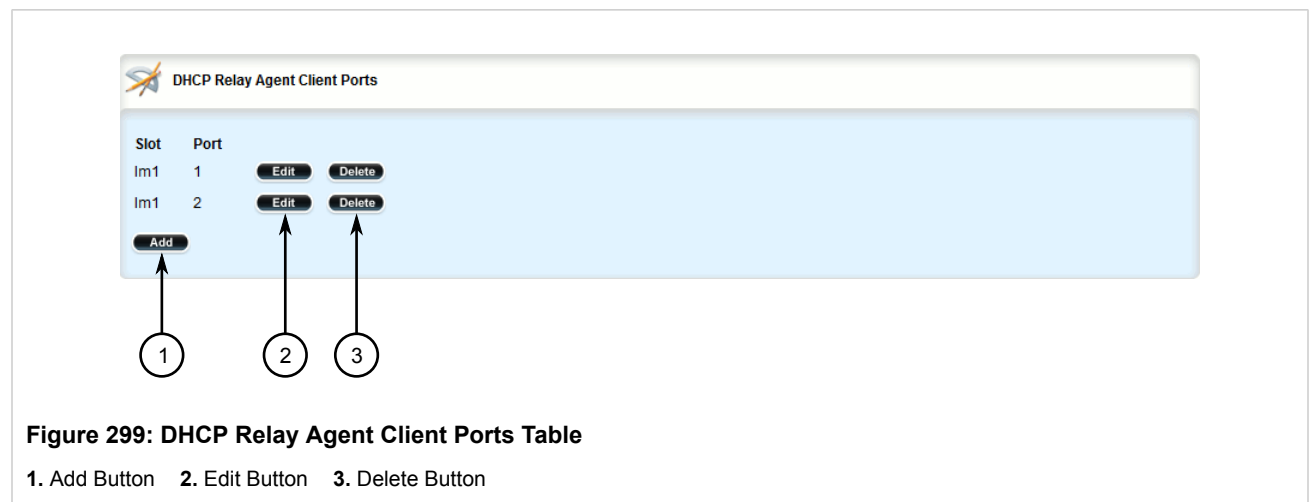
- Click **Add** to add the client port.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.13.4

## Deleting a DHCP Client Port

To delete a client port for the DHCP relay agent, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » dhcp-relay-agent » dhcp-client-ports**. The **DHCP Relay Agent Client Ports** table appears.



- Click **Delete** next to the chosen client port.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14

## 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.

The following sections describe how to configure and manage the DHCP server:

- [Section 5.14.1, “Configuring the DHCP Server”](#)
- [Section 5.14.2, “Enabling/Disabling the DHCP Server”](#)
- [Section 5.14.3, “Enabling/Disabling the DHCP Relay Support”](#)
- [Section 5.14.4, “Viewing a List of Active Leases”](#)
- [Section 5.14.5, “Managing DHCP Listen Interfaces”](#)
- [Section 5.14.6, “Managing Shared Networks”](#)
- [Section 5.14.7, “Managing Subnets”](#)
- [Section 5.14.8, “Managing Custom Client Options for Subnets”](#)
- [Section 5.14.9, “Managing Hosts”](#)
- [Section 5.14.10, “Managing Custom Host Client Configurations”](#)
- [Section 5.14.11, “Managing Host Groups”](#)
- [Section 5.14.12, “Managing Custom Host Group Client Configurations”](#)
- [Section 5.14.13, “Managing IP Pools”](#)
- [Section 5.14.14, “Managing IP Ranges for Subnets”](#)
- [Section 5.14.15, “Managing IP Ranges for IP Pools”](#)
- [Section 5.14.16, “Managing Option 82 Classes for IP Pools”](#)

#### Section 5.14.1

## Configuring the DHCP Server

To configure the DHCP server, do the following:

1. Enable the DHCP Server. For more information, refer to [Section 5.14.2, “Enabling/Disabling the DHCP Server”](#).
2. Add and configure DHCP listen interfaces. For more information, refer to [Section 5.14.5.2, “Adding a DHCP Listen Interface”](#).
3. Add and configure shared networks. For more information, refer to [Section 5.14.6.2, “Adding a Shared Network”](#).



#### NOTE

*At least one shared network must be available before a subnet is added.*

4. Add and configure subnets. For more information, refer to [Section 5.14.7.2, “Adding a Subnet”](#).
5. Add and configure hosts. For more information, refer to [Section 5.14.9.2, “Adding a Host”](#).
6. Add and configure host-groups. For more information, refer to [Section 5.14.11.2, “Adding a Host Group”](#).

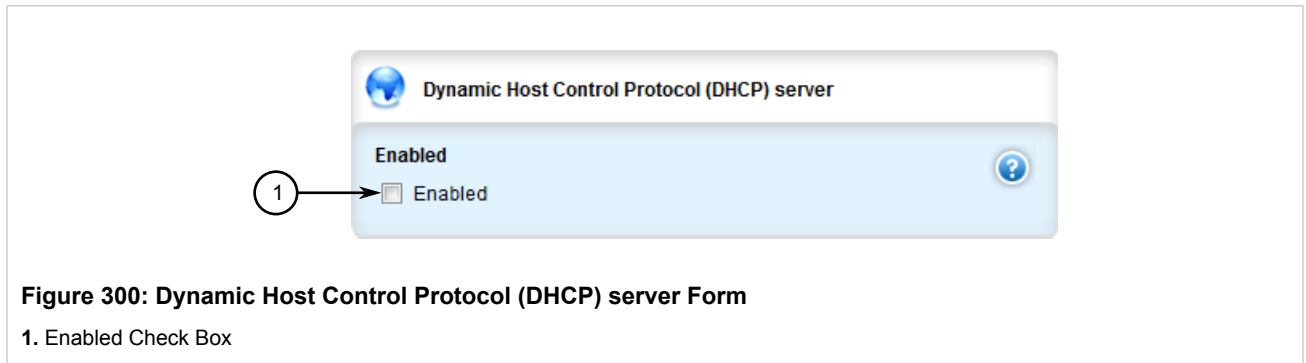
#### Section 5.14.2

## Enabling/Disabling the DHCP Server

To enable or disable the DHCP server, do the following:



1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver**. The **Dynamic Host Control Protocol (DHCP) server** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
enabled	<b>Synopsis:</b> typeless Enables and disables the the DHCP server.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.14.3

## Enabling/Disabling the DHCP Relay Support

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 protocol message to disallow the lease. Enabling Option 82 disables the NAK protocol message so that 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.



#### NOTE

*Option 82 support should only be enabled if the DHCP server and clients are on the same subnet.*



#### NOTE

*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.*



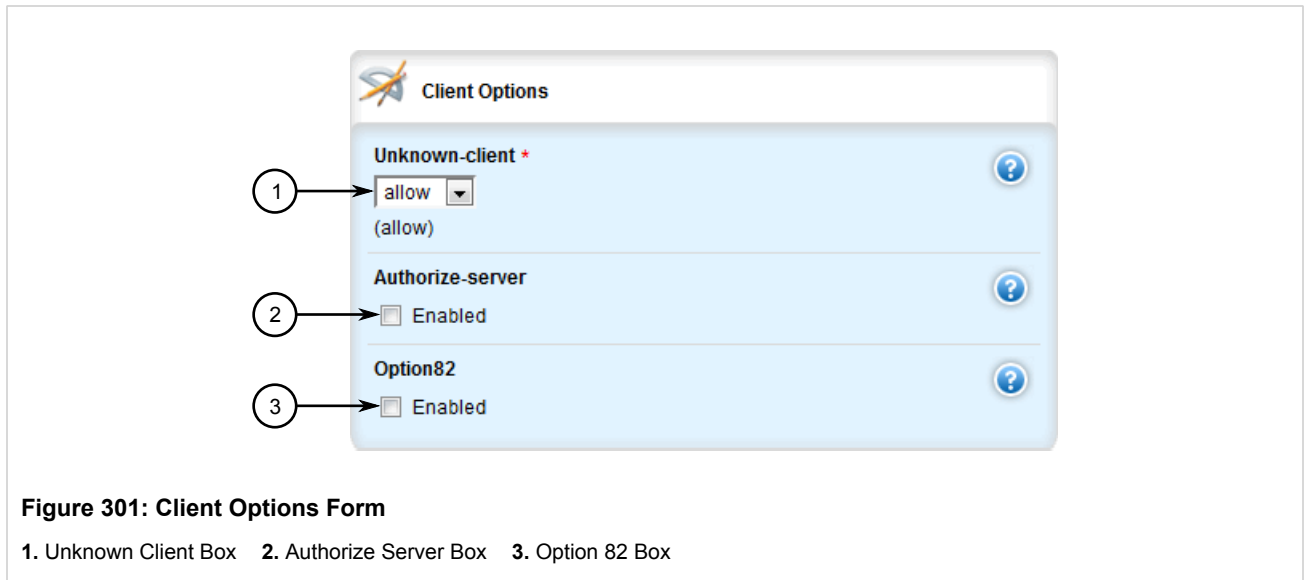
#### NOTE

*DHCP relay support can also be enabled on an individual subnet. For more information, refer to [Section 5.14.7.3, "Configuring Subnet Options"](#).*

To enable or disable DHCP relay support on the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **services » dhcpserver » options**. The **Client Options** form appears.



3. Under **Option 82**, select the **Enabled** check box to enable Option 82 support, or clear the check box to disable support.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

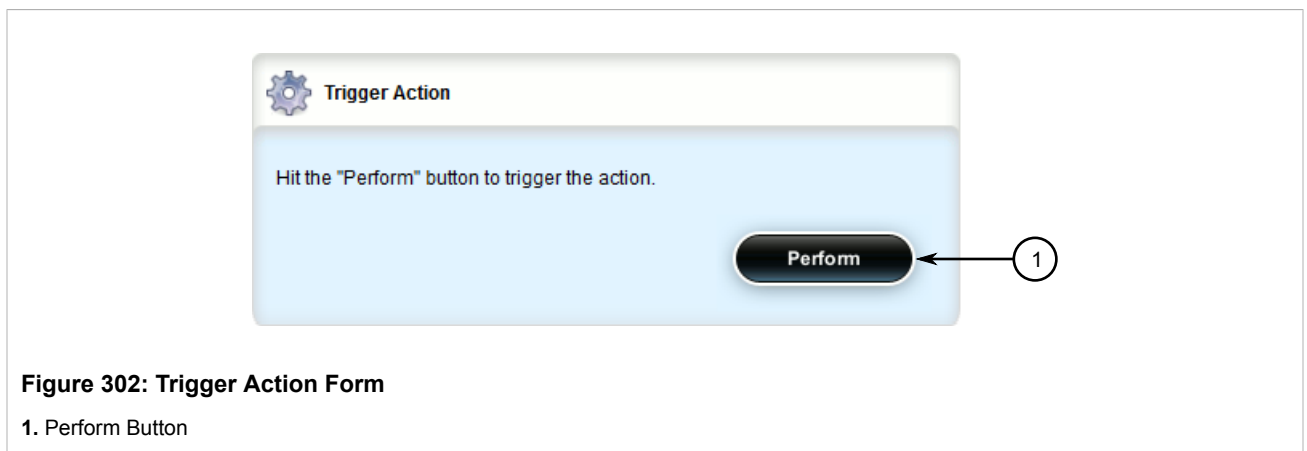
#### Section 5.14.4

## 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:

1. Navigate to **services » dhcpserver** and click **show-active-leases** in the menu. The **Trigger Action** form appears.



- Click **Perform**. The **Show Active Leases** table appears listing the active DHCP leases.

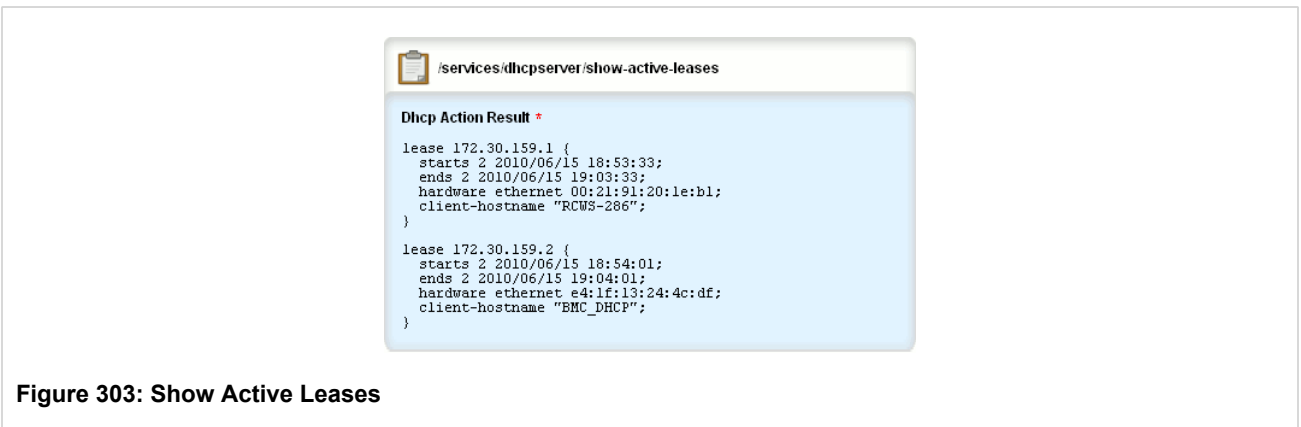


Figure 303: Show Active Leases

#### Section 5.14.5

## Managing DHCP Listen Interfaces

DHCP listen interfaces specify the IP interface to which the client sends a request.

The following sections describe how to manage DHCP listen interfaces:

- [Section 5.14.5.1, “Viewing a List of DHCP Listen Interfaces”](#)
- [Section 5.14.5.2, “Adding a DHCP Listen Interface”](#)
- [Section 5.14.5.3, “Deleting a DHCP Listen Interface”](#)

#### Section 5.14.5.1

### Viewing a List of DHCP Listen Interfaces

To view a list of DHCP listen interfaces, navigate to **services » dhcpserver » interface**. If DHCP listen interfaces have been configured, the **Listen Interfaces** table appears.

The screenshot shows a web interface window titled "Listen Interfaces". Below the title bar, there is a table with one row:

Name
fe-cm-1

Figure 304: Listen Interfaces Table

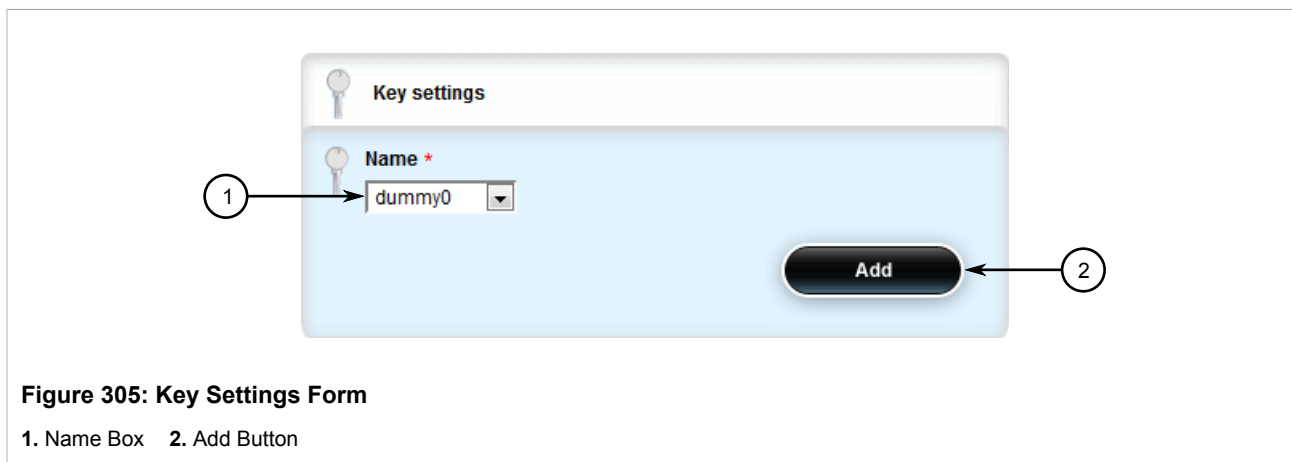
If no DHCP listen interfaces have been configured, add interfaces as needed. For more information, refer to [Section 5.14.5.2, “Adding a DHCP Listen Interface”](#).

#### Section 5.14.5.2

### Adding a DHCP Listen Interface

To add a DHCP listen interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » interface** and click **<Add interface>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
name	

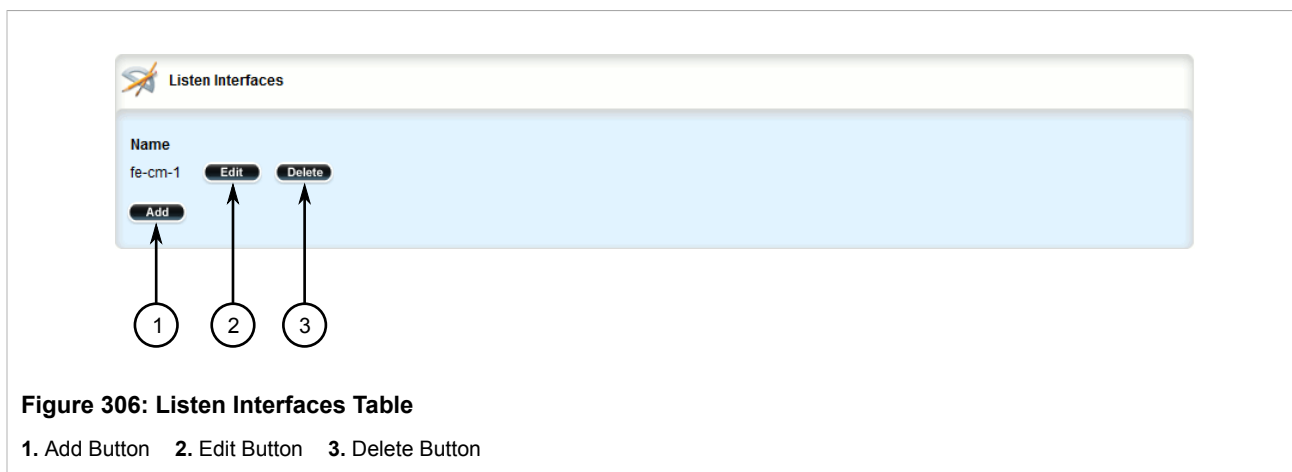
4. Click **Add** to create the new DHCP listen interface.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 5.14.5.3

### Deleting a DHCP Listen Interface

To delete a DHCP listen interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » interface**. The **Listen Interfaces** table appears.



3. Click **Delete** next to the chosen DHCP listen interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.14.6

## 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.

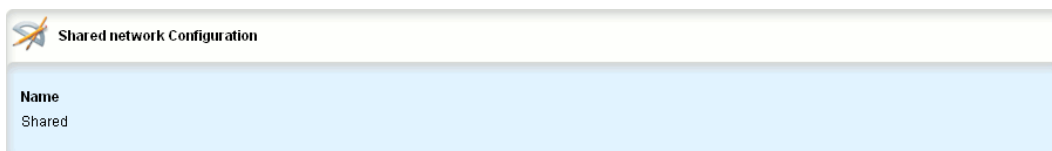
The following sections describe how to configure and manage shared networks on a DHCP server:

- [Section 5.14.6.1, “Viewing a List of Shared Networks”](#)
- [Section 5.14.6.2, “Adding a Shared Network”](#)
- [Section 5.14.6.3, “Configuring Shared Network Options”](#)
- [Section 5.14.6.4, “Configuring a Shared Network Client”](#)
- [Section 5.14.6.5, “Customizing Shared Network Clients”](#)
- [Section 5.14.6.6, “Deleting a Shared Network”](#)

## Section 5.14.6.1

### Viewing a List of Shared Networks

To view a list of shared networks, navigate to **services » dhcpserver » shared-network**. If shared networks have been configured, the **Shared network Configuration** table appears.



Name
Shared

**Figure 307: Shared Network Configuration Table**

If no shared networks have been configured, add shared networks as needed. For more information, refer to [Section 5.14.6.2, “Adding a Shared Network”](#).

## Section 5.14.6.2

### Adding a Shared Network

To add a shared network to the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

- Navigate to **services » dhcpserver » shared-network** and click **<Add shared-network>**. The **Key Settings** form appears.

**Figure 308: Key Settings Form**

1. Name Box    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.

- Click **Add** to create the new shared network.
- Configure options for the shared network. For more information, refer to [Section 5.14.6.3, “Configuring Shared Network Options”](#).
- Configure the client for the shared network. For more information, refer to [Section 5.14.6.4, “Configuring a Shared Network Client”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.14.6.3

## 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.*

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » shared-network{shared network} » options**, where *{shared network}* is the name of the shared network. The **Leased Configuration** and **Client Configuration** forms appear.

Figure 309: Leased Configuration Form

1. Default Box    2. Maximum Box

Figure 310: Client Configuration Form

1. Unknown Client List    2. Authorize Server Check Box    3. Option 82 Check Box

3. On the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	<b>Default:</b> 600 The minimum leased time in seconds that the server offers to the client.
maximum	<b>Default:</b> 7200 The maximum leased time in seconds that the server offers to the clients.

4. On the **Client Configuration** form, configure the following parameters as required:

Parameter	Description
Unknown Client	<b>Synopsis:</b> { allow, deny, ignore } The action to take for previously unregistered clients.
Authorize Server	<b>Synopsis:</b> typeless

Parameter	Description
	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	<b>Synopsis:</b> typeless Enables/disables the NAK of option 82 clients for this subnet.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

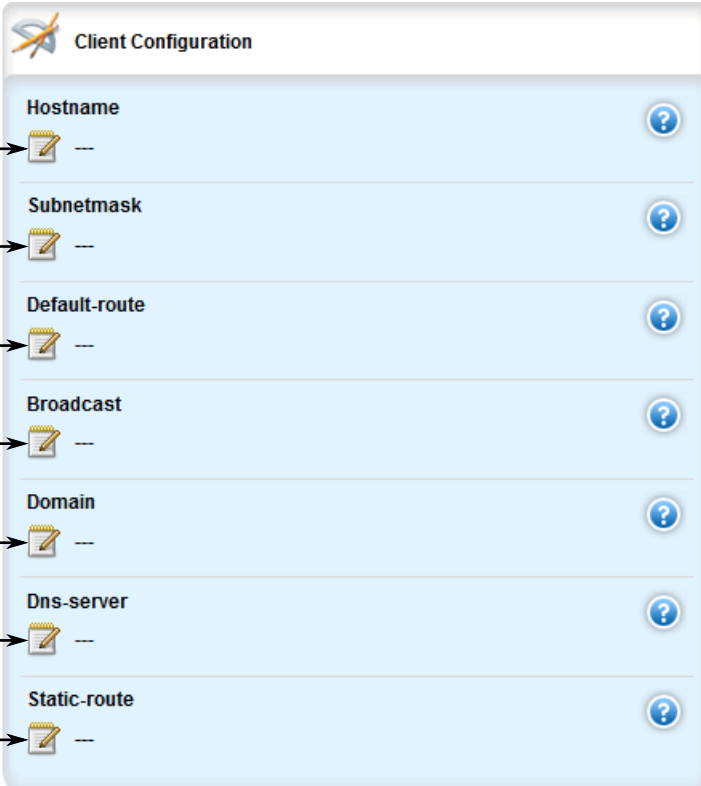
#### Section 5.14.6.4

### Configuring a Shared Network Client

To configure the client for a shared network on the DHCP server, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » shared-network{shared network} » options » client**, where *{shared network}* is the name of the shared network. The **Client Configuration**, **NIS Configuration** and **NetBios Configuration** forms appear.



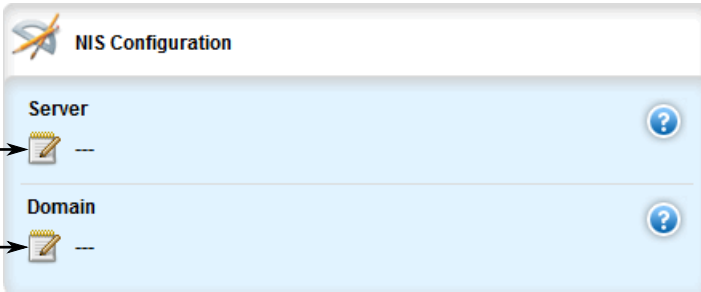


The Client Configuration form is a light blue rectangular box with a title bar at the top containing a network icon and the text "Client Configuration". Below the title bar, there are seven configuration rows, each with a label, a text input field with a yellow notepad icon, and a blue circular help button with a question mark. The rows are: Hostname, Subnetmask, Default-route, Broadcast, Domain, Dns-server, and Static-route. To the left of the form, seven numbered circles (1 through 7) have arrows pointing to the input fields of the corresponding rows.

Field	Input Field	Help Button
1. Hostname	---	?
2. Subnetmask	---	?
3. Default-route	---	?
4. Broadcast	---	?
5. Domain	---	?
6. Dns-server	---	?
7. Static-route	---	?

**Figure 311: Client Configuration Form**

1. Host Name Box   2. Subnet Mask Box   3. Default Route Box   4. Broadcast Box   5. Domain Box   6. DNS Server Box  
7. Static Route Box



The NIS Configuration form is a light blue rectangular box with a title bar at the top containing a network icon and the text "NIS Configuration". Below the title bar, there are two configuration rows, each with a label, a text input field with a yellow notepad icon, and a blue circular help button with a question mark. The rows are: Server and Domain. To the left of the form, two numbered circles (1 and 2) have arrows pointing to the input fields of the corresponding rows.

Field	Input Field	Help Button
1. Server	---	?
2. Domain	---	?

**Figure 312: NIS Configuration Form**

1. Server Box   2. Domain Box

The image shows a 'NetBios Configuration' form. It has two main sections: 'Scope \*' and 'Nameserver \*'. The 'Scope \*' section contains a text input field with the value 'netbios' and a dropdown menu showing '(netbios)'. The 'Nameserver \*' section contains a text input field with the value '127.0.0.1' and a dropdown menu showing '(127.0.0.1)'. Both sections have a blue question mark icon in the top right corner. Two numbered circles with arrows point to the respective sections: circle 1 points to the Scope section, and circle 2 points to the Nameserver section.

**Figure 313: NetBios Configuration Form**

1. Scope Box 2. Name Server Box

3. On the **Client Configuration** form, configure the following parameters as required:

Parameter	Description
Host Name	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.
Subnet Mask	<b>Synopsis:</b> A string 7 to 15 characters long Subnet mask
Default Route	<b>Synopsis:</b> 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	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long The domain name that the server offers to the client when it issues the lease to the client.
DNS Server	<b>Synopsis:</b> A string 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	<b>Synopsis:</b> 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. On the **NIS Configuration** form, configure the following parameters as required:

Parameter	Description
server	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 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. On the **NetBios Configuration** form, configure the following parameters as required:

Parameter	Description
scope	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
Name Server	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

6. If custom options are required for the shared network client, refer to [Section 5.14.6.5, “Customizing Shared Network Clients”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.14.6.5

### Customizing Shared Network Clients

Custom DHCP options can be set for a shared network client.

To add a custom DHCP option to a shared network client, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » shared-network » {name} » options » client » custom**, where *{name}* is the name of the shared network.
3. Click **<Add custom>**. The **Key Settings** form appears.

**Figure 314: Key Settings Form**

1. Number Box 2. Value Box

4. Configure the following parameter(s) as required:

Parameter	Description
number	
value	The value of the custom option.

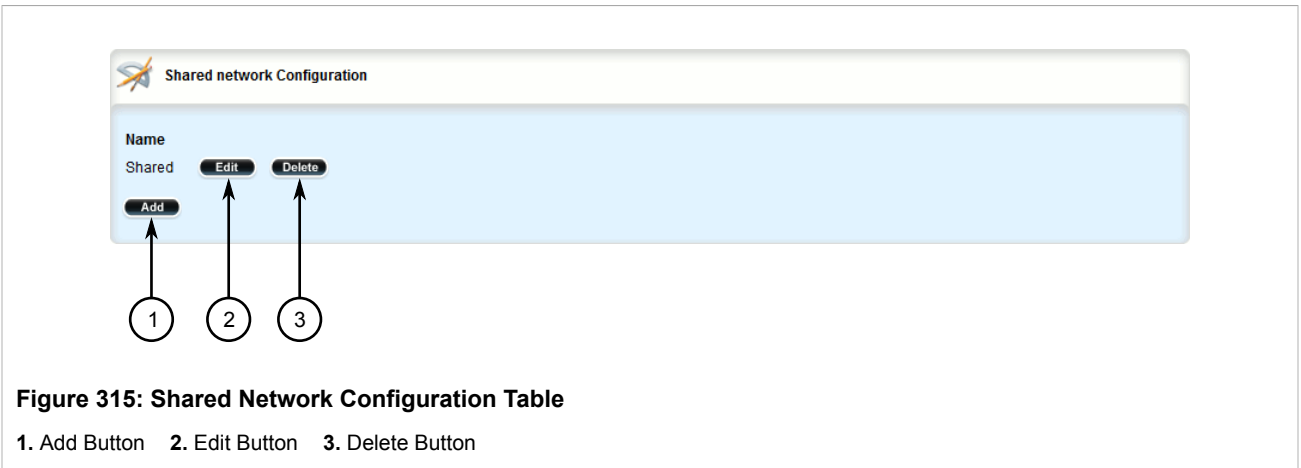
5. Click **Add**.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.14.6.6

### Deleting a Shared Network

To delete a shared network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » shared-network**. The **Shared network Configuration** table appears.



3. Click **Delete** next to the chosen shared network.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.14.7

## 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.

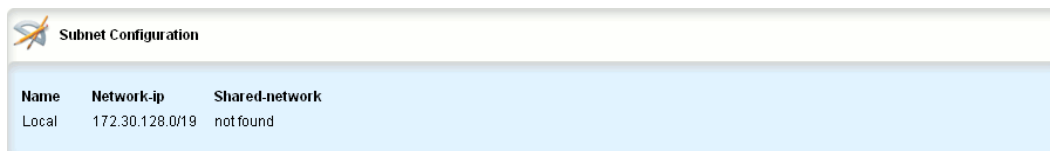
The following sections describe how to configure and manage subnets on a DHCP server:

- [Section 5.14.7.1, "Viewing a List of Subnets"](#)
- [Section 5.14.7.2, "Adding a Subnet"](#)
- [Section 5.14.7.3, "Configuring Subnet Options"](#)
- [Section 5.14.7.4, "Configuring a Subnet Client"](#)
- [Section 5.14.7.5, "Deleting a Subnet"](#)

#### Section 5.14.7.1

### Viewing a List of Subnets

To view a list of subnets, navigate to **services » dhcpserver » subnet**. If subnets have been configured, the **Subnet Configuration** table appears.



Name	Network-ip	Shared-network
Local	172.30.128.0/19	not found

**Figure 316: Subnet Configuration Table**

If no subnets have been configured, add subnets as needed. For more information, refer to [Section 5.14.7.2, “Adding a Subnet”](#).

## Section 5.14.7.2

### Adding a Subnet

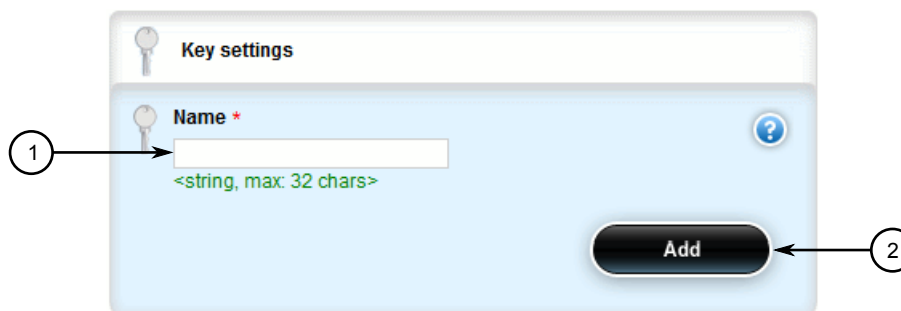
To add a subnet to the DHCP server, do the following:



#### NOTE

Make sure a shared network is configured before adding a new subnet. For information about configuring a shared network, refer to [Section 5.14.6.2, “Adding a Shared Network”](#).

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet** and click **<Add subnet>** in the menu. The **Key Settings** form appears.



The image shows a 'Key settings' form with a 'Name' field and an 'Add' button. A circled '1' points to the 'Name' field, and a circled '2' points to the 'Add' button. The 'Name' field has a red asterisk and a help icon. Below the field is the text '<string, max: 32 chars>'. The 'Add' button is a dark rounded rectangle with the word 'Add' in white.

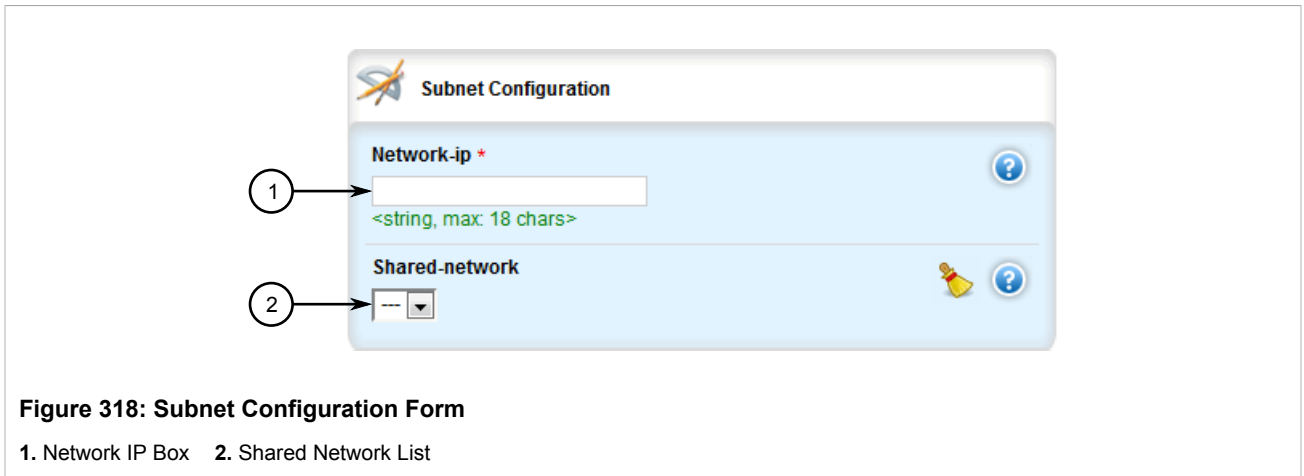
**Figure 317: Key Settings Form**

1. Name Box 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.

4. Click **Add** to create the new subnet. The **Subnet Configuration** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Network IP	<b>Synopsis:</b> A string 9 to 18 characters long The network IP address for this subnet.
Shared Network	The shared-network that this subnet belongs to.

- Configure the options for the subnet. For more information, refer to [Section 5.14.7.3, “Configuring Subnet Options”](#)
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.7.3

### 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.*

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » subnet » {name} » options**, where {name} is the name of the subnet. The **Leased Configuration** and **Client Configuration** forms appear.

**Leased Configuration**

**Default \*** ?

600  
(600)

**Maximum \*** ?

7200  
(7200)

**Figure 319: Leased Configuration Form**

1. Default Box 2. Maximum Box

**Client Configuration**

**Unknown-client** ?

--

**Authorize-server** ?

☒ Enabled

**Option82** ?

☒ Enabled

**Figure 320: Client Configuration Form**

1. Unknown Client Box 2. Authorize Server Box 3. Option 82 Box

- In the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	<b>Default:</b> 600 The minimum leased time in seconds that the server offers to the client.
maximum	<b>Default:</b> 7200 The maximum leased time in seconds that the server offers to the clients.

- In the **Client Configuration** form, configure the following parameters as required:

**NOTE**  
For more information about enabling/disabling the Option82 parameter, refer to [Section 5.14.3, "Enabling/Disabling the DHCP Relay Support"](#).



Parameter	Description
Unknown Client	<b>Synopsis:</b> { allow, deny, ignore } The action to take for previously unregistered clients.
Authorize Server	<b>Synopsis:</b> typeless 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	<b>Synopsis:</b> typeless Enables/disables the NAK of option 82 clients for this subnet.

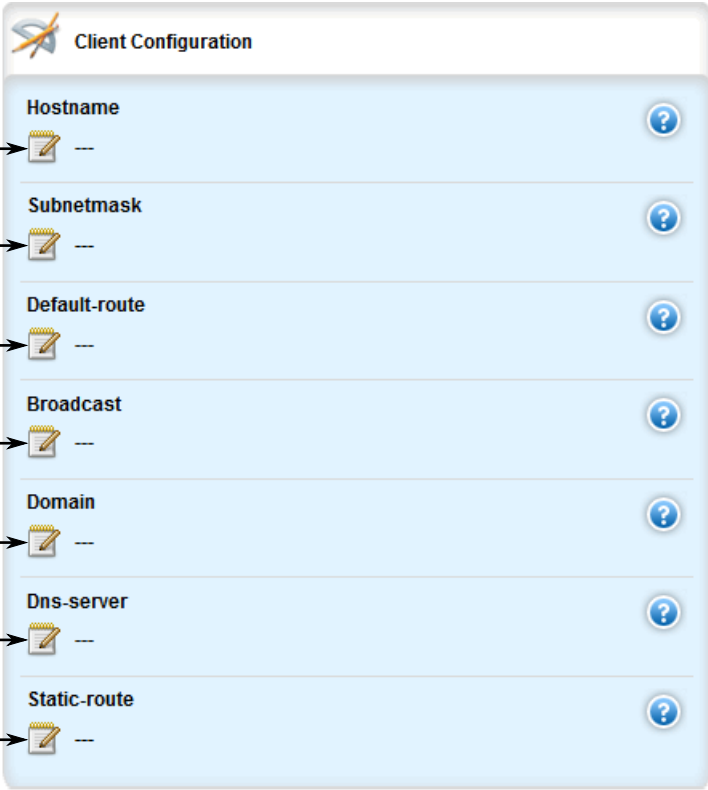
5. Configure the client for the subnet. For more information, refer to [Section 5.14.7.4, "Configuring a Subnet Client"](#)
6. Configure one or more IP pools to the subnet. For more information, refer to [Section 5.14.13.2, "Adding an IP Pool"](#)
7. Configure one or more IP ranges to the subnet. For more information, refer to [Section 5.14.14.2, "Adding an IP Range to a DHCP Subnet"](#)
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

## Section 5.14.7.4

## Configuring a Subnet Client

To configure a client for a subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet » {name} » options » client**, where *{name}* is the name of the subnet. The **Client Configuration**, **NIS Configuration** and **NetBios Configuration** forms appear.

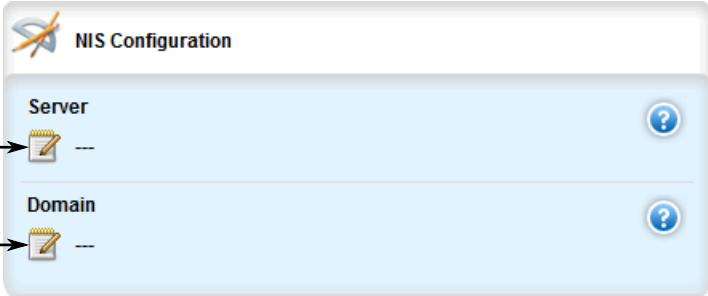


The Client Configuration form is a light blue panel with a title bar containing a logo and the text "Client Configuration". It contains seven rows, each with a label, a text input field with a yellow notepad icon, and a blue circular help button with a question mark. The rows are: Hostname, Subnetmask, Default-route, Broadcast, Domain, Dns-server, and Static-route. Numbered circles 1 through 7 are placed to the left of each row, with arrows pointing to the input fields.

Field	Input Field	Help Button
1. Hostname	---	?
2. Subnetmask	---	?
3. Default-route	---	?
4. Broadcast	---	?
5. Domain	---	?
6. Dns-server	---	?
7. Static-route	---	?

**Figure 321: Client Configuration Form**

1. Host Name Box   2. Subnet Mask Box   3. Default Route Box   4. Broadcast Box   5. Domain Box   6. DNS Server Box  
7. Static Route Box



The NIS Configuration form is a light blue panel with a title bar containing a logo and the text "NIS Configuration". It contains two rows, each with a label, a text input field with a yellow notepad icon, and a blue circular help button with a question mark. The rows are: Server and Domain. Numbered circles 1 and 2 are placed to the left of each row, with arrows pointing to the input fields.

Field	Input Field	Help Button
1. Server	---	?
2. Domain	---	?

**Figure 322: NIS Configuration Form**

1. Server Box   2. Domain Box



**Figure 323: NetBios Configuration Form**

1. Scope Box    2. Name Server Box

3. In the **Client Configuration** form, configure the following parameters as required:.

Parameter	Description
Host Name	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.
Subnet Mask	<b>Synopsis:</b> A string 7 to 15 characters long Subnet mask
Default Route	<b>Synopsis:</b> 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	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long The domain name that the server offers to the client when it issues the lease to the client.
DNS Server	<b>Synopsis:</b> A string 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	<b>Synopsis:</b> 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. In the **NIS Configuration** form, configure the following parameters as required:

Parameter	Description
server	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long

Parameter	Description
	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.

- In the **NetBios Configuration** form, configure the following parameters as required:

Parameter	Description
scope	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
Name Server	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

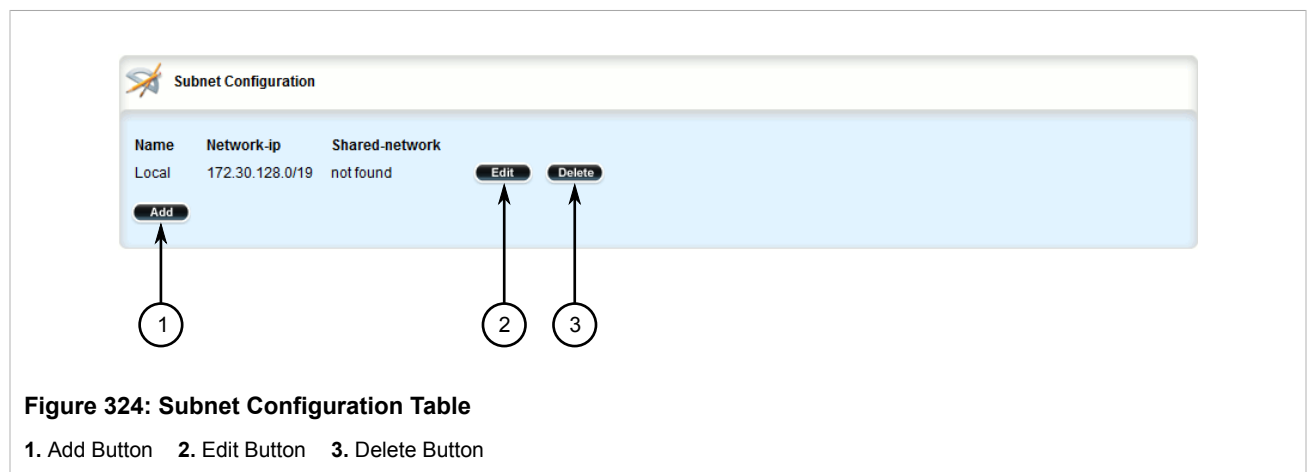
- If custom options are required for the subnet client, refer to [Section 5.14.8.2, “Adding a Custom Client Option”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.7.5

### Deleting a Subnet

To delete a subnet, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » subnet**. The **Subnet Configuration** table appears.



- Click **Delete** next to the chosen subnet.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.8

## Managing Custom Client Options for Subnets

The following sections describe how to configure and manage custom client options for a DHCP subnet:

- [Section 5.14.8.1, “Viewing a List of Custom Client Options”](#)
- [Section 5.14.8.2, “Adding a Custom Client Option”](#)
- [Section 5.14.8.3, “Deleting a Custom Client Option”](#)

## Section 5.14.8.1

### Viewing a List of Custom Client Options

To view a list of custom client options configured for a DHCP subnet, navigate to **services » dhcpserver » subnet » {name} » options » client » custom**, where {name} is the name of the subnet. The **Custom Configuration** table appears.



Number	Value
22	2
23	1

Figure 325: Custom Configuration Table

If no custom client options have been configured, add options as needed. For more information, refer to [Section 5.14.8.2, “Adding a Custom Client Option”](#).

## Section 5.14.8.2

### Adding a Custom Client Option

To add a custom client option to a DHCP subnet, 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 this custom option can be configured. For more information about DHCP options, refer to [RFC 2132](http://tools.ietf.org/html/rfc2132) [<http://tools.ietf.org/html/rfc2132>].*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet » {name} » options » client » custom**, where {name} is the name of the subnet.
3. Click **<Add custom>**. The **Key Settings** form appears.

**Figure 326: Key Settings Form**

1. Number Box   2. Value Box   3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
number	
value	The value of the custom option.

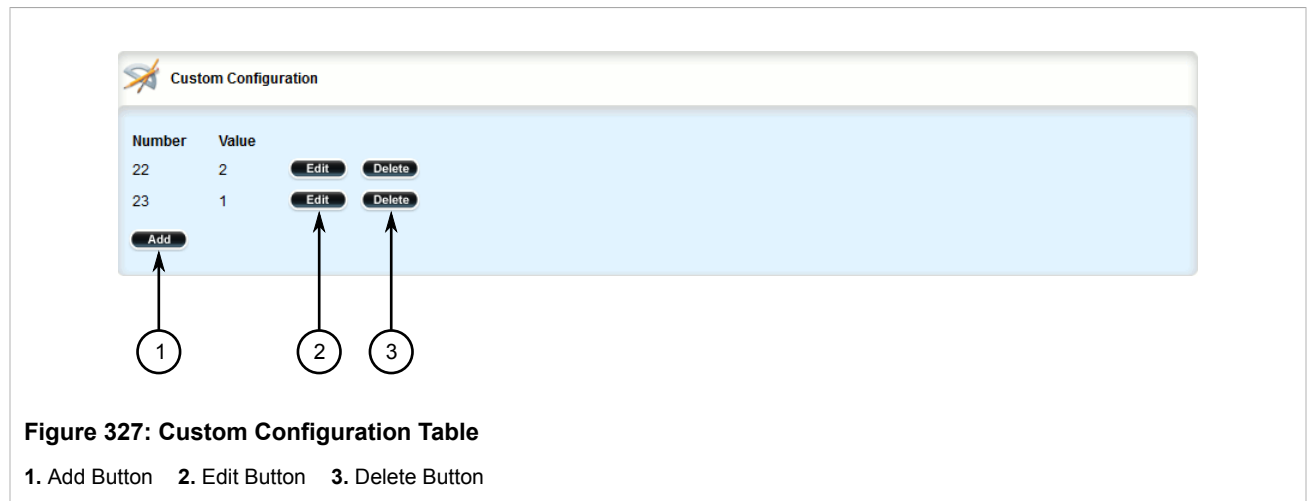
5. Click **Add**.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.14.8.3

### Deleting a Custom Client Option

To delete a custom client option for a DHCP subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet » {name} » options » client » custom**, where {name} is the name of the subnet. The **Custom Configuration** table appears.



3. Click **Delete** next to the chosen custom client option.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.14.9

## Managing Hosts

Host entries assign settings to a specific client based on its Ethernet MAC address.

The following sections describe how to configure and manage hosts on a DHCP server:

- [Section 5.14.9.1, “Viewing a List of Hosts”](#)
- [Section 5.14.9.2, “Adding a Host”](#)
- [Section 5.14.9.3, “Configuring Host Options”](#)
- [Section 5.14.9.4, “Configuring a Host Client”](#)
- [Section 5.14.9.5, “Deleting Hosts”](#)

#### Section 5.14.9.1

### Viewing a List of Hosts

To view a list of hosts on the DHCP server, navigate to **services » dhcpserver » hosts**. If hosts have been configured, the **Host Configuration** table appears.

Host Configuration	
Name	
157	
RCWS-286	

**Figure 328: Host Configuration Table**

If no hosts have been configured, add hosts as needed. For more information, refer to [Section 5.14.9.2, “Adding a Host”](#).

#### Section 5.14.9.2

### Adding a Host

To add a host to the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » hosts** and click **<Add host>**. The **Key Settings** form appears.

**Figure 329: Key Settings Form**

1. Name Box 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.

4. Click **Add** to create the new host.
5. Configure options for the host. For more information, refer to [Section 5.14.9.3, “Configuring Host Options”](#).
6. Configure the client for the host. For more information, refer to [Section 5.14.9.4, “Configuring a Host Client”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.



Section 5.14.9.3

## 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.*

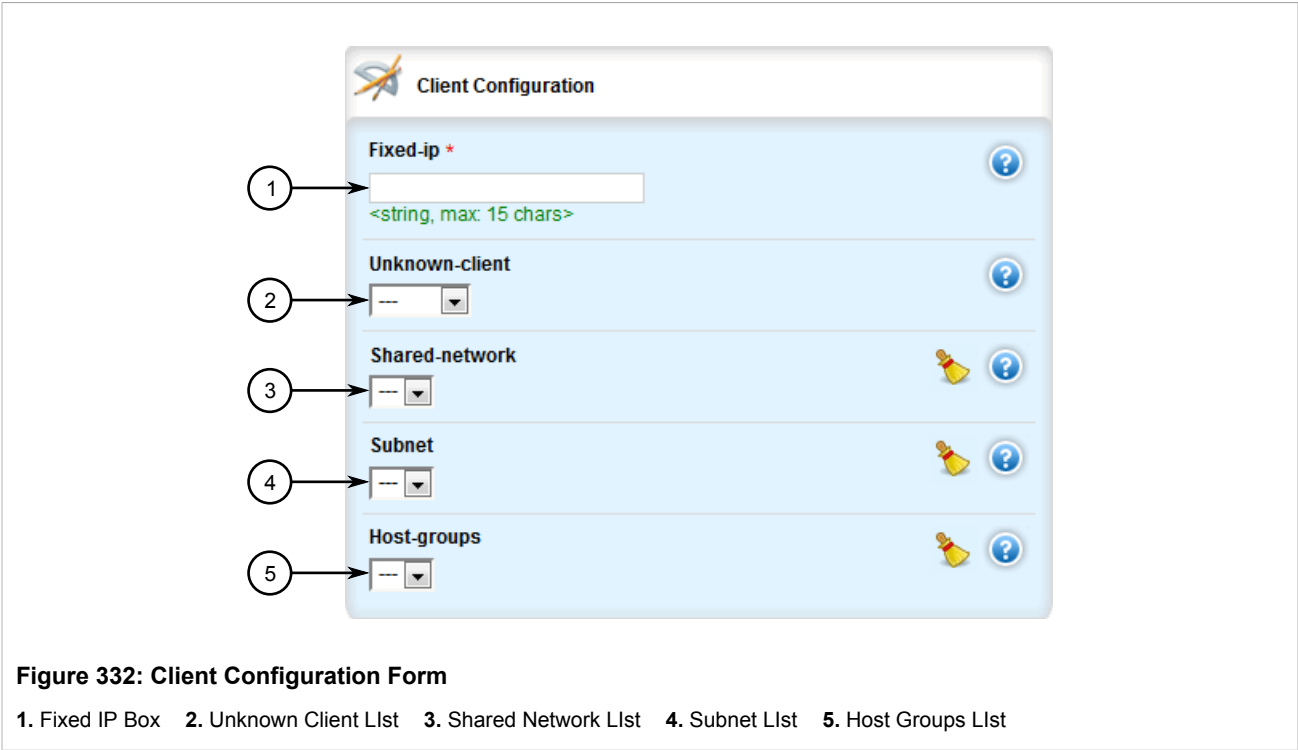
1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » hosts » {host} » options**, where {host} is the name of the host. The **Hardware Configuration**, **Leased Configuration** and **Client Configuration** forms appear.

**Figure 330: Hardware Configuration Form**

1. Type List    2. MAC Box

**Figure 331: Leased Configuration Form**

1. Default Box    2. Maximum Box



**Figure 332: Client Configuration Form**

1. Fixed IP Box    2. Unknown Client Llist    3. Shared Network Llist    4. Subnet Llist    5. Host Groups Llist

3. On the **Hardware Configuration** form, configure the following parameters as required:

Parameter	Description
type	<b>Synopsis:</b> { fddi, token-ring, ethernet } <b>Default:</b> ethernet The type of network hardware used by the client, associated with the host entry.
mac	<b>Synopsis:</b> A string The physical network address of the client. Note that this corresponds to the hardware type; for example, the MAC address for the ethernet.

4. On the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	<b>Default:</b> 600 The minimum leased time in seconds that the server offers to the client.
maximum	<b>Default:</b> 7200 The maximum leased time in seconds that the server offers to the clients.

5. On the **Client Configuration** form, configure the following parameters as required:

Parameter	Description
fixed-ip	<b>Synopsis:</b> A string 7 to 15 characters long

Parameter	Description
	The IP address that the server assigns to the matching client.
unknown-client	<b>Synopsis:</b> { allow, deny, ignore } The action to take for previously unregistered clients.
shared-network	The shared-network that this host belongs to.
subnet	The subnet that this host belongs to.
host-groups	The host groups that this host belongs to.

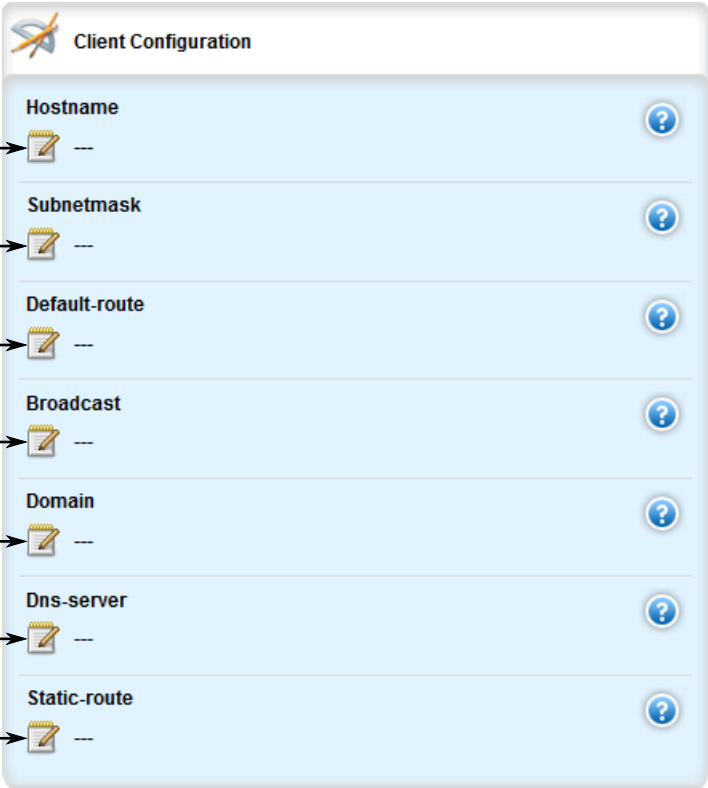
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.9.4

## Configuring a Host Client

To configure a client for a host on the DHCP Server, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » hosts » {host} » options » client**, where *{host}* is the name of the host. The **Client Configuration**, **NIS Configuration** and **NetBios Configuration** forms appear.

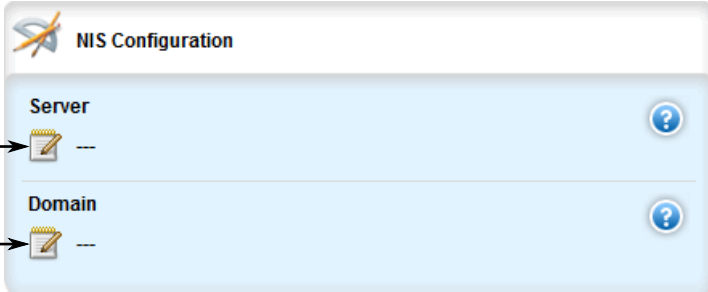


The image shows a 'Client Configuration' form with a light blue background and a white header. The header contains a logo and the title 'Client Configuration'. The form has seven rows, each with a label, a text input field, and a help icon. The rows are: 'Hostname', 'Subnetmask', 'Default-route', 'Broadcast', 'Domain', 'Dns-server', and 'Static-route'. Each row has a yellow notepad icon in the input field. To the left of the form, there are seven numbered circles (1 through 7) with arrows pointing to the input fields of the corresponding rows.

Field	Value
Hostname	---
Subnetmask	---
Default-route	---
Broadcast	---
Domain	---
Dns-server	---
Static-route	---

**Figure 333: Client Configuration Form**

1. Host Name Box   2. Subnet Mask Box   3. Default Route Box   4. Broadcast Box   5. Domain Box   6. DNS Server Box  
7. Static Route Box



The image shows an 'NIS Configuration' form with a light blue background and a white header. The header contains a logo and the title 'NIS Configuration'. The form has two rows: 'Server' and 'Domain'. Each row has a text input field and a help icon. To the left of the form, there are two numbered circles (1 and 2) with arrows pointing to the input fields of the corresponding rows.

Field	Value
Server	---
Domain	---

**Figure 334: NIS Configuration Form**

1. Server Box   2. Domain Box

The screenshot shows the 'NetBios Configuration' form. It has two main sections: 'Scope \*' and 'Nameserver \*'. The 'Scope \*' section contains a dropdown menu with 'netbios' selected, and a help icon. The 'Nameserver \*' section contains a text input field with '127.0.0.1' entered, and a help icon. Two numbered circles with arrows point to these sections: circle 1 points to the 'Scope \*' section, and circle 2 points to the 'Nameserver \*' section.

**Figure 335: NetBios Configuration Form**

1. Scope Box 2. Name Server Box

- On the **Client Configuration** form, configure the following parameters as required:

Parameter	Description
hostname	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.
subnetmask	<b>Synopsis:</b> A string 7 to 15 characters long Subnet mask
default-route	<b>Synopsis:</b> 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	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long The domain name that the server offers to the client when it issues the lease to the client.
dns-server	<b>Synopsis:</b> A string 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	<b>Synopsis:</b> 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.

- On the **NIS Configuration** form, configure the following parameters as required:

Parameter	Description
server	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long

Parameter	Description
	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.

- On the **NetBios Configuration** form, configure the following parameters as required:

Parameter	Description
scope	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
nameserver	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

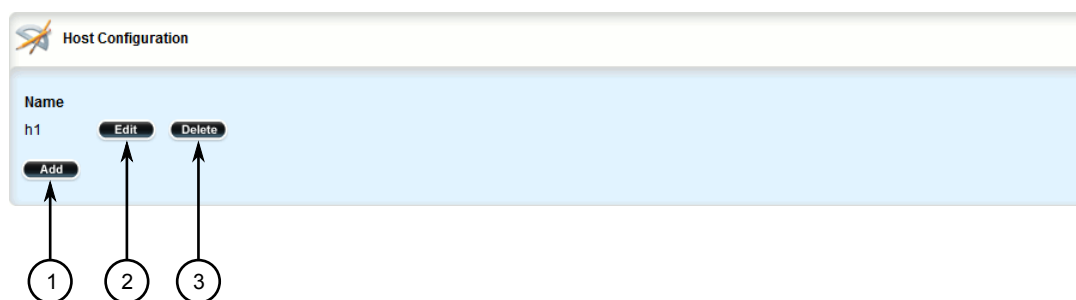
- If custom configuration settings are required for the host client, refer to [Section 5.14.10, “Managing Custom Host Client Configurations”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.9.5

### Deleting Hosts

To delete a host, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » hosts**. The **Host Configuration** table appears.



**Figure 336: Host Configuration Table**

1. Add Button    2. Edit Button    3. Delete Button

- Click **Delete** next to the chosen host.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.10

## Managing Custom Host Client Configurations

Custom configuration settings can be set for each host client.

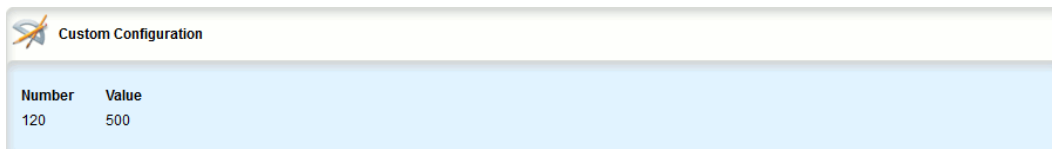
The following sections describe how to configure and manage custom host client configurations on a DHCP server:

- [Section 5.14.10.1, “Viewing a List of Custom Host Client Configurations”](#)
- [Section 5.14.10.2, “Adding Custom Host Client Configurations”](#)
- [Section 5.14.10.3, “Deleting Custom Host Client Configurations”](#)

## Section 5.14.10.1

### Viewing a List of Custom Host Client Configurations

To view a list of custom configurations for host clients on the DHCP server, navigate to **services » dhcpserver » hosts » {host} » options » client » custom**, where {host} is the name of the host. If custom configurations have been configured, the **Custom Configuration** table appears.



Number	Value
120	500

Figure 337: Custom Configuration Table

If no custom configurations have been configured for the host client, add custom configurations as needed. For more information, refer to [Section 5.14.10.2, “Adding Custom Host Client Configurations”](#).

## Section 5.14.10.2

### Adding Custom Host Client Configurations

To add a custom configuration to a host client on the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » hosts » {host} » options » client » custom**, where {host} is the name of the host.
3. Click **<Add custom>**. The **Key Settings** form appears.

**Figure 338: Key Settings Form**

1. Number Box   2. Value Box   3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
number	
value	The value of the custom option.

5. Click **Add** to create the new custom configuration.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

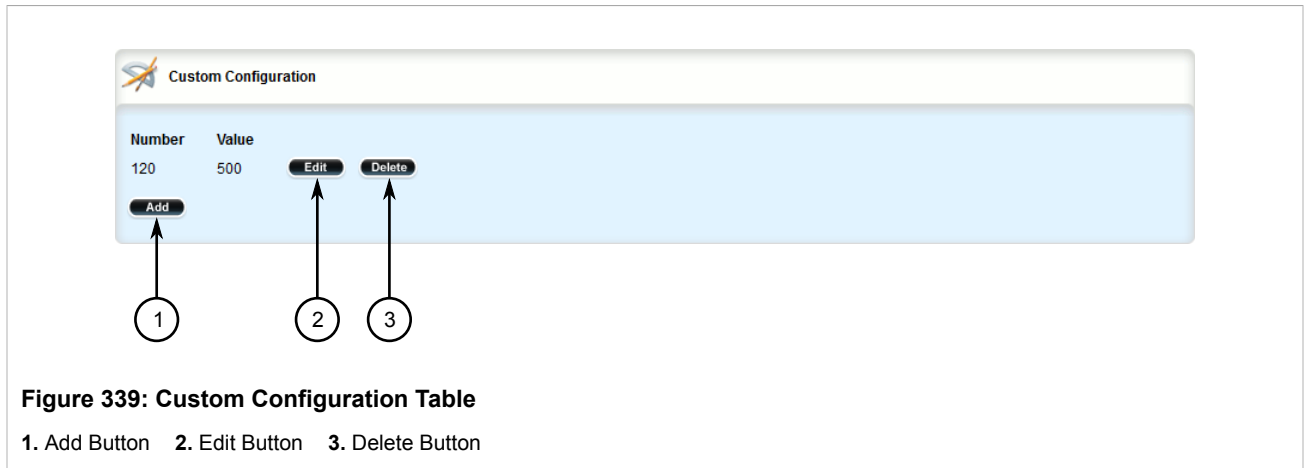
#### Section 5.14.10.3

### Deleting Custom Host Client Configurations

To delete a custom configuration for a host client on the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » hosts » {host} » options » client » custom**, where {host} is the name of the host. The **Custom Configuration** table appears.





3. Click **Delete** next to the chosen custom configuration.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.14.11

## 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.

The following sections describe how to configure and manage host groups on a DHCP server:

- [Section 5.14.11.1, “Viewing a List of Host Groups”](#)
- [Section 5.14.11.2, “Adding a Host Group”](#)
- [Section 5.14.11.3, “Configuring Host Group Options”](#)
- [Section 5.14.11.4, “Configuring a Host Group Client”](#)
- [Section 5.14.11.5, “Deleting a Host Group”](#)

#### Section 5.14.11.1

### Viewing a List of Host Groups

To view a list of host groups, navigate to **services » dhcpserver » host-groups**. If host groups have been configured, the **Host Group Configuration** table appears.

Name
Local Group

**Figure 340: Host Group Configuration Table**

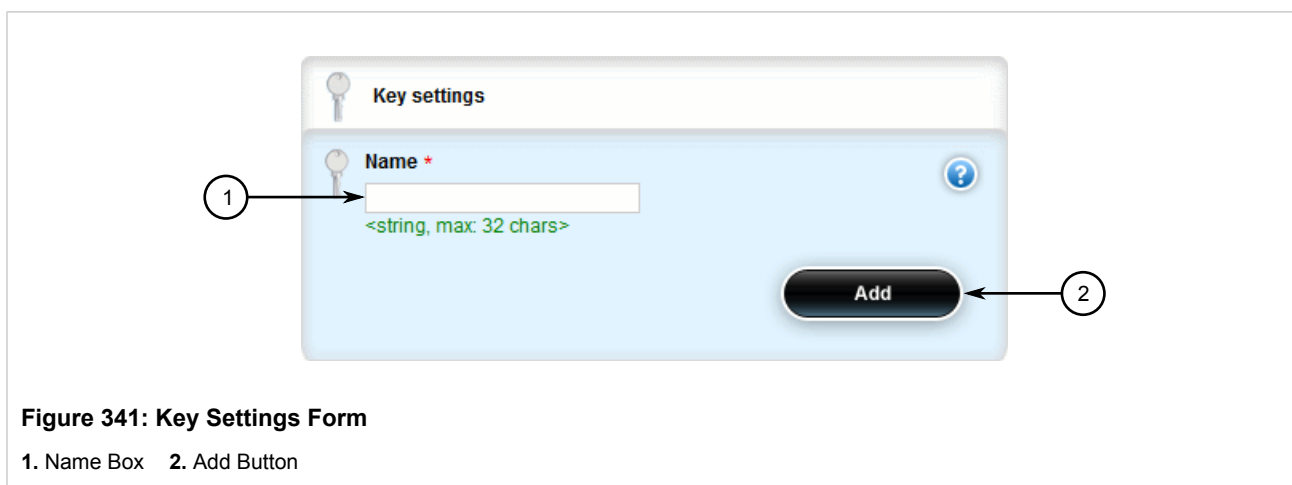
If no host groups have been configured, add host groups as needed. For more information, refer to [Section 5.14.11.2, “Adding a Host Group”](#).

#### Section 5.14.11.2

### Adding a Host Group

To add a host group to the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » host-groups** and click **<Add host-groups>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 32 characters long The description of the host groups.

4. Click **Add** to create the new host group.
5. Configure the options for the host group. For more information, refer to [Section 5.14.11.3, “Configuring Host Group Options”](#)
6. Configure the client for the host group. For more information, refer to [Section 5.14.11.4, “Configuring a Host Group Client”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.14.11.3

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » host-groups » {host} » options**, where {host} is the name of the host group. The **Leased Configuration** and **Client Configuration** forms appear.

**Figure 342: Leased Configuration Form**

1. Default Box 2. Maximum Box

**Figure 343: Client Configuration Form**

1. Unknown Client Llist 2. Shared Network Llist 3. Subnet Llist

3. On the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	<b>Default:</b> 600 The minimum leased time in seconds that the server offers to the client.
maximum	<b>Default:</b> 7200

Parameter	Description
	The maximum leased time in seconds that the server offers to the clients.

- On the **Client Configuration** form, configure the following parameters as required:

Parameter	Description
unknown-client	<b>Synopsis:</b> { allow, deny, ignore } <b>Default:</b> allow The action to take for previously unregistered clients.
shared-network	The shared network that this host group belongs to.
subnet	The subnet that this host group belongs to.

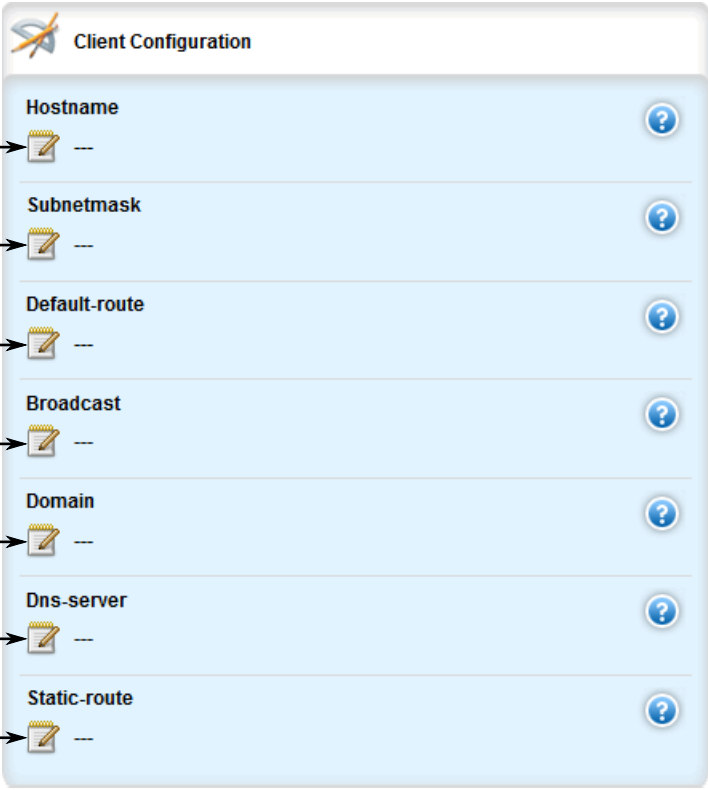
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.11.4

### Configuring a Host Group Client

To configure a client for a host on the DHCP Server, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » host-groups » {host} » options » client**, where *{host}* is the name of the host group. The **Client Configuration**, **NIS Configuration** and **NetBios Configuration** forms appear.

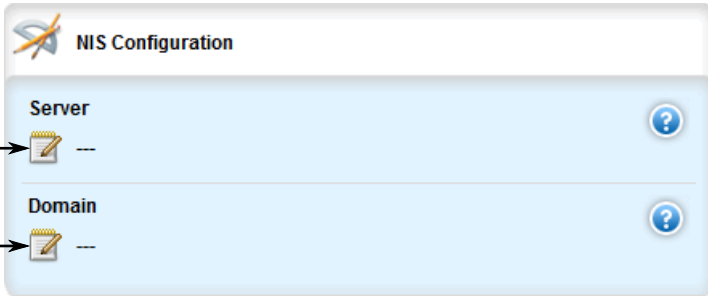


The Client Configuration form is a light blue panel with a white header containing a blue icon and the title "Client Configuration". It contains seven rows, each with a label, a text input field with a yellow notepad icon, and a blue circular help button with a question mark. The rows are: Hostname, Subnetmask, Default-route, Broadcast, Domain, Dns-server, and Static-route. To the left of the form, seven numbered circles (1-7) have arrows pointing to the input fields of the corresponding rows.

Field	Value
1. Hostname	---
2. Subnetmask	---
3. Default-route	---
4. Broadcast	---
5. Domain	---
6. Dns-server	---
7. Static-route	---

**Figure 344: Client Configuration Form**

1. Hostname Box   2. Subnet Mask Box   3. Default Route Box   4. Broadcast Box   5. Domain Box   6. DNS Server Box   7. Static Route Box



The NIS Configuration form is a light blue panel with a white header containing a blue icon and the title "NIS Configuration". It contains two rows: Server and Domain. Each row has a text input field with a yellow notepad icon and a blue circular help button with a question mark. To the left of the form, two numbered circles (1-2) have arrows pointing to the input fields of the corresponding rows.

Field	Value
1. Server	---
2. Domain	---

**Figure 345: NIS Configuration Form**

1. Server Box   2. Domain Box



**Figure 346: NetBios Configuration Form**

1. Scope Box 2. Net Server Box

- On the **Client Configuration** form, configure the following parameters as required:

Parameter	Description
hostname	<b>Synopsis:</b> A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.
subnetmask	<b>Synopsis:</b> A string 7 to 15 characters long Subnet mask
default-route	<b>Synopsis:</b> 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	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long The domain name that the server offers to the client when it issues the lease to the client.
dns-server	<b>Synopsis:</b> A string 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	<b>Synopsis:</b> 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.

- On the **NIS Configuration** form, configure the following parameters as required:

Parameter	Description
server	<b>Synopsis:</b> 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	<b>Synopsis:</b> A string 1 to 256 characters long

Parameter	Description
	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.

- On the **NetBios Configuration** form, configure the following parameters as required:

Parameter	Description
scope	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
nameserver	<b>Synopsis:</b> A string 1 to 256 characters long <b>Default:</b> 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

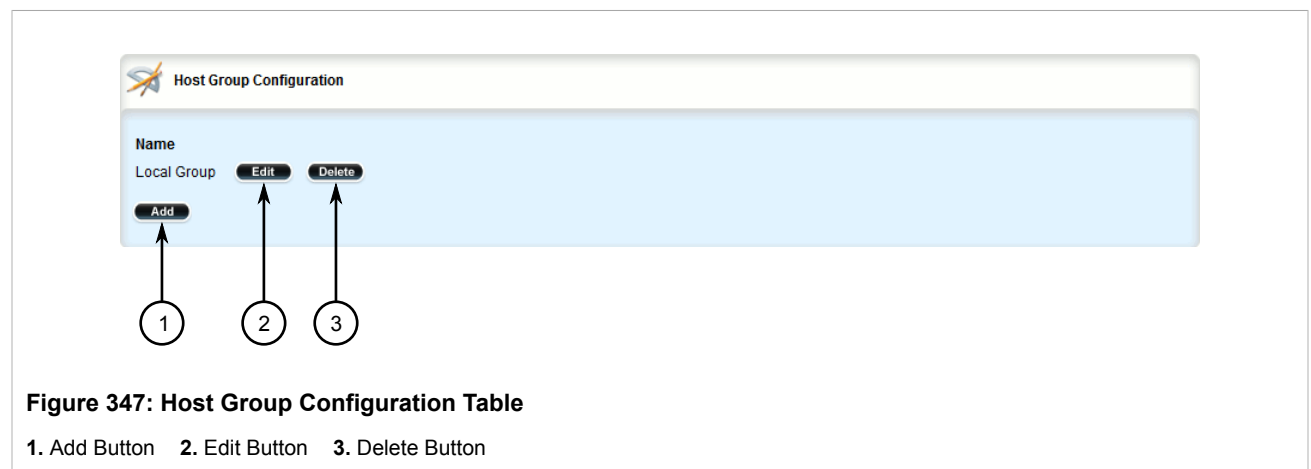
- If custom configuration settings are required for the host group client, refer to [Section 5.14.12, “Managing Custom Host Group Client Configurations”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.11.5

### Deleting a Host Group

To delete a host group, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » host-groups**. The **Host Group Configuration** table appears.



- Click **Delete** next to the chosen host group.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.12

## Managing Custom Host Group Client Configurations

Custom configuration settings can be set for each host group client.

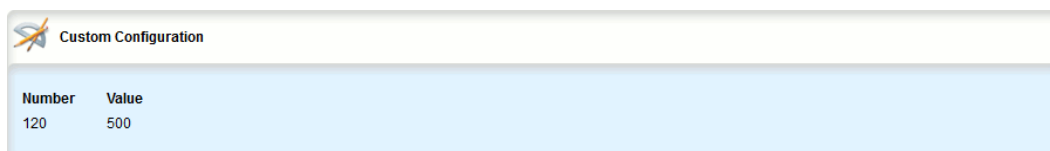
The following sections describe how to configure and manage custom host group client configurations on a DHCP server:

- [Section 5.14.12.1, “Viewing a List of Custom Host Group Client Configurations”](#)
- [Section 5.14.12.2, “Adding Custom Host Group Client Configurations”](#)
- [Section 5.14.12.3, “Deleting Custom Host Group Client Configurations”](#)

## Section 5.14.12.1

### Viewing a List of Custom Host Group Client Configurations

To view a list of custom configurations for host group clients on the DHCP server, navigate to **services » dhcpserver » host-groups » {host} » options » client » custom**, where {host} is the name of the host group. If custom configurations have been configured, the **Custom Configuration** table appears.



Number	Value
120	500

Figure 348: Custom Configuration Table

If no custom configurations have been configured for the host group client, add custom configurations as needed. For more information, refer to [Section 5.14.10.2, “Adding Custom Host Client Configurations”](#).

## Section 5.14.12.2

### Adding Custom Host Group Client Configurations

To add a custom configuration to a host group client on the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » host-groups » {host} » options » client » custom**, where {host} is the name of the host group.
3. Click **<Add custom>**. The **Key Settings** form appears.



**Figure 349: Key Settings Form**

1. Number Box   2. Value Box   3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
number	
value	The value of the custom option.

5. Click **Add** to create the new custom configuration.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.14.12.3

### Deleting Custom Host Group Client Configurations

To delete a custom configuration for a host group client on the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » host-groups » {host} » options » client » custom**, where *{host}* is the name of the host group. The **Custom Configuration** table appears.

Number	Value
120	500

**Figure 350: Custom Configuration Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen custom configuration.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.14.13

## Managing IP Pools

The following sections describe how to configure and manage IP pools for DHCP subnets:

- [Section 5.14.13.1, “Viewing a List of IP Pools”](#)
- [Section 5.14.13.2, “Adding an IP Pool”](#)
- [Section 5.14.13.3, “Deleting an IP Pool”](#)

#### Section 5.14.13.1

### Viewing a List of IP Pools

To view a list of IP pools configured for a DHCP subnet, navigate to **services » dhcpserver » subnet » {name} » options » ippool**, where *{name}* is the name of the subnet. If pools have been configured, the **IP Pool Configuration** table appears.

Description	Unknown-client	Failover-peer
pool1	not found	not found

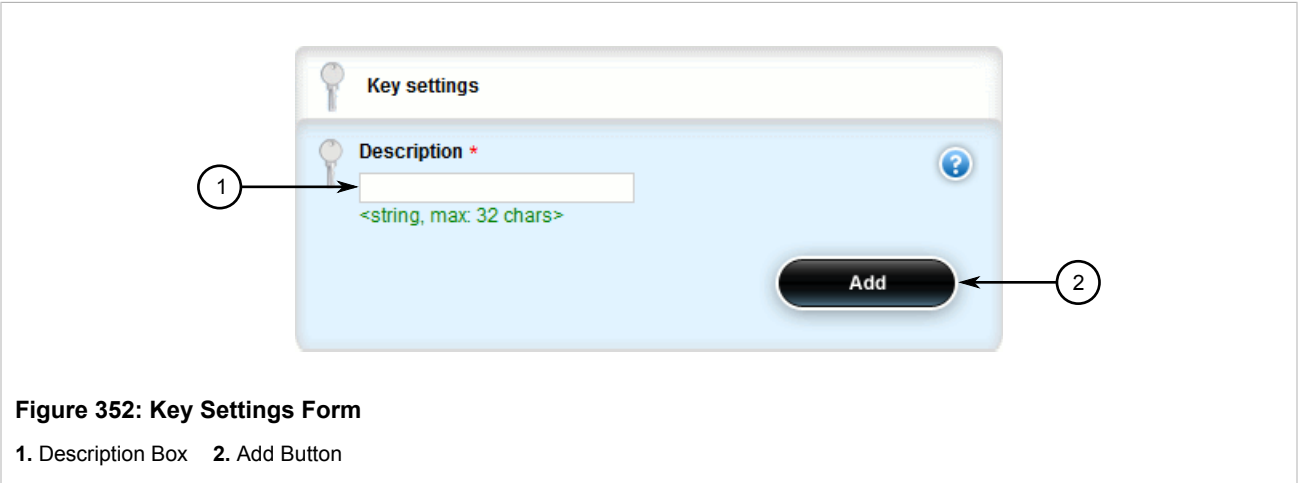
**Figure 351: IP Pool Configuration Table**

If no IP pools have been configured, add pools as needed. For more information, refer to [Section 5.14.13.2, “Adding an IP Pool”](#).

Section 5.14.13.2

Adding an IP Pool

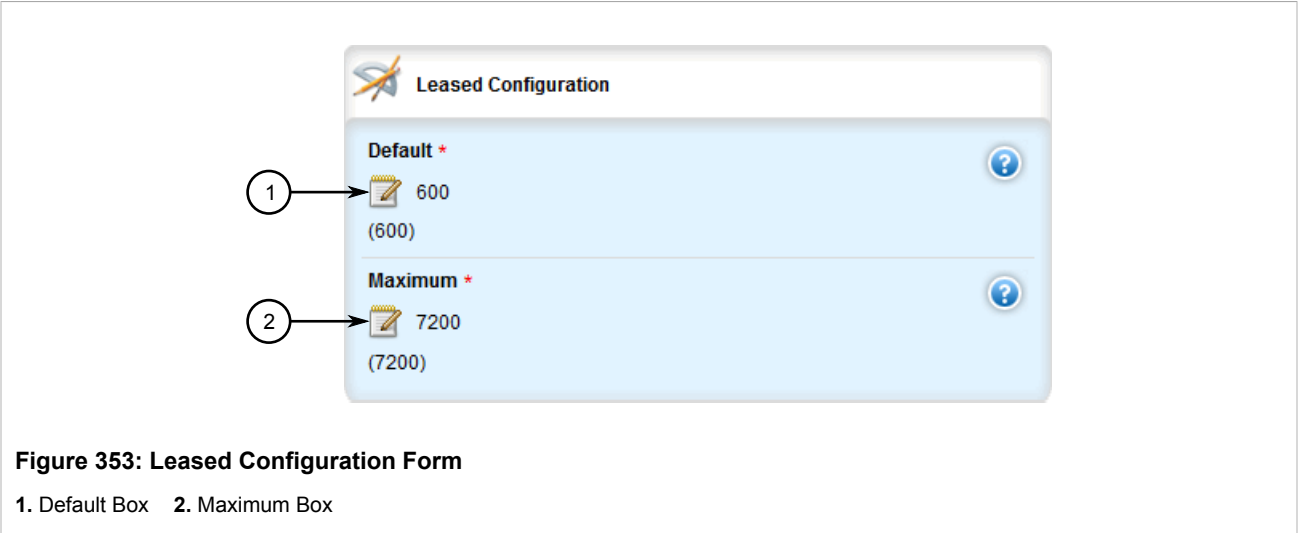
- To add an IP pool to a DHCP subnet, do the following:
1. Change the mode to **Edit Private** or **Edit Exclusive**.
  2. Navigate to **services » dhcpserver » subnet » {name} » options » ippool**, where {name} is the name of the subnet.
  3. Click **<Add ippool>**. The **Key Settings** form appears.

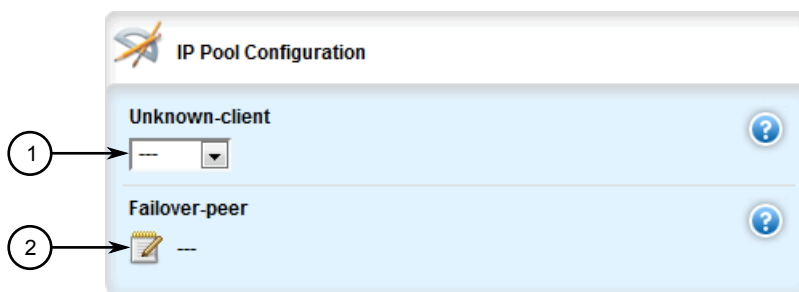


4. Configure the following parameter(s) as required:

Parameter	Description
description	<b>Synopsis:</b> A string 1 to 32 characters long Describes the IP pool.

5. Click **Add** to create the IP pool. The **Leased Configuration** and **IP Pool Configuration** forms appear.





**Figure 354: IP Pool Configuration Form**

1. Unknown Client Box    2. Failover Peer Box

6. On the **Leased Configuration** form, configure the following parameter(s) as required:

Parameter	Description
default	<b>Default:</b> 600 The minimum leased time in seconds that the server offers to the client.
maximum	<b>Default:</b> 7200 The maximum leased time in seconds that the server offers to the clients.

7. On the **IP Pool Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Unknown Client	<b>Synopsis:</b> { allow, deny, ignore } The action to take for previously unregistered clients
Failover Peer	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of a DHCP peer server if a failover pool is created.

8. Add one or more IP ranges for the pool. For more information, refer to [Section 5.14.15.2, “Adding an IP Range to an IP Pool”](#).
9. Add one or more Option82 classes to the pool. For more information, refer to [Section 5.14.16.2, “Adding an Option 82 Class to an IP Pool”](#).
10. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
11. Click **Exit Transaction** or continue making changes.

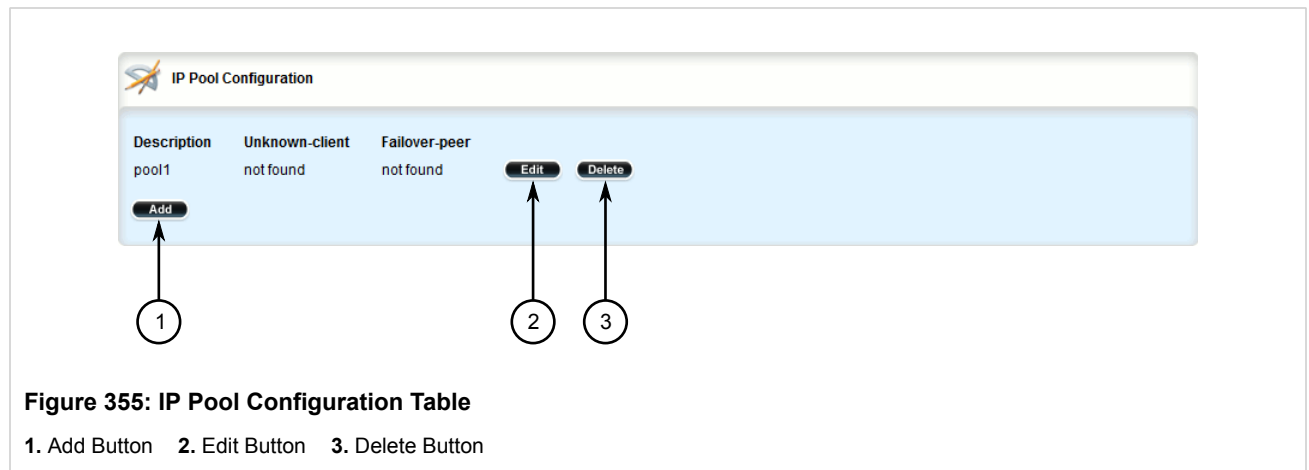
#### Section 5.14.13.3

### Deleting an IP Pool

To delete an IP pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

- Navigate to **services » dhcpserver » subnet » {name} » options » ippool**, where {name} is the name of the subnet. The **IP Pool Configuration** table appears.



- Click **Delete** next to the chosen pool.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.14

## Managing IP Ranges for Subnets

The following sections describe how to configure and manage IP ranges for DHCP subnets:

- [Section 5.14.14.1, “Viewing a List of IP Ranges for Subnets”](#)
- [Section 5.14.14.2, “Adding an IP Range to a DHCP Subnet”](#)
- [Section 5.14.14.3, “Deleting an IP Range From a Subnet”](#)

#### Section 5.14.14.1

### Viewing a List of IP Ranges for Subnets

To view a list of IP ranges configured for a DHCP subnet, navigate to **services » dhcpserver » subnet » {name} » options » iprange**, where {name} is the name of the subnet. If ranges have been configured, the **IP Range Configuration** table appears.

Start	End
172.30.144.251	172.30.144.254

**Figure 356: IP Range Configuration Table**

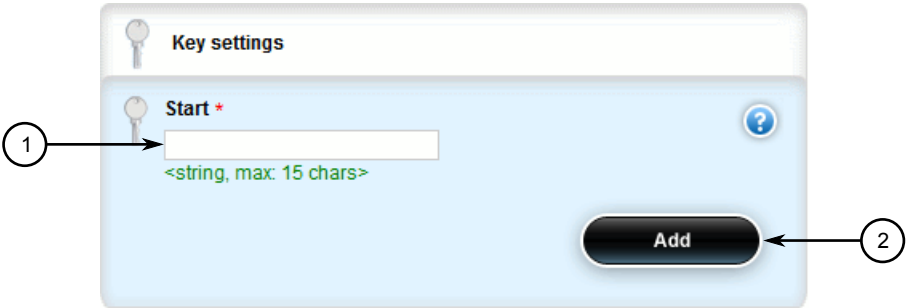
If no IP ranges have been configured, add ranges as needed. For more information, refer to [Section 5.14.14.2](#), “Adding an IP Range to a DHCP Subnet”.

#### Section 5.14.14.2

### Adding an IP Range to a DHCP Subnet

To add an IP range to a DHCP subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet » {name} » options » iprange**, where {name} is the name of the subnet.
3. Click **<Add iprange>**. The **Key Settings** form appears.



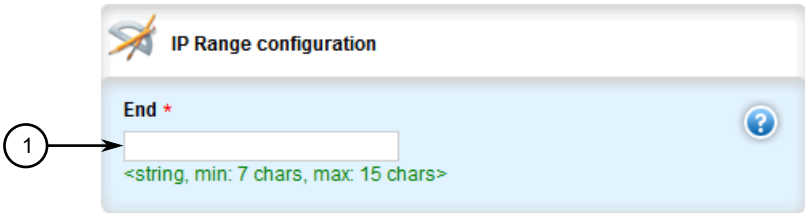
**Figure 357: Key Settings Form**

1. Start Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
start	<b>Synopsis:</b> A string 7 to 15 characters long The starting IP address pool that the server uses to offer to the client.

5. Click **Add** to create the IP range. The **IP Range Configuration** form appears.



**Figure 358: IP Range Configuration Form**

1. End Box

6. Configure the following parameter(s) as required:

Parameter	Description
end	<b>Synopsis:</b> A string 7 to 15 characters long The ending IP address pool that the server uses to offer to the client.

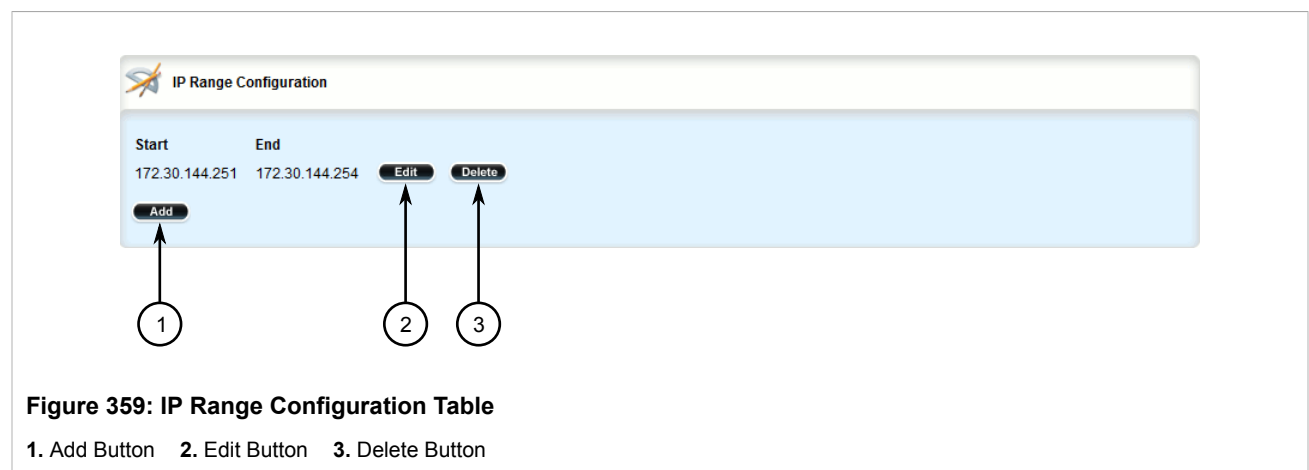
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.14.3

## Deleting an IP Range From a Subnet

To delete an IP range from a DHCP subnet, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » subnet » {name} » options » iprange**, where {name} is the name of the subnet. The **IP Range Configuration** table appears.



- Click **Delete** next to the chosen IP range.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.15

## Managing IP Ranges for IP Pools

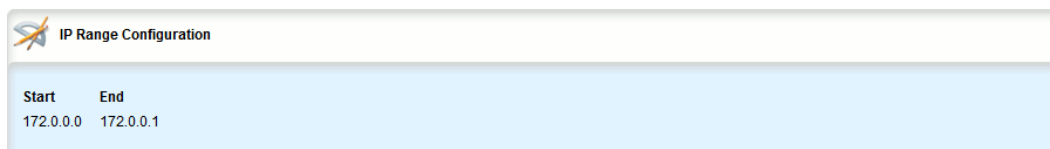
The following sections describe how to configure and manage IP ranges for IP pools:

- [Section 5.14.15.1, "Viewing a List of IP Ranges for IP Pools"](#)
- [Section 5.14.15.2, "Adding an IP Range to an IP Pool"](#)
- [Section 5.14.15.3, "Deleting an IP Range From an IP Pool"](#)

#### Section 5.14.15.1

### Viewing a List of IP Ranges for IP Pools

To view a list of IP ranges configured for an IP pool, navigate to **services » dhcpserver » subnet » {name} » options » ippool » {description} » iprange**, where {name} is the name of the subnet and {description} is the name of the IP pool. If ranges have been configured, the **IP Range Configuration** table appears.



Start	End
172.0.0.0	172.0.0.1

**Figure 360: IP Range Configuration Table**

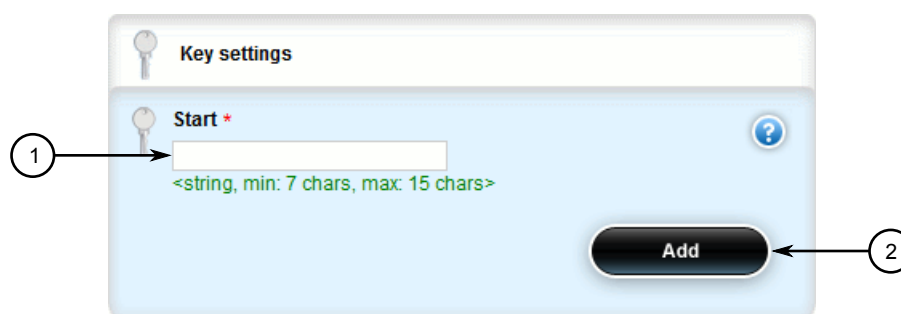
If no IP ranges have been configured, add ranges as needed. For more information, refer to [Section 5.14.15.2, “Adding an IP Range to an IP Pool”](#).

#### Section 5.14.15.2

### Adding an IP Range to an IP Pool

To add an IP range to an IP pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet » {name} » options » ippool » {description} » iprange**, where {name} is the name of the subnet and {description} is the name of the IP pool.
3. Click **<Add iprange>**. The **Key Settings** form appears.



**Figure 361: Key Settings Form**

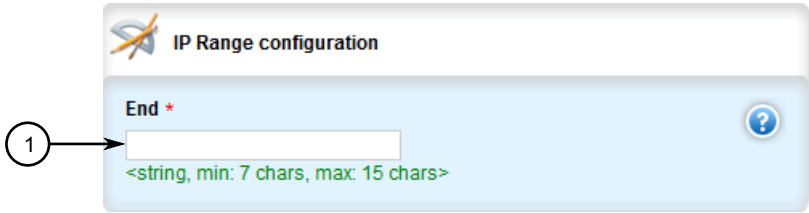
1. Start Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
start	<b>Synopsis:</b> A string 7 to 15 characters long The starting IP address pool that the server uses to offer to the client.



- Click **Add** to create the IP range. The **IP Range Configuration** form appears.



**Figure 362: IP Range Configuration Form**

1. End Box

- Configure the following parameter(s) as required:

Parameter	Description
end	<b>Synopsis:</b> A string 7 to 15 characters long The ending IP address pool that the server uses to offer to the client.

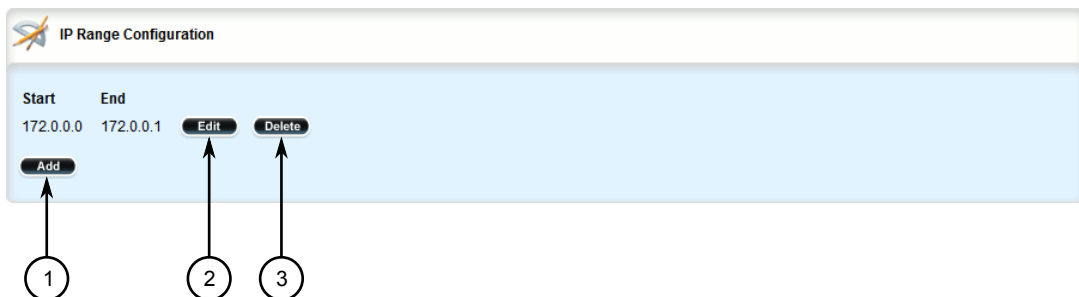
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.14.15.3

### Deleting an IP Range From an IP Pool

To delete an IP range from an IP Pool, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » subnet » {name} » options » ippool » {description} » iprange**, where **{name}** is the name of the subnet and **{description}** is the name of the IP pool. The **IP Range Configuration** table appears.



**Figure 363: IP Range Configuration Table**

1. Add Button   2. Edit Button   3. Delete Button

- Click **Delete** next to the chosen IP range.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.14.16

## Managing Option 82 Classes for IP Pools

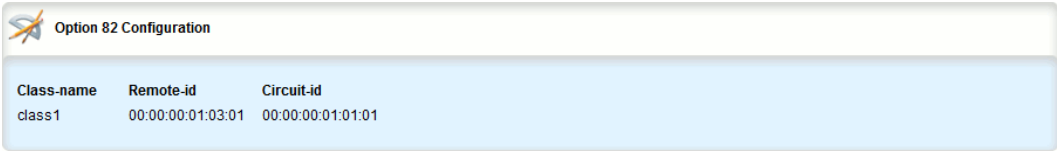
The following sections describe how to configure and manage Option82 classes for IP pools:

- [Section 5.14.16.1, “Viewing a List of Option 82 Classes for IP Pools”](#)
- [Section 5.14.16.2, “Adding an Option 82 Class to an IP Pool”](#)
- [Section 5.14.16.3, “Deleting an Option 82 Class From an IP Pool”](#)

## Section 5.14.16.1

### Viewing a List of Option 82 Classes for IP Pools

To view a list of Option 82 classes configured for an IP pool, navigate to **services » dhcpserver » subnet » {name} » options » ippool » {description} » option82**, where *{name}* is the name of the subnet and *{description}* is the name of the IP pool. If classes have been configured, the **Option 82 Configuration** table appears.

A screenshot of the 'Option 82 Configuration' table in a web interface. The table has three columns: 'Class-name', 'Remote-id', and 'Circuit-id'. There is one row with the values 'class1', '00:00:00:01:03:01', and '00:00:00:01:01:01'.

Class-name	Remote-id	Circuit-id
class1	00:00:00:01:03:01	00:00:00:01:01:01

Figure 364: Option 82 Configuration Table

If no Option 82 classes have been configured, add classes as needed. For more information, refer to [Section 5.14.16.2, “Adding an Option 82 Class to an IP Pool”](#).

## Section 5.14.16.2

### Adding an Option 82 Class to an IP Pool

To add an Option 82 class to an IP pool, do the following:

**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.

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » dhcpserver » subnet » {name} » options » ippool » {description} » option82**, where *{name}* is the name of the subnet and *{description}* is the name of the IP pool.
- Click **<Add option82>**. The **Key Settings** form appears.

A screenshot of the 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a light blue panel. Inside this panel, there is a label 'Class-name \*' followed by a text input box. Below the input box is the text '<string, max: 32 chars>'. To the right of the input box is a blue circular help icon with a question mark. At the bottom right of the panel is a black button with the text 'Add'. A circled number '1' with an arrow points to the input box, and a circled number '2' with an arrow points to the 'Add' button.

**Figure 365: Key Settings Form**  
1. Class Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Class Name	<b>Synopsis:</b> A string 1 to 32 characters long The class name of option 82.

5. Click **Add** to create the class. The **Option 82 Configuration** form appears.

A screenshot of the 'Option 82 Configuration' form. It has a title bar with a wrench and screwdriver icon and the text 'Option 82 Configuration'. Below the title bar is a light blue panel. Inside this panel, there are two sections. The first section has a label 'Remote-id \* U' followed by a text input box. Below the input box is the text '<string, must be exactly 17 chars>'. To the right of the input box is a blue circular help icon with a question mark. The second section has a label 'Circuit-id \* U' followed by a text input box. Below the input box is the text '<string, must be exactly 17 chars>'. To the right of the input box is a blue circular help icon with a question mark. A circled number '1' with an arrow points to the 'Remote-id' input box, and a circled number '2' with an arrow points to the 'Circuit-id' input box.

**Figure 366: Option 82 Configuration Form**  
1. Remote ID Box    2. Circuit ID Box

6. Configure the following parameter(s) as required:

Parameter	Description
remote-id	<b>Synopsis:</b> A string Specifies the information relating to the remote host end of the circuit.
circuit-id	<b>Synopsis:</b> A string 1 to 17 characters long Specifies the local information to which circuit the request came in on (ie. 00:02:03:02)

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

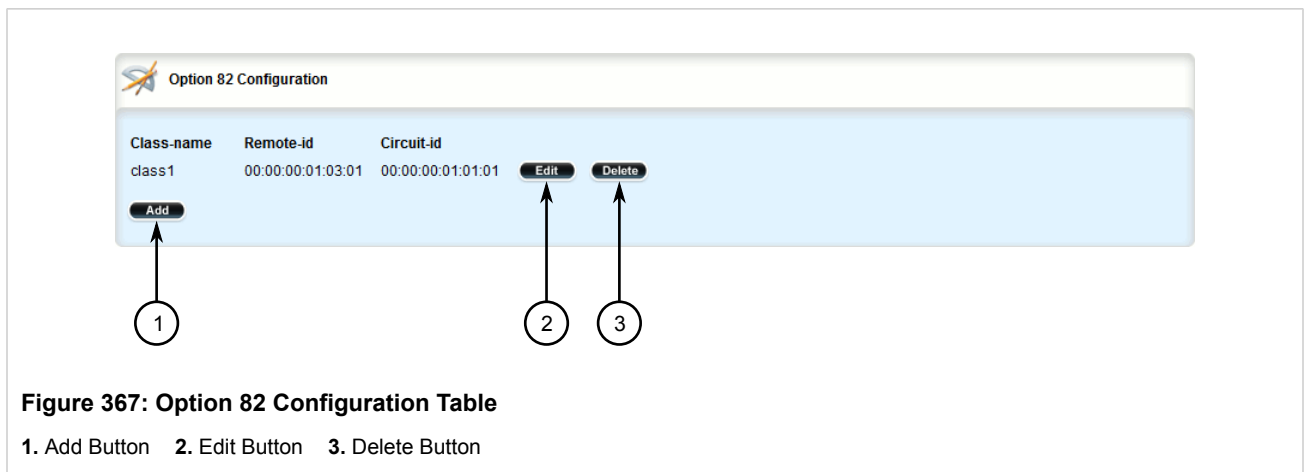
8. Click **Exit Transaction** or continue making changes.

#### Section 5.14.16.3

### Deleting an Option 82 Class From an IP Pool

To delete an Option 82 class from an IP Pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » dhcpserver » subnet » {name} » options » ippool » {description} » option82**, where *{name}* is the name of the subnet and *{description}* is the name of the IP pool. The **Option 82 Configuration** table appears.



3. Click **Delete** next to the chosen class.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.15

## 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.

The following sections describe how to configure and manage port mirroring:

- [Section 5.15.1, “Configuring Port Mirroring”](#)
- [Section 5.15.2, “Managing Egress Source Ports”](#)
- [Section 5.15.3, “Managing Ingress Source Ports”](#)

## Section 5.15.1

## Configuring Port Mirroring

To configure port mirroring, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » port-mirroring**. The **Port Mirror** form appears.

**Figure 368: Port Mirror Form**

1. Target Slot List    2. Admin State Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Target Slot	The slot where a monitoring device should be connected.
Target Port	The port where a monitoring device should be connected.
Admin State	<b>Synopsis:</b> typeless Enabling port mirroring causes all frames received and/or transmitted by the source port to be transmitted out of the target port.

4. Add egress and ingress source ports. For more information, refer to [Section 5.15.2.2, “Adding an Egress Source Port”](#) and [Section 5.15.3.2, “Adding an Ingress Source Port”](#).

5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

## Section 5.15.2

## Managing Egress Source Ports

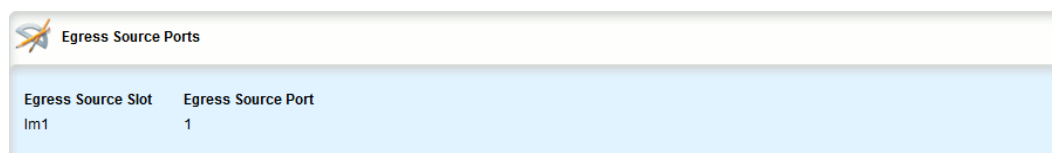
The following sections describe how to configure and manage egress source ports for port mirroring:

- [Section 5.15.2.1, “Viewing a List of Egress Source Ports”](#)
- [Section 5.15.2.2, “Adding an Egress Source Port”](#)
- [Section 5.15.2.3, “Deleting an Egress Source Port”](#)

## Section 5.15.2.1

### Viewing a List of Egress Source Ports

To view a list of egress source ports for port mirroring, navigate to **switch » port-mirroring » egress-src**. If source ports have been configured, the **Egress Source Ports** table appears.



The screenshot shows a web interface window titled "Egress Source Ports". Inside, there is a table with two columns: "Egress Source Slot" and "Egress Source Port". The table contains one row with the values "Im1" and "1".

Egress Source Slot	Egress Source Port
Im1	1

**Figure 369: Egress Source Ports Table**

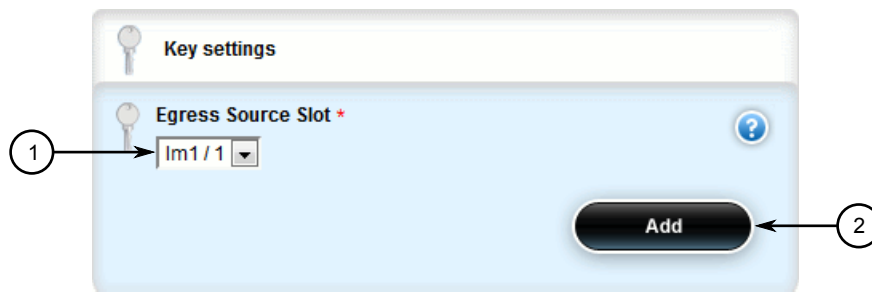
If no egress source ports have been configured, add egress source ports as needed. For more information, refer to [Section 5.15.2.2, “Adding an Egress Source Port”](#).

## Section 5.15.2.2

### Adding an Egress Source Port

To add an egress source port for port mirroring, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » port-mirroring » egress-src** and click **<Add egress-src>**. The **Key Settings** form appears.



**Figure 370: Key Settings Form**

1. Egress Source Slot List    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
Egress Source Slot	The name of the module location provided on the silkscreen across the top of the device.
Egress Source Port	The selected ports on the module installed in the indicated slot.

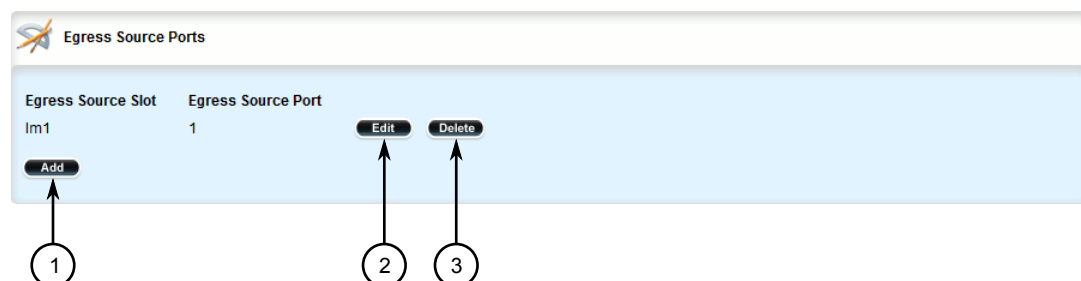
- Click **Add** to create the new egress source port.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.15.2.3

### Deleting an Egress Source Port

To delete an egress source port for port mirroring, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » port-mirroring » egress-src**. The **Egress Source Ports** table appears.



**Figure 371: Egress Source Ports Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen source port.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.15.3

## Managing Ingress Source Ports

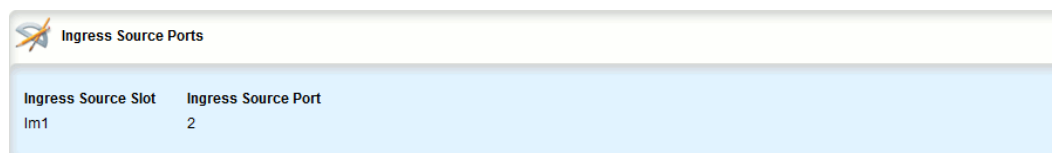
The following sections describe how to configure and manage ingress source ports for port mirroring:

- [Section 5.15.3.1, “Viewing a List of Ingress Source Ports”](#)
- [Section 5.15.3.2, “Adding an Ingress Source Port”](#)
- [Section 5.15.3.3, “Deleting an Ingress Source Port”](#)

## Section 5.15.3.1

### Viewing a List of Ingress Source Ports

To view a list of ingress source ports for port mirroring, navigate to **switch » port-mirroring » ingress-src**. If source ports have been configured, the **Ingress Source Ports** table appears.



The screenshot shows a web interface titled "Ingress Source Ports" with a table containing one row of data.

Ingress Source Slot	Ingress Source Port
Im1	2

**Figure 372: Ingress Source Ports Table**

If no ingress source ports have been configured, add ingress source ports as needed. For more information, refer to [Section 5.15.3.2, “Adding an Ingress Source Port”](#).

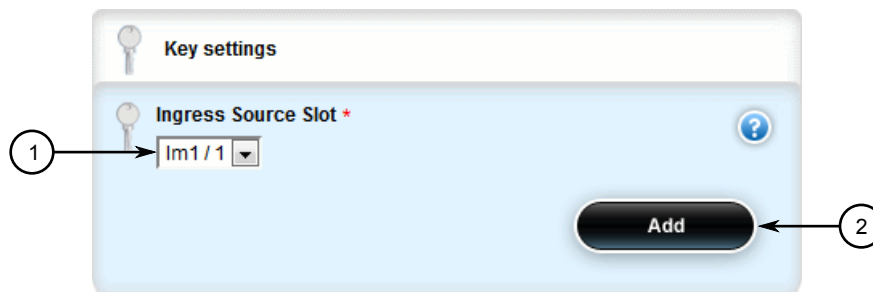
## Section 5.15.3.2

### Adding an Ingress Source Port

To add an ingress source port for port mirroring, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » port-mirroring » ingress-src** and click **<Add ingress-src>**. The **Key Settings** form appears.





**Figure 373: Key Settings Form**

1. Ingress Source Slot List    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
Ingress Source Slot	The name of the module location provided on the silkscreen across the top of the device.
Ingress Source Port	The selected ports on the module installed in the indicated slot.

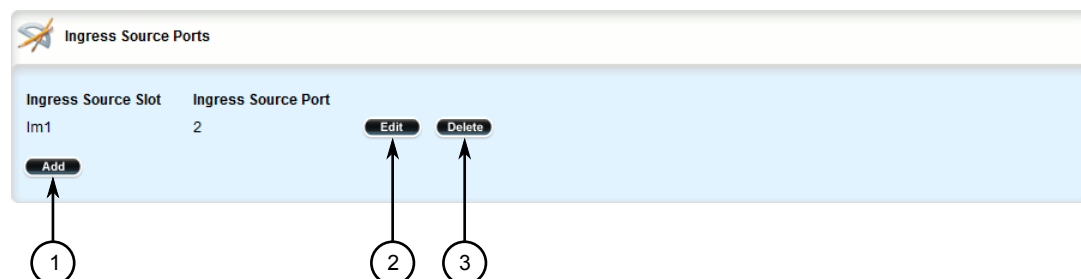
- Click **Add** to create the new ingress source port.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.15.3.3

## Deleting an Ingress Source Port

To delete an ingress source port for port mirroring, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » port-mirroring » ingress-src**. The **Ingress Source Ports** table appears.



**Figure 374: Ingress Source Ports Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen source port.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.16

# 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 5.16.1, “Firewall Concepts”](#).

The following sections describe how to configure and manage a firewall:

- [Section 5.16.2, “Viewing a List of Firewalls”](#)
- [Section 5.16.3, “Adding a Firewall”](#)
- [Section 5.16.4, “Deleting a Firewall”](#)
- [Section 5.16.5, “Working with Multiple Firewall Configurations”](#)
- [Section 5.16.9, “Managing Interfaces”](#)
- [Section 5.16.8, “Managing Zones”](#)
- [Section 5.16.11, “Managing Policies”](#)
- [Section 5.16.12, “Managing Network Address Translation Settings”](#)
- [Section 5.16.13, “Managing Masquerade and SNAT Settings”](#)
- [Section 5.16.10, “Managing Hosts”](#)
- [Section 5.16.14, “Managing Rules”](#)

- [Section 5.16.6, “Configuring the Firewall for a VPN”](#)
- [Section 5.16.7, “Configuring the Firewall for a VPN in a DMZ”](#)
- [Section 5.16.15, “Validating a Firewall Configuration”](#)
- [Section 5.16.16, “Enabling/Disabling a Firewall”](#)

#### Section 5.16.1

## Firewall Concepts

The following sections describe some of the concepts important to the implementation of firewalls in RUGGEDCOM ROX II:

- [Section 5.16.1.1, “Stateless vs. Stateful Firewalls”](#)
- [Section 5.16.1.2, “Linux netfilter”](#)
- [Section 5.16.1.3, “Network Address Translation”](#)
- [Section 5.16.1.4, “Port Forwarding”](#)
- [Section 5.16.1.5, “Protecting Against a SYN Flood Attack”](#)

#### Section 5.16.1.1

### 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 5.16.1.2

### 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.

ROX implements an IP firewall using a structured user interface to configure iptables rules and netfilter rulesets.

## Section 5.16.1.3

## 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 5.16.1.4

## 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 5.16.1.5

### 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.

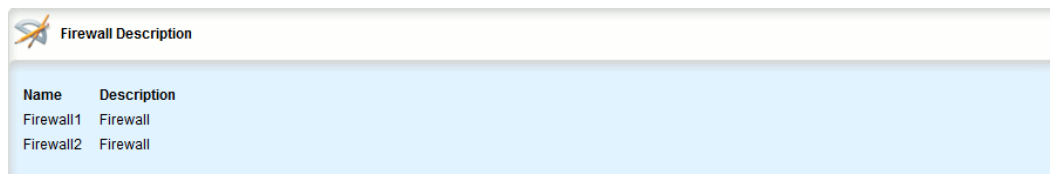
To prevent SYN flood attacks on closed ports, set the firewall to block all traffic to closed ports. This prevents SYN packets from reaching the kernel.

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 5.16.2

### Viewing a List of Firewalls

To view a list of firewalls, navigate to **security » firewall » fwconfig**. If firewalls have been configured, the **Firewall Description** table appears.

The screenshot shows a web interface window titled "Firewall Description" with a light blue header and a white body. Inside the body is a table with two columns: "Name" and "Description". There are two rows of data: "Firewall1" with description "Firewall" and "Firewall2" with description "Firewall".

Name	Description
Firewall1	Firewall
Firewall2	Firewall

Figure 375: Firewall Description Table

If no firewalls have been configured, add firewalls as needed. For more information, refer to [Section 5.16.3](#), "Adding a Firewall".

#### Section 5.16.3

### Adding a Firewall

To add a new firewall, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig** and click **<Add fwconfig>** in the menu. The **Key Settings** form appears.

**Figure 376: Key Settings Form**

1. Name Box 2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string

- Click **Add**. The **Firewall Description** form appears.

**Figure 377: Firewall Description Form**

1. Description Box

- Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string An optional description string.

- Add interfaces associated with the firewall. For more information about adding interfaces, refer to [Section 5.16.9.2, “Adding an Interface”](#).
- 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 5.16.8.2, “Adding a Zone”](#).
- Associate an interface with each zone. For more information about associating interfaces with zones, refer to [Section 5.16.9.3, “Associating an Interface with a Zone”](#).
- 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 5.16.11, “Managing Policies”](#).
- Configure the network address translation (NAT), masquerading or static network address translation (SNAT) settings. For more information about configuring NAT settings, refer to [Section 5.16.12, “Managing Network](#)

[Address Translation Settings](#). For more information about configuring masquerading and/or SNAT settings, refer to [Section 5.16.13, “Managing Masquerade and SNAT Settings”](#).

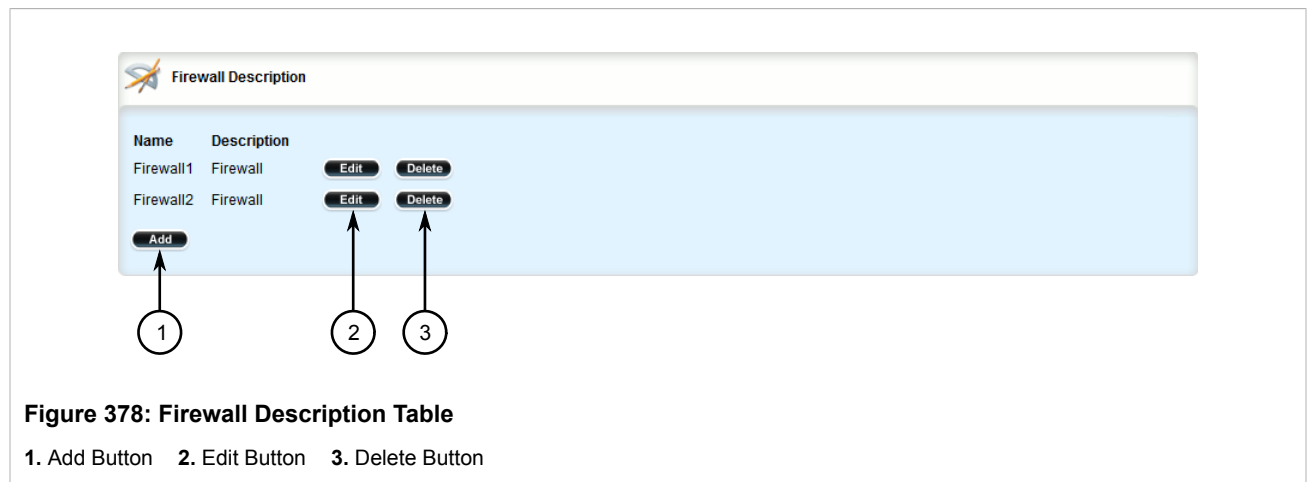
11. If hosts on the network must accept sessions from the Internet, configure the firewall to support Destination Network Address Translation (DNAT). For more information about configuring hosts, refer to [Section 5.16.10, “Managing Hosts”](#).
12. If required, configure rules that override the default policies. For more information about configuring rules, refer to [Section 5.16.14, “Managing Rules”](#).
13. If required, configure support for a VPN. For more information, refer to:
  - [Section 5.16.6, “Configuring the Firewall for a VPN”](#)
  - [Section 5.16.7, “Configuring the Firewall for a VPN in a DMZ”](#)
14. Validate the configuration. For more information about validating a firewall configuration, refer to [Section 5.16.15, “Validating a Firewall Configuration”](#).
15. Enable the firewall. For more information, refer to [Section 5.16.16, “Enabling/Disabling a Firewall”](#).
16. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
17. Click **Exit Transaction** or continue making changes.

#### Section 5.16.4

## Deleting a Firewall

To delete a firewall, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig**. The **Firewall Description Settings** table appears.



3. Click **Delete** next to the chosen firewall.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

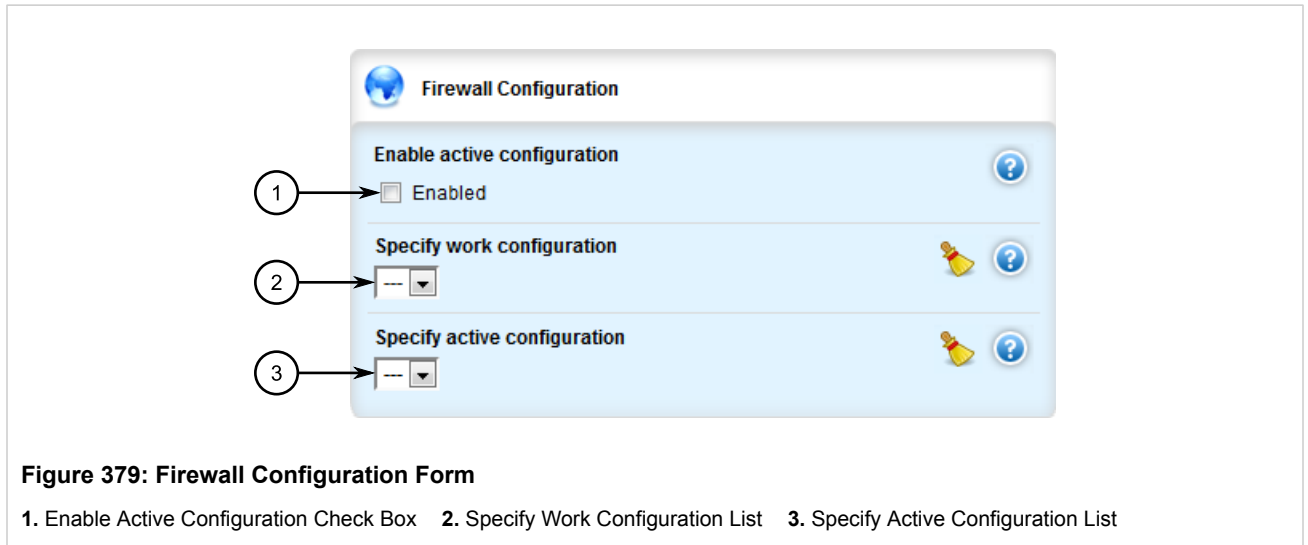
Section 5.16.5

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall**. The **Firewall Configuration** form appears.



3. Under **Specify work configuration**, select a firewall configuration from the list to work on. The firewall configuration selected under **Specify active configuration** is the configuration that is actively running.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.16.6

## 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 5.16.3, "Adding a Firewall"](#).
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to **security » firewall » fwconfig** and select the firewall to configure.
4. Make sure zones for local, network and VPN traffic have been configured. For more information about managing zones, refer to [Section 5.16.8, "Managing Zones"](#).
5. Make sure a zone called *Any* exists and is of the type IPsec. For more information about managing zones, refer to [Section 5.16.8, "Managing Zones"](#).



6. 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 5.16.9.3, “Associating an Interface with a Zone”](#).
7. 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 5.16.10, “Managing Hosts”](#).
8. 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 5.16.10, “Managing Hosts”](#).

**NOTE**

*The VPN host must be specified before the network host so the more specific VPN zone subnet can be inspected first.*

**Table: Example**

Host	Interface	Subnet	IPsec Zone
vpn	W1ppp	192.168.1.0/24	Yes
net	W1ppp	0.0.0.0/0	No

9. 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.*

**Table: Example**

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 5.16.14, “Managing Rules”](#).

10. Configure the following rule to allow traffic from openswan, the IPsec daemon, to enter the firewall:

**NOTE**

*IPsec traffic arriving at the firewall is directed to openswan, the IPsec daemon. Openswan 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.*

**Table: Example**

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	vpn	loc	—	—

For more information about configuring rules, refer to [Section 5.16.14, “Managing Rules”](#).

## Section 5.16.7

## 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 5.16.3, “Adding a Firewall”](#).
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to **security » firewall » fwconfig** and select the firewall to configure.
4. Make sure a zone called *dmz* exists. For more information about managing zones, refer to [Section 5.16.8, “Managing Zones”](#).
5. 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.*

**Table: Example**

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 5.16.14, “Managing Rules”](#).

## Section 5.16.8

## Managing Zones

A network zone is a collection of interfaces for which forwarding decisions are made. Common zones include:

**Table: Example**

Zone	Description
Net	The Internet
Loc	The local network
DMZ	Demilitarized zone
Fw	The firewall itself

Zone	Description
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.

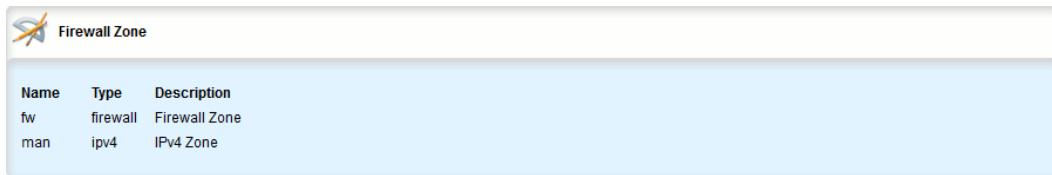
The following sections describe how to configure and manage zones for a firewall:

- [Section 5.16.8.1, “Viewing a List of Zones”](#)
- [Section 5.16.8.2, “Adding a Zone”](#)
- [Section 5.16.8.3, “Deleting a Zone”](#)

#### Section 5.16.8.1

### Viewing a List of Zones

To view a list of zones, navigate to **security » firewall » fwconfig » {firewall} » fwzone**, where *{firewall}* is the name of the firewall. If zones have been configured, the **Firewall Zone** table appears.



Name	Type	Description
fw	firewall	Firewall Zone
man	ipv4	IPv4 Zone

**Figure 380: Firewall Zone Table**

If no zones have been configured, add zones as needed. For more information, refer to [Section 5.16.8.2, “Adding a Zone”](#).

#### Section 5.16.8.2

### Adding a Zone

To add a new zone for a firewall, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig » {firewall} » fwzone**, where *{firewall}* is the name of the firewall.
3. Click **<Add fwzone>** in the menu. The **Key Settings** form appears.

Key settings

Name \*

<string, min: 0 chars, max: 5 chars>

Add

**Figure 381: Key Settings Form**  
1. Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 0 to 5 characters long A unique name to assign to this zone. Be sure to <b>also create</b> a zone called <b>fw</b> that is of the zone type <b>firewall</b> .

5. Click **Add**. The **Firewall Zone** form appears.

Firewall Zone

Type \*

ipv4  
(ipv4)

Description

**Figure 382: Firewall Zone Form**  
1. Type List    2. Description Box

6. Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
type46	<b>Synopsis:</b> { ip, ipsec, firewall } <b>Default:</b> ip

Parameter	Description
	<b>Prerequisite:</b> ../iptype='ipv4ipv6' Zone types applying to both IPv4 and IPv6: plain IP, firewall, or IPSec
type6	<b>Synopsis:</b> { ipv6, ipsec, firewall } <b>Default:</b> ipv6 <b>Prerequisite:</b> ../iptype='ipv6' Zone types are plain IPv6, firewall, or IPSec
Type	<b>Synopsis:</b> { ipv4, ipsec, firewall } <b>Default:</b> ipv4 <b>Prerequisite:</b> ../iptype='ipv4' Zone types are plain IPv4, firewall, or IPSec
description	<b>Synopsis:</b> A string (Optional) The description string for this zone

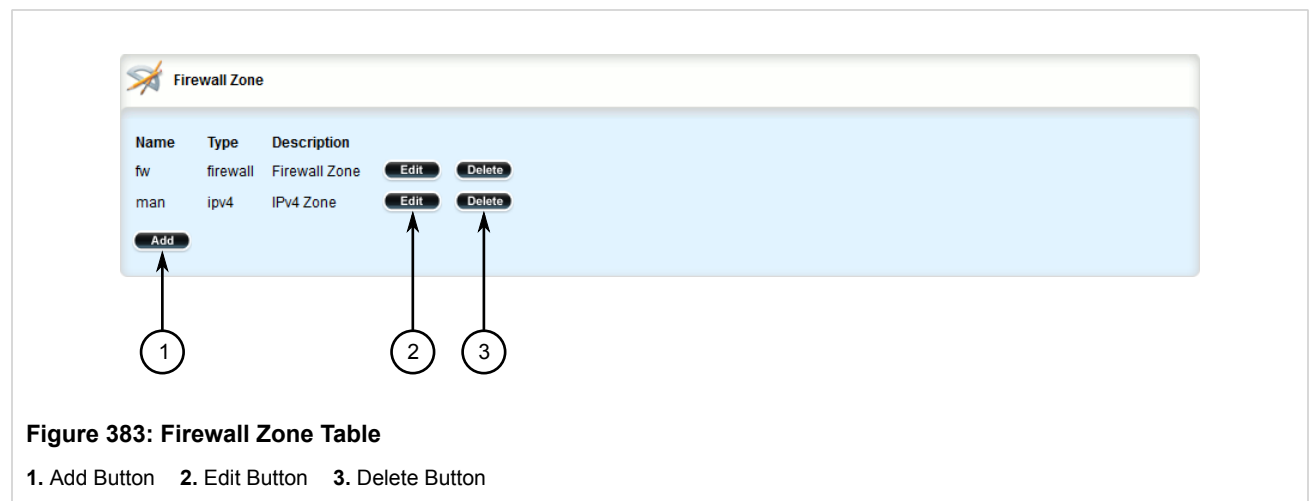
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.16.8.3

### Deleting a Zone

To delete a zone, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwzone**, where *{firewall}* is the name of the firewall. The **Firewall Zone** table appears.



- Click **Delete** next to the chosen zone.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.16.9

## 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

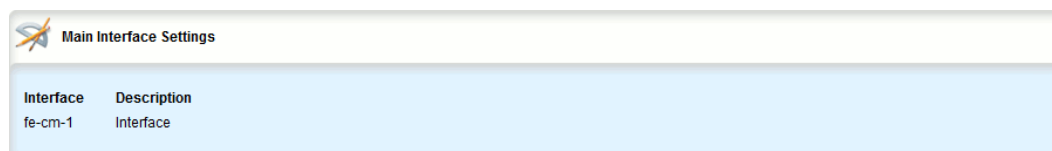
The following sections describe how to configure and manage zones for a firewall:

- [Section 5.16.9.1, “Viewing a List of Interfaces”](#)
- [Section 5.16.9.2, “Adding an Interface”](#)
- [Section 5.16.9.3, “Associating an Interface with a Zone”](#)
- [Section 5.16.9.4, “Configuring a Broadcast Address”](#)
- [Section 5.16.9.5, “Deleting an Interface”](#)

## Section 5.16.9.1

### Viewing a List of Interfaces

To view a list of interfaces, navigate to **security » firewall » fwconfig » {firewall} » fwinterface**, where *{firewall}* is the name of the firewall. If interfaces have been configured, the **Main Interface Settings** table appears.



Main Interface Settings	
Interface	Description
fe-cm-1	Interface

**Figure 384: Main Interface Settings Table**

If no interfaces have been configured, add interfaces as needed. For more information, refer to [Section 5.16.9.2, “Adding an Interface”](#).

## Section 5.16.9.2

### Adding an Interface

To configure an interface for a firewall, do the following:

1. Navigate to **ip** and record the name of the chosen interface.

2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to **security » firewall » fwconfig » {firewall} » fwinterface**, where {firewall} is the name of the firewall.
4. Click **<Add fwinterface>** in the menu. The **Key Settings** form appears.

**Figure 385: Key Settings Form**

1. Interface Box    2. Add Button

5. Insert the name of the chosen interface and then click **Add**.
6. Click **Add**. The **Main Interface Settings** and **Interface Options** forms appear.

**Figure 386: Main Interface Settings Form**

1. Description Box

1

2

3

4

5

6

7

8

9

10

Interface Options

Arp Filter

☐ Enabled

?

routeback

☐ Enabled

?

tcpflags

☐ Enabled

?

dhcp

☐ Enabled

?

norfc1918

☐ Enabled

?

routefilter

☐ Enabled

?

proxyarp

☐ Enabled

?

maclist

☐ Enabled

?

nosmurfs

☐ Enabled

?

logmartians

☐ Enabled

?

**Figure 387: Interface Options Form**

1. ARP Filter Check Box   2. Route Back Check Box   3. TCP Flags Check Box   4. DHCP Check Box   5. NORFC1918 Check Box   6. Route Filter Check Box   7. Proxy Arp Check Box   8. MAC List Check Box   9. No Smurfs Check Box   10. Log Martians Check Box

7. On the **Main Interface Settings**, configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
description	<b>Synopsis:</b> A string (Optional) The description string for this interface

8. On the **Interface Options**, configure the following parameter(s) as required:



Parameter	Description
ARP Filter	<b>Synopsis:</b> typeless IPv4 ONLY. 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	<b>Synopsis:</b> typeless IPv4 and IPv6. Allows traffic on this interface to be routed back out that same interface.
TCP Flags	<b>Synopsis:</b> typeless IPv4 and IPv6. Illegal combinations of TCP flags dropped and logged at info level.
DHCP	<b>Synopsis:</b> typeless IPv4 and IPv6. Allows DHCP datagrams to enter and leave the interface.
NORFC1918	<b>Synopsis:</b> typeless Not currently implemented
Route Filter	<b>Synopsis:</b> typeless IPv4 only. Enables route filtering.
Proxy ARP	<b>Synopsis:</b> typeless IPv4 ONLY. 1Enables proxy ARP.
MAC List	<b>Synopsis:</b> typeless IPv4 ONLY. Not currently implemented
No Smurfs	<b>Synopsis:</b> typeless IPv4 ONLY. Packets with a broadcast address as the source are dropped and logged at info level.
Log Martians	<b>Synopsis:</b> typeless IPv4 ONLY. Enables logging of packets with impossible source addresses.

- 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 5.16.9.3, “Associating an Interface with a Zone”](#)
- Configure a broadcast address for the interface. For more information configuring a broadcast address, refer to [Section 5.16.9.4, “Configuring a Broadcast Address”](#)
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

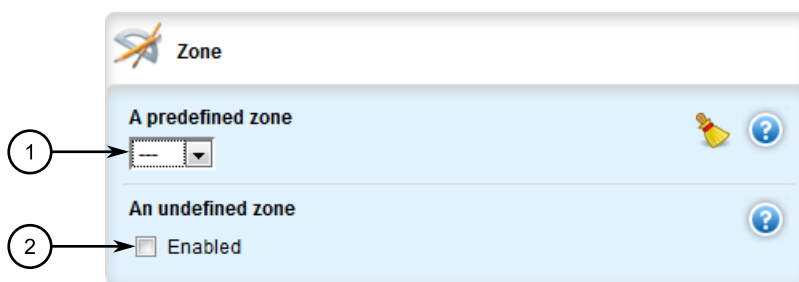
### Section 5.16.9.3

## 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:

- Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **security » firewall » fwconfig » fwconfig » {firewall} » fwinterface{interface} » zone**, where **{firewall}** is the name of the firewall and **{interface}** is the name of the interface. The **Zone** form appears.



**Figure 388: Zone Form**

1. Predefined Zone List    2. Undefined Zone Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone	A pre-defined zone
undefined-zone	This is used in conjunction with hosts definitions.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.16.9.4

### Configuring a Broadcast Address

To configure a broadcast address for an interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig » fwconfig » {firewall} » fwinterface{interface} » broadcast-addr**, where **{firewall}** is the name of the firewall and **{interface}** is the name of the interface. The **Broadcast Address** form appears.

**Figure 389: Broadcast Address Form**

1. IPv4 Address Box   2. Auto Detect Check Box   3. None Check Box

- Configure the following parameter(s) as required:

Parameter	Description
ipv4-address	<b>Synopsis:</b> A string An IPv4 address for a broadcast address.
detect	Automatic detection of the broadcast address(es).
none	The default.

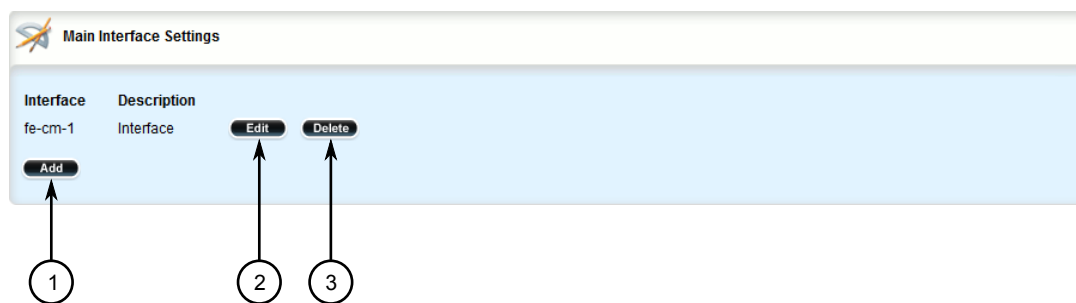
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.16.9.5

### Deleting an Interface

To delete an interface, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwinterface**, where *{firewall}* is the name of the firewall. The **Main Interface Settings** table appears.

**Figure 390: Main Interface Settings Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.16.10

## 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

The following sections describe how to configure and manage hosts for a firewall:

- [Section 5.16.10.1, “Viewing a List of Hosts”](#)
- [Section 5.16.10.2, “Adding a Host”](#)
- [Section 5.16.10.3, “Deleting a Host”](#)

#### Section 5.16.10.1

### Viewing a List of Hosts

To view a list of hosts, navigate to **security » firewall » fwconfig » {firewall} » fwhost**, where *{firewall}* is the name of the firewall. If hosts have been configured, the **Main Host Settings** table appears.

Main Host Settings				
Name	Zone	Interface	IP Address List	Description
host1	man	fe-cm-1	not found	not found

Figure 391: Main Host Settings Table

If no hosts have been configured, add hosts as needed. For more information, refer to [Section 5.16.10.2, “Adding a Host”](#).

Section 5.16.10.2

Adding a Host

To add a new host for a firewall, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to **security » firewall » fwconfig » {firewall} » fwhost**, where *{firewall}* is the name of the firewall.
- 3. Click **<Add fwhost>** in the menu. The **Key Settings** form appears.

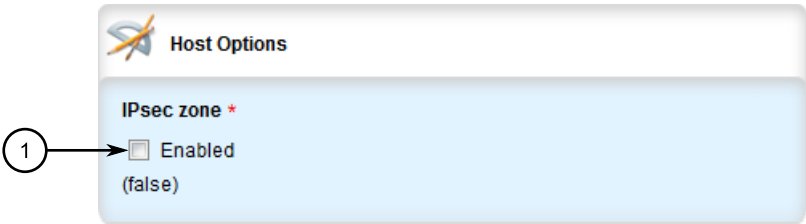
Figure 392: Key Settings Form

1. Name Box    2. Add Button

- 4. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string The name of a host configuration entry.

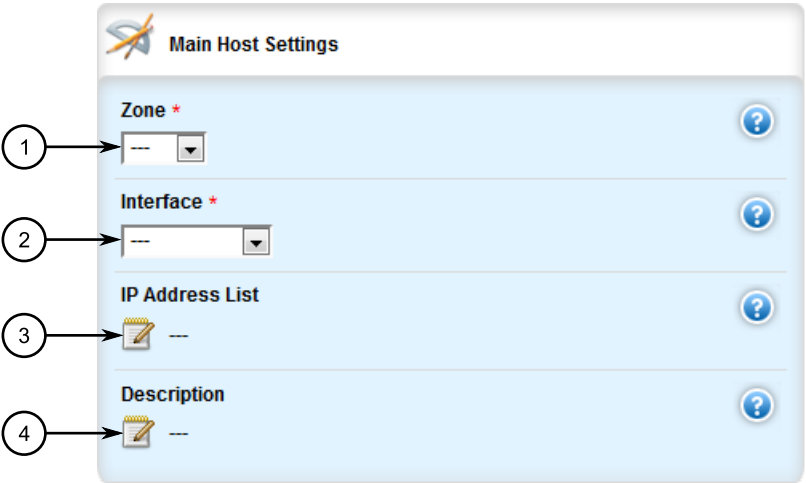
- 5. Click **Add**. The **Host Options** and **Main Host Settings** forms appear.



The image shows a web form titled "Host Options". It contains a single section labeled "IPsec zone \*" with a checkbox labeled "Enabled" and the text "(false)" below it. A circled number "1" with an arrow points to the checkbox.

Figure 393: Host Options Form

1. IPsec Zone Check Box



The image shows a web form titled "Main Host Settings". It contains four sections: "Zone \*" with a dropdown menu, "Interface \*" with a dropdown menu, "IP Address List" with a text input field and a plus icon, and "Description" with a text input field and a plus icon. Each section has a blue question mark icon to its right. Circled numbers 1 through 4 with arrows point to the dropdown menu of the Zone field, the dropdown menu of the Interface field, the plus icon of the IP Address List field, and the plus icon of the Description field, respectively.

Figure 394: Main Host Settings Form

1. Zone List   2. Interface List   3. IP Address Box   4. Description Box

6. On the **Host Options** form, configure the following parameter(s) as required:

Parameter	Description
IPSec zone	<b>Synopsis:</b> true or false <b>Default:</b> false

7. On the **Main Host Settings** form, configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Zone	A pre-defined zone
Interface	A pre-defined interface to which optional IPs and/or networks can be added.

Parameter	Description
IP Address List	<b>Synopsis:</b> A string Additional IP addresses or networks - comma separated, or a range in the form of low.address-high.address
description	<b>Synopsis:</b> A string (Optional) The description string for this host.

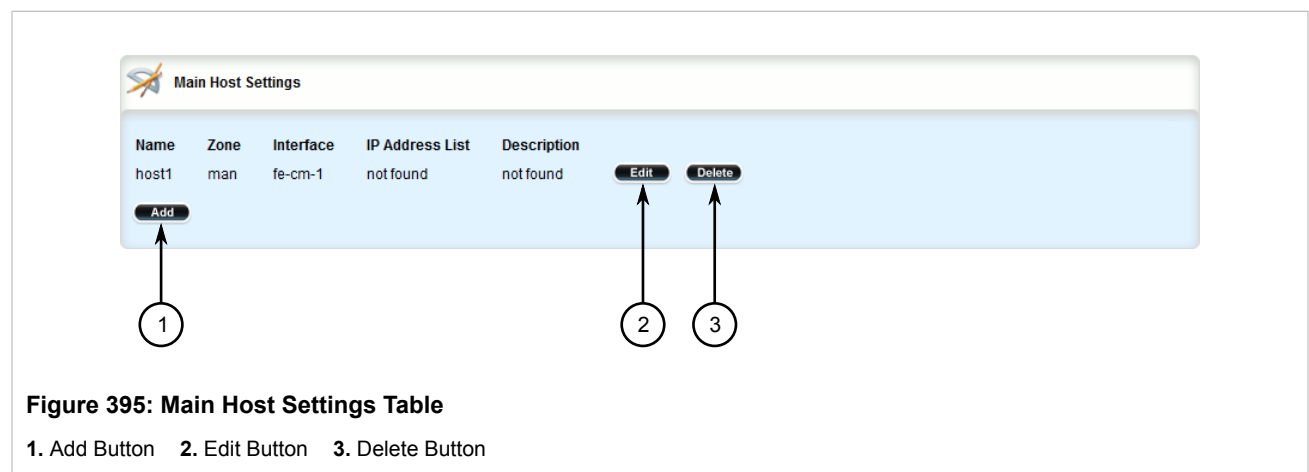
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.16.10.3

## Deleting a Host

To delete a host, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwhost**, where **{firewall}** is the name of the firewall. The **Main Host Settings** table appears.



- Click **Delete** next to the chosen host.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.16.11

## 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.

**Table: Example**

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 5.16.8, “Managing Zones”](#).*



**NOTE**

*Policies for specific hosts or types of traffic can be overridden by rules. For more information about rules, refer to [Section 5.16.14, “Managing Rules”](#).*

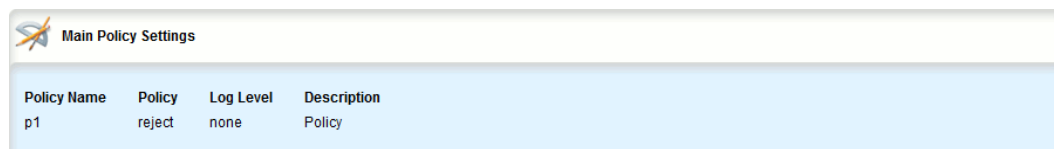
The following sections describe how to configure and manage policies for a firewall:

- [Section 5.16.11.1, “Viewing a List of Policies”](#)
- [Section 5.16.11.2, “Adding a Policy”](#)
- [Section 5.16.11.3, “Configuring the Source Zone”](#)
- [Section 5.16.11.4, “Configuring the Destination Zone”](#)
- [Section 5.16.11.5, “Deleting a Policy”](#)

## Section 5.16.11.1

### Viewing a List of Policies

To view a list of policies, navigate to **security » firewall » fwconfig » {firewall} » fwpolicy**, where {firewall} is the name of the firewall. If policies have been configured, the **Main Policy Settings** table appears.



Main Policy Settings			
Policy Name	Policy	Log Level	Description
p1	reject	none	Policy

**Figure 396: Main Policy Settings Table**

If no policies have been configured, add policies as needed. For more information, refer to [Section 5.16.11.2, “Adding a Policy”](#).



Section 5.16.11.2

Adding a Policy

To configure a policy for the firewall, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to **security » firewall » fwconfig » {firewall} » fwpolicy**, where {firewall} is the name of the firewall.
- 3. Click **<Add fwpolicy>** in the menu. The **Key Settings** form appears.

Figure 397: Key Settings Form

1. Policy Name Box    2. Add Button

- 4. Configure the following parameter(s) as required:

Parameter	Description
Policy Name	<b>Synopsis:</b> A string Enter a name tag for this policy.

- 5. Click **Add**. The **Main Policy Settings** form appears.

Figure 398: Main Policy Settings Form

1. Policy List    2. Log Level List    3. Description Box

6. Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Policy	<b>Synopsis:</b> { accept, drop, reject, continue } <b>Default:</b> reject A default action for connection establishment between different zones.
Log Level	<b>Synopsis:</b> { none, debug, info, notice, warning, error, critical, alert, emergency } <b>Default:</b> none (Optional) Determines whether or not logging will take place and at which logging level.
description	<b>Synopsis:</b> A string (Optional) The description string for this policy.

7. Configure the source zone for the policy. For more information, refer to [Section 5.16.11.3, “Configuring the Source Zone”](#).
8. Configure the destination zone for the policy. For more information, refer to [Section 5.16.11.4, “Configuring the Destination Zone”](#).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
10. Click **Exit Transaction** or continue making changes.

#### Section 5.16.11.3

### Configuring the Source Zone

To configure the source zone for a firewall policy, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
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. The **Source Zone** form appears.

**Figure 399: Source Zone Form**

1. Pre-Defined Zone List    2. All Check Box

- Configure the following parameter(s) as required:

Parameter	Description
predefined-zone	
all	

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.16.11.4

### Configuring the Destination Zone

To configure the destination zone for a firewall policy, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwpolicy » {policy} » destintion-zone**, where **{firewall}** is the name of the firewall and **{policy}** is the name of the policy. The **Destination Zone** form appears.

**Figure 400: Destination Zone Form**

1. Pre-Defined Zone List    2. All Check Box

- Configure the following parameter(s) as required:

Parameter	Description
predefined-zone	
all	

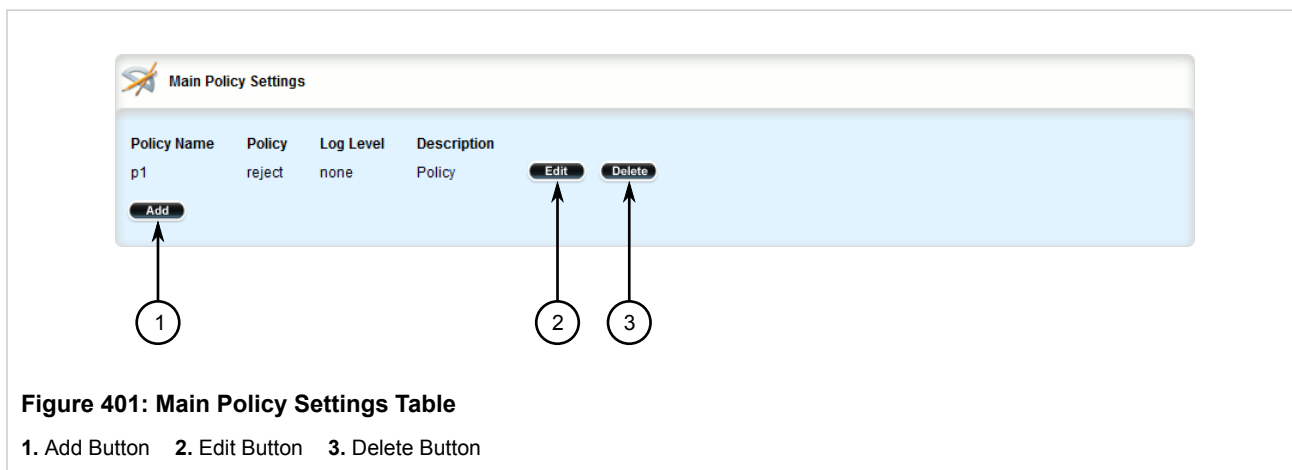
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.16.11.5

## Deleting a Policy

To delete a policy, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwpolicy**, where *{firewall}* is the name of the firewall. The **Main Policy Settings** table appears.



- Click **Delete** next to the chosen policy.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.16.12

## 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 5.16.14, "Managing Rules"](#).*

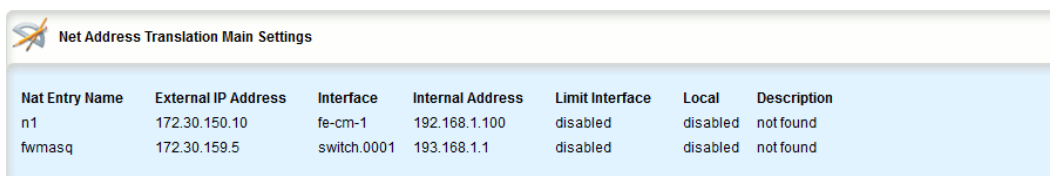
The following sections describe how to configure and manage network address translation settings for a firewall:

- [Section 5.16.12.1, “Viewing a List of NAT Settings”](#)
- [Section 5.16.12.2, “Adding a NAT Setting”](#)
- [Section 5.16.12.3, “Deleting a NAT Setting”](#)

#### Section 5.16.12.1

### Viewing a List of NAT Settings

To view a list of NAT settings, navigate to **security » firewall » fwconfig » {firewall} » fwnat**, where *{firewall}* is the name of the firewall. If NAT settings have been configured, the **Net Address Translation Main Settings** table appears.



Nat Entry Name	External IP Address	Interface	Internal Address	Limit Interface	Local	Description
n1	172.30.150.10	fe-cm-1	192.168.1.100	disabled	disabled	not found
fwmasq	172.30.159.5	switch.0001	193.168.1.1	disabled	disabled	not found

**Figure 402: Net Address Translation Main Settings Table**

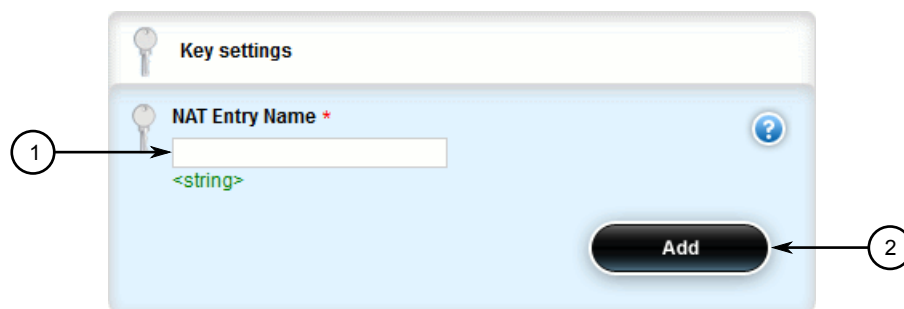
If no NAT settings have been configured, add NAT settings as needed. For more information, refer to [Section 5.16.12.2, “Adding a NAT Setting”](#).

#### Section 5.16.12.2

### Adding a NAT Setting

To configure a Network Address Translation (NAT) entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig » {firewall} » fwnat**, where *{firewall}* is the name of the firewall.
3. Click **<Add fwnat>** in the menu. The **Key Settings** form appears.



The image shows a web form titled "Key settings". Inside the form, there is a field labeled "NAT Entry Name \*" with a red asterisk indicating it is required. Below the field is a placeholder text "<string>". To the right of the field is a blue question mark icon. At the bottom right of the form is a dark blue button labeled "Add". Two numbered circles with arrows point to the form: circle 1 points to the "NAT Entry Name" field, and circle 2 points to the "Add" button.

**Figure 403: Key Settings Form**

1. NAT Entry Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
NAT Entry Name	<b>Synopsis:</b> A string Enter a name for this NAT entry

5. Click **Add**. The **Net Address Translation Main Settings** forms appear.

**Figure 404: Net Address Translation Main Settings Form**

1. External IP Address Box   2. Interface List   3. IP Alias Check Box   4. Internal Address Box   5. Limit Interface Check Box  
6. Local Check Box   7. Description Box

6. Configure the following parameter(s) as required:



**NOTE**

ARP or Ping requests for the translated external IP address will be blocked by the unit unless the external IP address is manually added to the device's external interface. For more information about adding IP addresses to routable interfaces, refer to [Section 5.39, "Managing IP Addresses for Routable Interfaces"](#).

Parameter	Description
External IP Address	<b>Synopsis:</b> A string The external IP Address. The address must not be a DNS name. External IP addresses must be manually added to the interface.
Interface	An interface that has an external IP address.

Parameter	Description
IP Alias	<b>Synopsis:</b> typeless Create IP Alias for NAT rule.
Internal Address	<b>Synopsis:</b> A string The internal IP address. The address must not be a DNS Name.
Limit Interface	<b>Synopsis:</b> typeless Translation only effective from the defined interface.
Local	<b>Synopsis:</b> typeless Translation effective from the firewall system.
description	<b>Synopsis:</b> A string (Optional) The description string for this NAT entry.

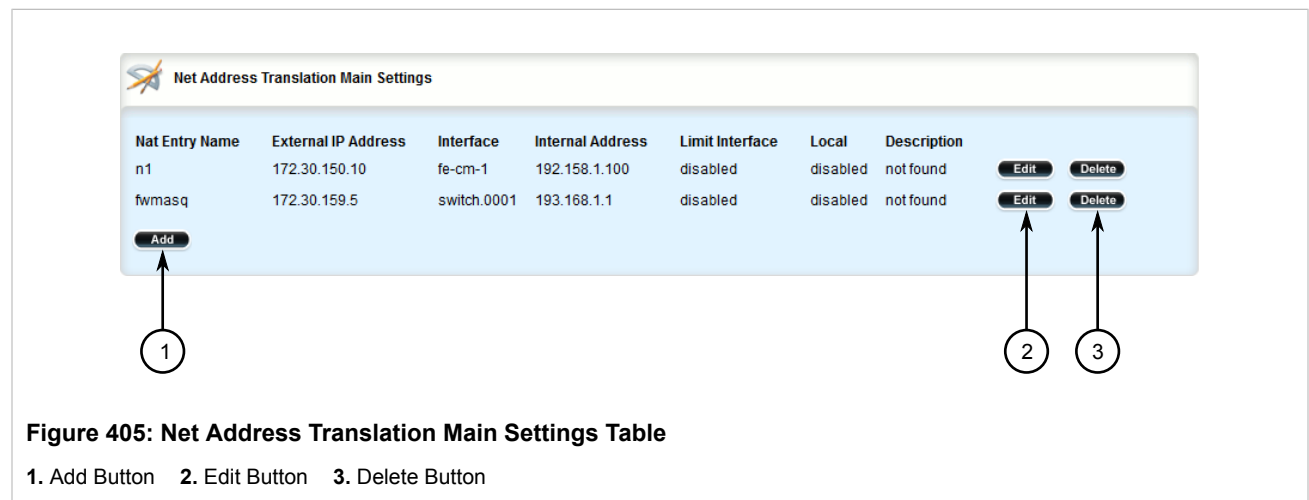
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.16.12.3

## Deleting a NAT Setting

To delete a network address translation entry, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwnat**, where **{firewall}** is the name of the firewall. The **Net Address Translation Main Settings** table appears.



- Click **Delete** next to the chosen NAT setting.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.16.13

# 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.

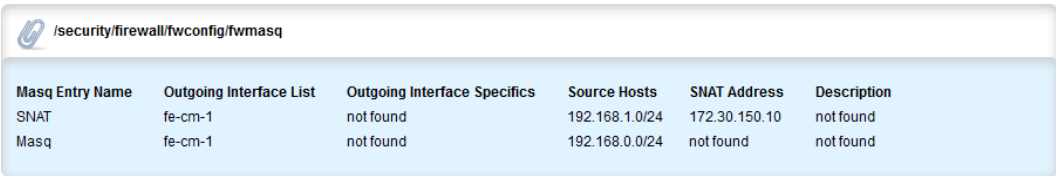
The following sections describe how to configure and manage masquerade and SNAT settings for a firewall:

- [Section 5.16.13.1, “Viewing a List of Masquerade and SNAT Settings”](#)
- [Section 5.16.13.2, “Adding Masquerade or SNAT Settings”](#)
- [Section 5.16.13.3, “Deleting a Masquerade or SNAT Setting”](#)

Section 5.16.13.1

## Viewing a List of Masquerade and SNAT Settings

To view a list of masquerade and SNAT settings, navigate to **security » firewall » fwconfig » {firewall} » fwmasq**, where *{firewall}* is the name of the firewall. If masquerade or SNAT settings have been configured, the **Net Address Translation Main Settings** table appears.



The screenshot shows a web interface with a breadcrumb path: /security/firewall/fwconfig/fwmasq. Below it is a table with the following data:

Masq Entry Name	Outgoing Interface List	Outgoing Interface Specifics	Source Hosts	SNAT Address	Description
SNAT	fe-cm-1	not found	192.168.1.0/24	172.30.150.10	not found
Masq	fe-cm-1	not found	192.168.0.0/24	not found	not found

**Figure 406: Net Address Translation Main Settings Table**

If no masquerade or SNAT settings have been configured, add masquerade or SNAT settings as needed. For more information, refer to [Section 5.16.13.2, “Adding Masquerade or SNAT Settings”](#).

Section 5.16.13.2

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig » {firewall} » fwmasq**, where *{firewall}* is the name of the firewall.
3. Click **<Add fwmasq>** in the menu. The **Key Settings** form appears.



Figure 407: Key Settings Form

1. Masq Entry Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Masq Entry Name	<b>Synopsis:</b> A string A name for this masquerading configuration entry.

5. Click **Add**. The **Net Address Translation Main Settings** form appears.

Figure 408: Net Address Translation Main Settings Form

1. Outgoing Interface List    2. Outgoing Interface Specifics Box    3. Source Hosts Box    4. SNAT Address Box    5. Description Box

6. Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 }

Parameter	Description
	<b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Outgoing Interface List	An outgoing interface list - usually the internet interface.
Outgoing Interface Specifics	<b>Synopsis:</b> A string (Optional) An outgoing interface list - specific IP destinations for the out-interface.
IP Alias	<b>Synopsis:</b> typeless Create IP Alias for NAT rule.
Source Hosts	<b>Synopsis:</b> A string Subnet range or comma-separated list of hosts (IPs)
SNAT Address	<b>Synopsis:</b> A string (Optional) By specifying an address here, SNAT will be used and this will be the source address.
description	<b>Synopsis:</b> A string (Optional) The description string for this masq entry.

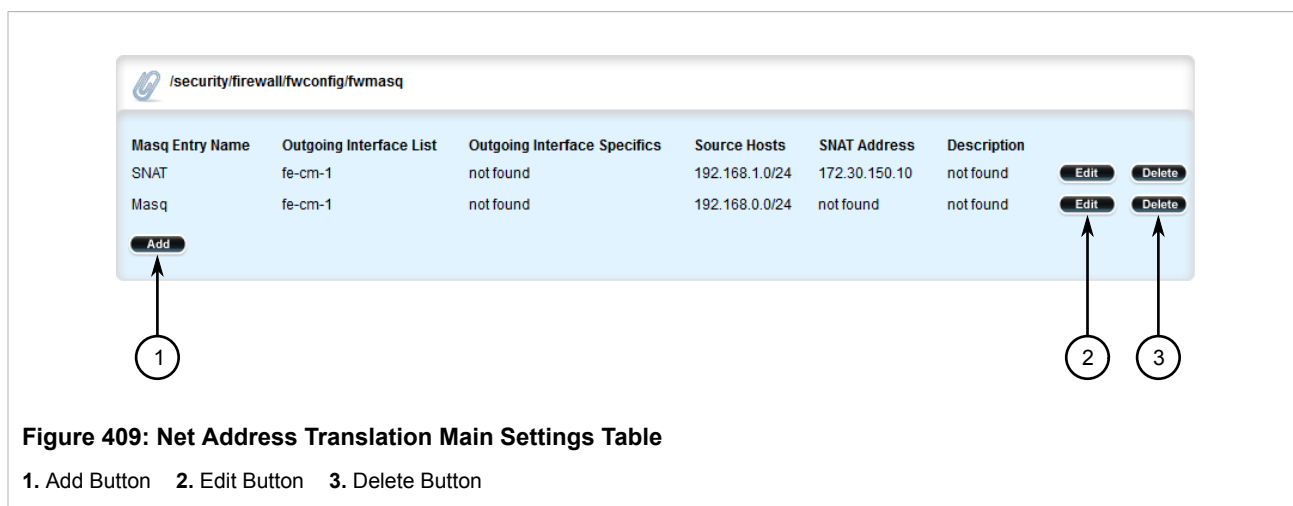
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.16.13.3

## Deleting a Masquerade or SNAT Setting

To delete a masquerade or SNAT setting, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **security » firewall » fwconfig » {firewall} » fwmasq**, where *{firewall}* is the name of the firewall. The **Net Address Translation Main Settings** table appears.



3. Click **Delete** next to the chosen masquerade or SNAT setting.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.16.14

## 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.

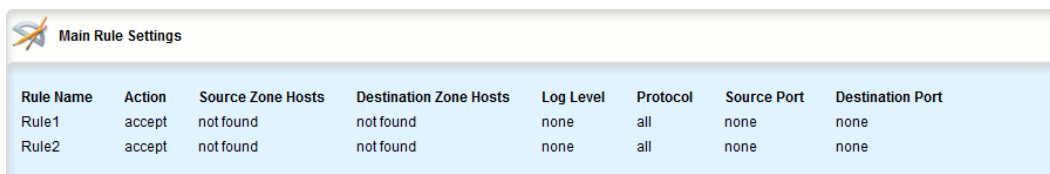
The following sections describe how to configure and manage rules for a firewall:

- [Section 5.16.14.1, “Viewing a List of Rules”](#)
- [Section 5.16.14.2, “Adding a Rule”](#)
- [Section 5.16.14.3, “Configuring the Source Zone”](#)
- [Section 5.16.14.4, “Configuring the Destination Zone”](#)
- [Section 5.16.14.5, “Deleting Rules”](#)

## Section 5.16.14.1

### Viewing a List of Rules

To view a list of rules, navigate to **security » firewall » fwconfig » {firewall} » fwrule**, where *{firewall}* is the name of the firewall. If rules have been configured, the **Main Rule Settings** table appears.



Rule Name	Action	Source Zone Hosts	Destination Zone Hosts	Log Level	Protocol	Source Port	Destination Port
Rule1	accept	not found	not found	none	all	none	none
Rule2	accept	not found	not found	none	all	none	none

**Figure 410: Main Rule Settings Table**

If no rules have been configured, add rules as needed. For more information, refer to [Section 5.16.14.2, “Adding a Rule”](#).

## Section 5.16.14.2

### Adding a Rule

To configure a rule for a firewall, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig » {firewall} » fwrule**, where *{firewall}* is the name of the firewall.
3. Click **<Add fwrule>** in the menu. The **Key Settings** form appears.

**Figure 411: Key Settings Form**

1. Rule Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Rule Name	<b>Synopsis:</b> A string Enter a unique name that identifies this rule.

5. Click **Add**. The **Main Rule Settings** form appears.

The image shows a 'Main Rule Settings' form with the following fields and callouts:

- 1** points to the **Action \*** dropdown menu, which has 'accept' selected and '(reject)' as an option.
- 2** points to the **Source Zone Hosts** field, which has a notepad icon and a dashed line.
- 3** points to the **Destination Zone Hosts** field, which has a notepad icon and a dashed line.
- 4** points to the **Log Level \*** dropdown menu, which has 'none' selected and '(none)' as an option.
- 5** points to the **Protocol \*** field, which has a notepad icon and 'all' selected, with '(all)' as an option.
- 6** points to the **Source Port \*** field, which has a notepad icon and 'none' selected, with '(none)' as an option.
- 7** points to the **Destination Port \*** field, which has a notepad icon and 'none' selected, with '(none)' as an option.
- 8** points to the **Original Destination \*** field, which has a notepad icon and 'none' selected, with '(none)' as an option.
- 9** points to the **Description** field, which has a notepad icon and a dashed line.

**Figure 412: Main Rule Settings Form**

1. Action List   2. Source Zone Hosts Box   3. Destination Zone Hosts Box   4. Log Level List   5. Protocol Box   6. Source Port Box   7. Destination Port Box   8. Original Destination Box   9. Description Box

6. 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 rule for the TCP and UDP protocols is applied.*
- The router sees both TCP and UDP traffic that qualifies for NAT.*
- 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	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Action	<b>Synopsis:</b> { accept, drop, reject, continue, redirect, dnat-, dnat } <b>Default:</b> reject The final action to take on incoming packets matching this rule.
Source Zone Hosts	<b>Synopsis:</b> A string (Optional) Add comma-separated host IPs to a predefined source-zone.
Destination Zone Hosts	<b>Synopsis:</b> A string (Optional) Add comma-separated host IPs to the destination-zone - may include :port for DNAT or REDIRECT.
Log Level	<b>Synopsis:</b> { none, debug, info, notice, warning, error, critical, alert, emergency } <b>Default:</b> none (Optional) Determines whether or not logging will take place and at which logging level.
Protocol	<b>Synopsis:</b> { tcp, udp, icmp, all } or a string <b>Default:</b> all The protocol to match for this rule.
Source Port	<b>Synopsis:</b> A string <b>Default:</b> 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 Port	<b>Synopsis:</b> A string <b>Default:</b> 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	<b>Synopsis:</b> { None } or a string <b>Default:</b> none (Optional) The destination IP address in the connection request as it was received by the firewall.
description	<b>Synopsis:</b> A string (Optional) The description string for this rule.

- Configure the source zone for the rule. For more information, refer to [Section 5.16.14.3, “Configuring the Source Zone”](#).
- Configure the destination zone for the rule. For more information, refer to [Section 5.16.14.4, “Configuring the Destination Zone”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

10. Click **Exit Transaction** or continue making changes.

## Section 5.16.14.3

## Configuring the Source Zone

To configure the source zone for a firewall rule, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
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. The **Source Zone** form appears.

**Figure 413: Source Zone Form**

1. Pre-Defined Zone List    2. Other Box    3. All Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone	A predefined zone
other	<b>Synopsis:</b> A string Type a custom definition - this can be a comma-separated list of zones.
all	All zones

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

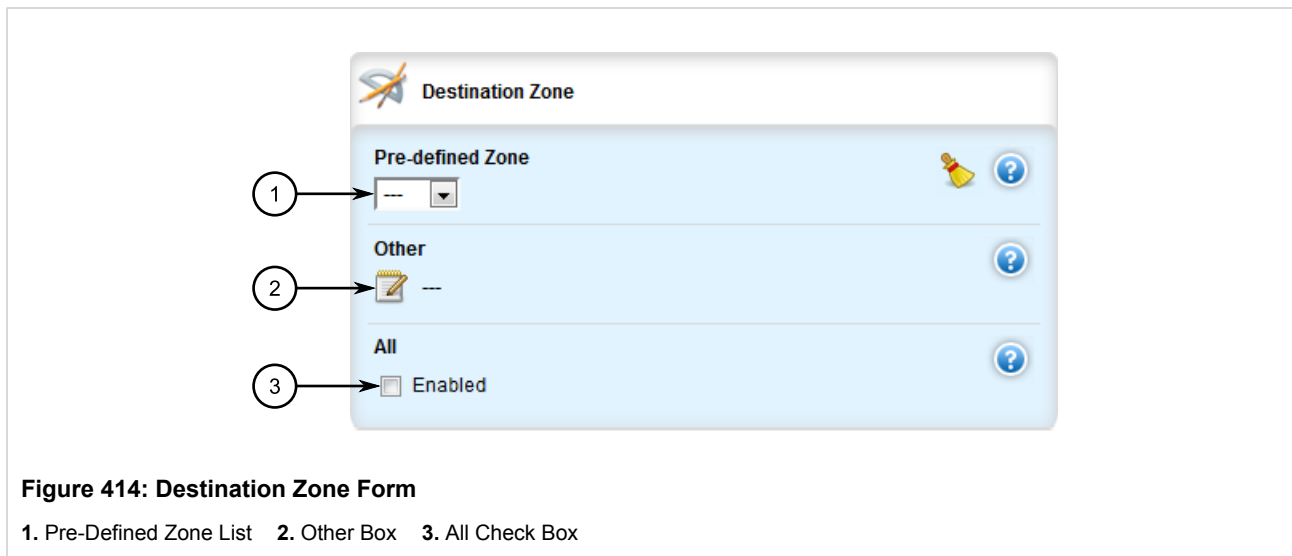
## Section 5.16.14.4

## Configuring the Destination Zone

To configure the destination zone for a firewall rule, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **security » firewall » fwconfig » {firewall} » fwrule{rule} » destination-zone**, where {firewall} is the name of the firewall and {rule} is the name of the rule. The **Destination Zone** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone	A pre-defined zone
other	<b>Synopsis:</b> A string An undefined zone (string).
all	All zones

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

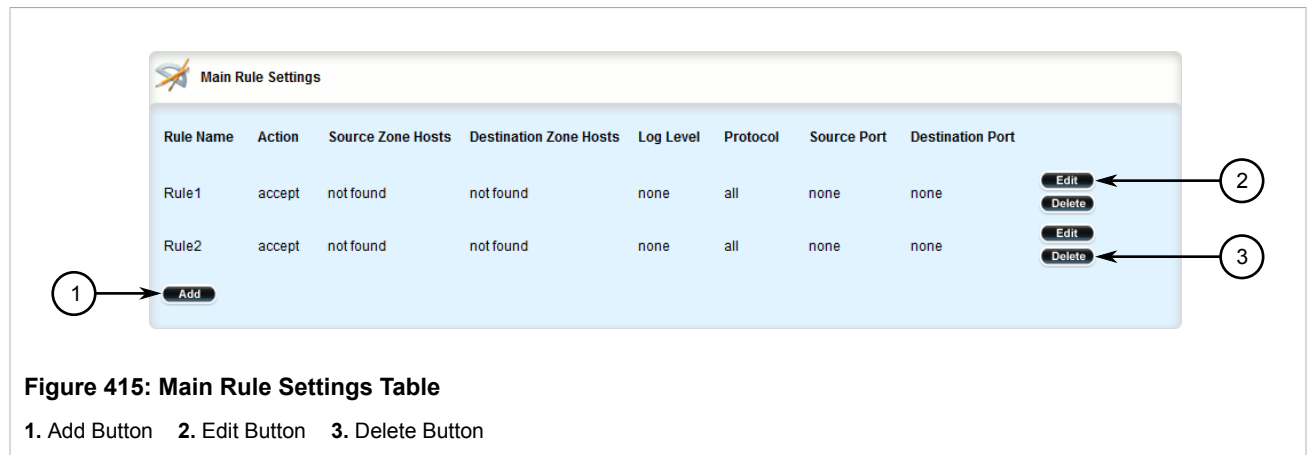
#### Section 5.16.14.5

### Deleting Rules

To delete a rule, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall » fwconfig » {firewall} » fwrule**, where {firewall} is the name of the firewall. The **Main Rule Settings** table appears.





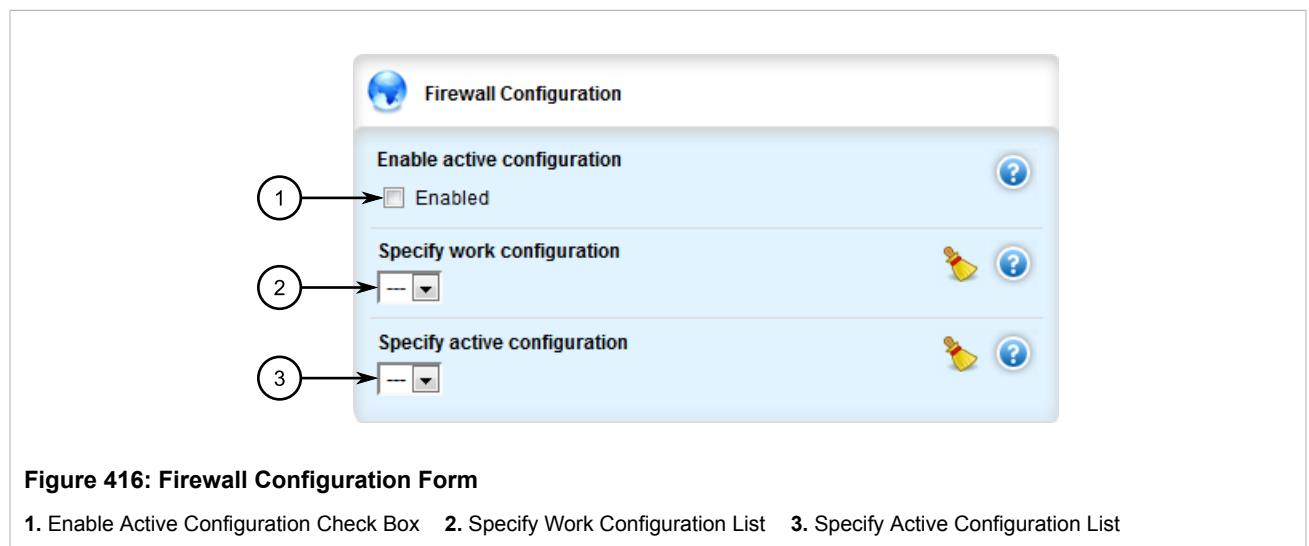
3. Click **Delete** next to the chosen rule.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.16.15

## Validating a Firewall Configuration

To validate a firewall configuration, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall**. The **Firewall Configuration** form appears.



3. Under **Specify work configuration**, select the firewall configuration from the list.
4. Click **Commit** to save the changes. The system validates the firewall configuration and displays the results.
5. Click **Exit Transaction** or continue making changes.

Section 5.16.16

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **security » firewall**. The **Firewall Configuration** form appears.

**Figure 417: Firewall Configuration Form**

1. Enable Active Configuration Check Box    2. Specify Work Configuration List    3. Specify Active Configuration List

3. Under **Specify active configuration**, select the firewall configuration from the list to enable.
4. Select the **Enabled** check box to enable the firewall or clear the check box to disable the firewall.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

Section 5.17

## Managing IS-IS

Intermediate System - Intermediate System (IS-IS) is one of a suite of routing protocols tasked with sharing routing information between routers. The job of the router is to enable the efficient movement of data over sometimes complex networks. Routing protocols are designed to share routing information across these networks and use sophisticated algorithms to decide the shortest route for the information to travel from point A to point B. One of the first link-state routing protocols was IS-IS developed in 1986 and later published in 1987 by ISO as ISO/IEC 10589. It was later republished as an IETF standard ([RFC 1142](http://tools.ietf.org/html/rfc1142) [http://tools.ietf.org/html/rfc1142]).

The following sections describe how to configure the IS-IS routing protocol:

- [Section 5.17.1, “IS-IS Concepts”](#)
- [Section 5.17.2, “Configuring IS-IS”](#)

- [Section 5.17.3, “Viewing the Status of Neighbors”](#)
- [Section 5.17.4, “Viewing the Status of the Link-State Database”](#)
- [Section 5.17.5, “Managing Area Tags”](#)
- [Section 5.17.6, “Managing Interfaces”](#)
- [Section 5.17.7, “Managing LSP Generation”](#)
- [Section 5.17.8, “Managing SPF Calculations”](#)
- [Section 5.17.9, “Managing the Lifetime of LSPs”](#)
- [Section 5.17.10, “Managing LSP Refresh Intervals”](#)
- [Section 5.17.11, “Managing Network Entity Titles \(NETs\)”](#)
- [Section 5.17.12, “Managing Redistribution Metrics”](#)

### Section 5.17.1

## IS-IS Concepts

IS-IS is an Interior Gateway Protocol (IGP) meant to exchange information within Autonomous Systems (AS). It is designed to operate within an administrative domain or network using link-state information to decide optimal data packet routing, similar to OSPF. IS-IS floods the network with link-state information and builds a database of the network's topology. The protocol computes the best path through the network (using Dijkstra's algorithm) and then forwards packets to their destination along that path.

Although it was originally designed as an ISO Connectionless-mode Network Protocol (CLNP), it was later adapted for IP network use (Dual IS-IS) in [RFC 1195](http://tools.ietf.org/html/rfc1195) [http://tools.ietf.org/html/rfc1195]. IS-IS is used primarily in ISP environments and better suited to *stringy* networks as opposed to central core based networks.



#### NOTE

*In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.*

The following sections describe IS-IS in more detail:

- [Section 5.17.1.1, “IS-IS Routers”](#)
- [Section 5.17.1.2, “Network Entity Title \(NET\) Addresses”](#)
- [Section 5.17.1.3, “Advantages and Disadvantages of Using IS-IS”](#)

### Section 5.17.1.1

## 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 5.17.1.2

## Network Entity Title (NET) Addresses

IS-IS routers are identified by their Network Entity Title (NET) address, which is in Network Service Access Point (NSAP) format ([RFC 1237](http://tools.ietf.org/html/rfc1237) [http://tools.ietf.org/html/rfc1237]). NSAP addresses range from 8 to 20 octets and consist of the Authority and Format Identifier (1 byte), the Area ID (0 to 12 bytes), the System ID (6 bytes) and the selector (1 byte).

The following is an example of an NSAP address:

NSAP address: 49.0001.1921.6800.1001.00

AFI: 49 (typical for IS-IS NET addresses)  
Area ID: 0001 (typically 4 bytes)  
System ID: 1921.6800.1001 (equates to the IP address 192.168.1.1)  
Selector: 00 (NET addresses always have a selector of 00)

## Section 5.17.1.3

## Advantages and Disadvantages of Using IS-IS

The advantages and disadvantages of using IS-IS include the following:

### Advantages

- runs natively on the OSI network layer
- can support both IPv4 and IPv6 networks due to its independence from IP addressing
- IS-IS concept of areas is simpler to understand and implement
- IS-IS updates grouped together and sent as one LSP, rather than several small LSAs as with OSPF
- 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

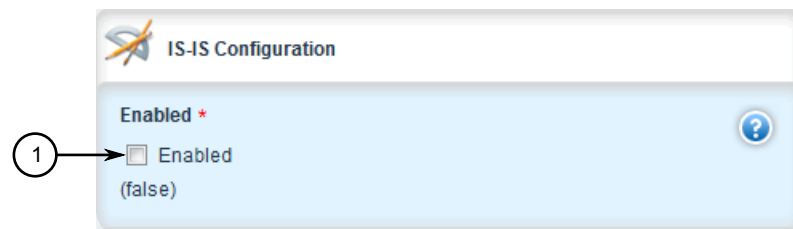
- used mostly by service providers
- limited support by network stack vendors and equipment makers
- CLNP addressing can be new and confusing to many users

## Section 5.17.2

## Configuring IS-IS

To configure dynamic routing with IS-IS, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis**. The **IS-IS Configuration** form appears.



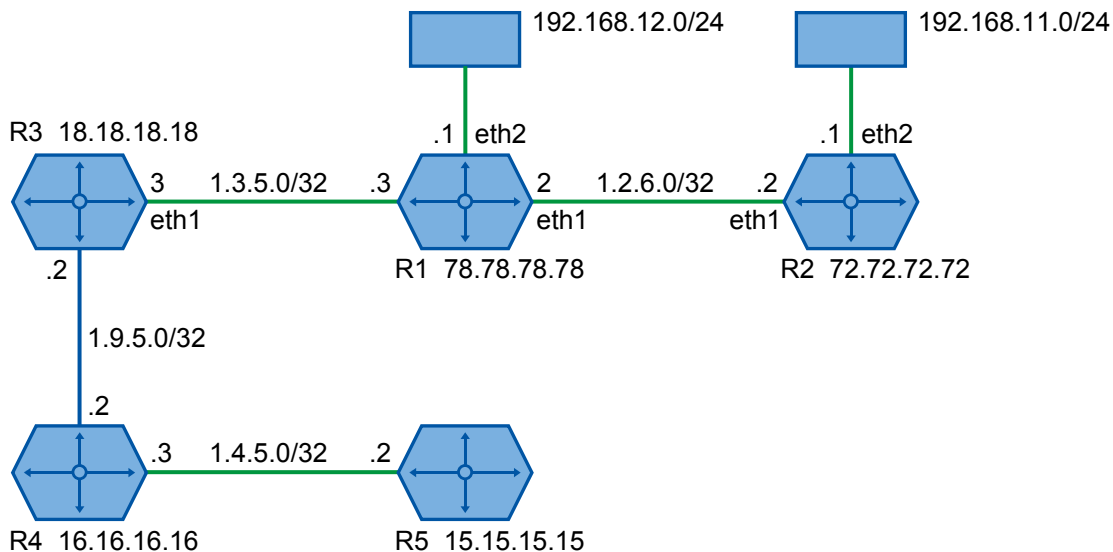
**Figure 418: IS-IS Configuration Form**

1. Enabled Check Box

3. Select the **Enabled** check box.
4. Associate the device with one or more areas in the IS-IS network by defining area tags. For more information, refer to [Section 5.17.5, “Managing Area Tags”](#).
5. Configure one or more interfaces on which to perform IS-IS routing. For more information, refer to [Section 5.17.6, “Managing Interfaces”](#).

## » 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.



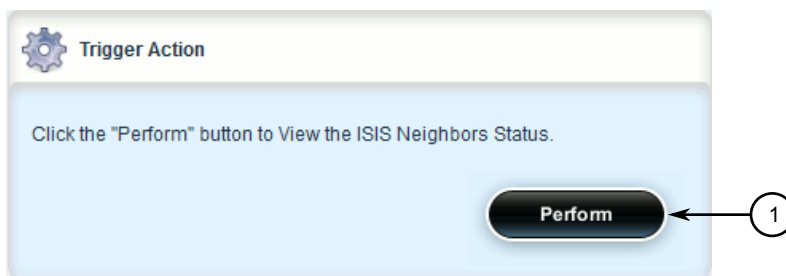
**Figure 419: Multi-Level IS-IS Configuration**

### Section 5.17.3

## 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 5.17.2, “Configuring IS-IS”](#).
2. Navigate to **routing » status » isis » isis-neighbors-status**. The **Trigger Action** form appears.



**Figure 420: Trigger Action Form**

1. Perform Button

3. Click **Perform**. The **ISIS Neighbors Status** form appears.



**Figure 421: ISIS Neighbors Status Form**

This form displays the following information:

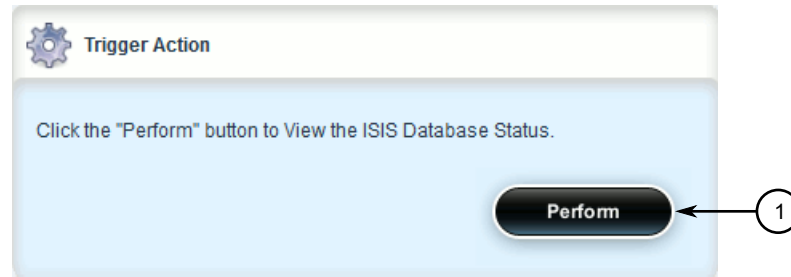
Parameter	Description
System ID	The system ID.
Interface	The name of the interface.
L	The level.
State	Adjacency state.
Holdtime	The remaining hold time in seconds.
SNPA	The MAC address of the Sub-Network Point of Attachment (SNPA).

Section 5.17.4

## 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 5.17.2, “Configuring IS-IS”](#).
2. Navigate to either **routing » status » isis » isis-database-status** for a basic view, or **routing » status » isis » isis-database-detail-status** for a more detailed view. The **Trigger Action** form appears.




**Figure 422: Trigger Action Form - Basic View**

1. Perform Button

3. Click **Perform**. The **ISIS Database Status** or **ISIS Database Detail Status** form appears.


**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	0x00000013	0xe838	1061	0/0/0

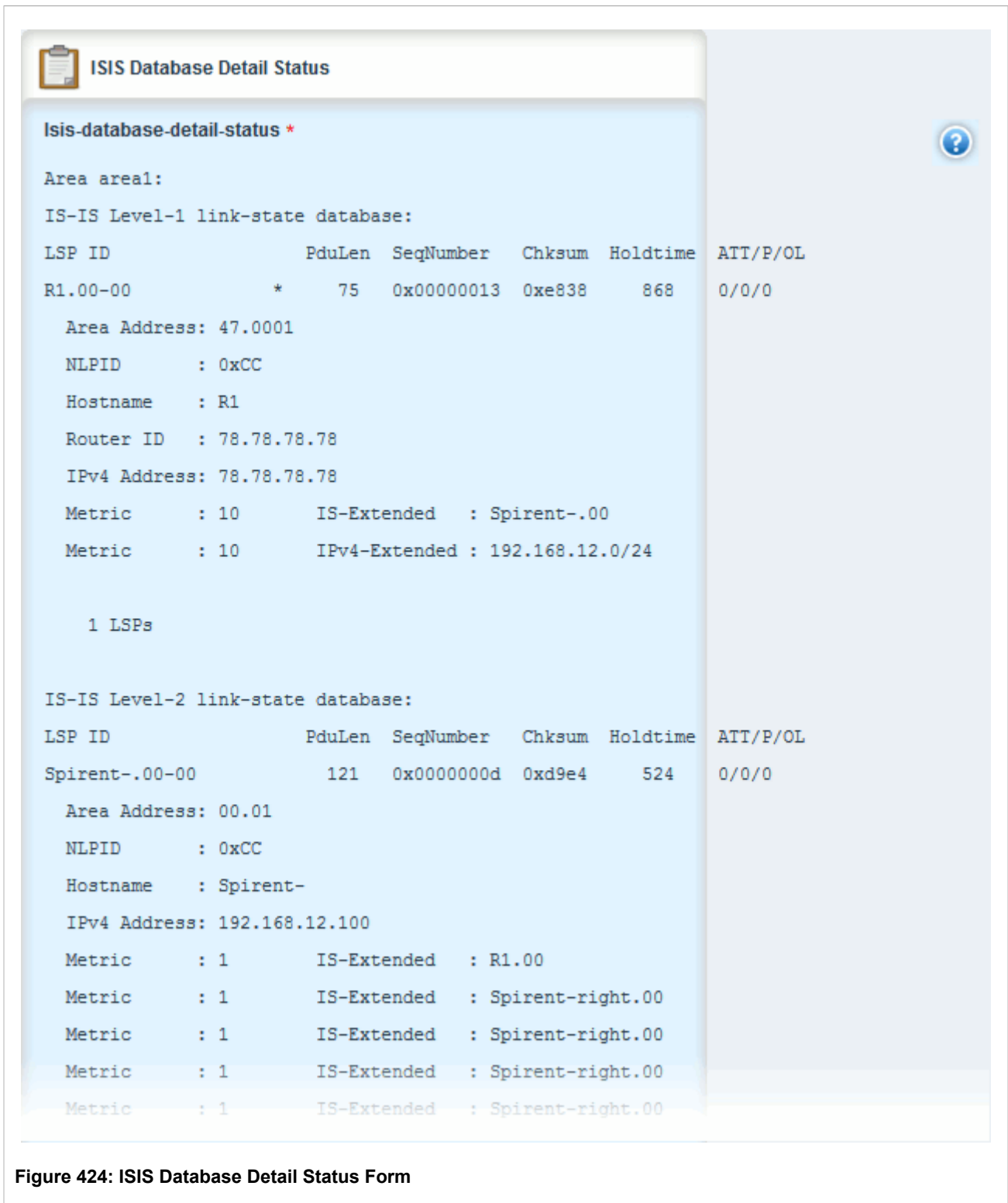
1 LSPs

IS-IS Level-2 link-state database:

LSP ID		PduLen	SeqNumber	Chksum	Holdtime	ATT/P/OL
Spirent-.00-00		121	0x0000000d	0xd9e4	717	0/0/0
R1.00-00	*	75	0x00000013	0xea34	937	0/0/0
Spirent-right.00-00		1465	0x0000000d	0x4163	718	0/0/0
Spirent-right.00-01		295	0x0000000d	0x6e0b	718	0/0/0
Spirent-right.00-00		1465	0x0000000d	0x4a36	717	0/0/0
Spirent-right.00-01		287	0x0000000d	0x58ce	717	0/0/0
Spirent-right.00-00		1462	0x0000000d	0x6926	717	0/0/0
Spirent-right.00-01		269	0x0000000d	0x8288	718	0/0/0
Spirent-right.00-00		1463	0x0000000d	0x9d9e	718	0/0/0

**Figure 423: ISIS Database Status Form**





**Figure 424: ISIS Database Detail Status Form**

These forms display 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 5.17.5

## 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.

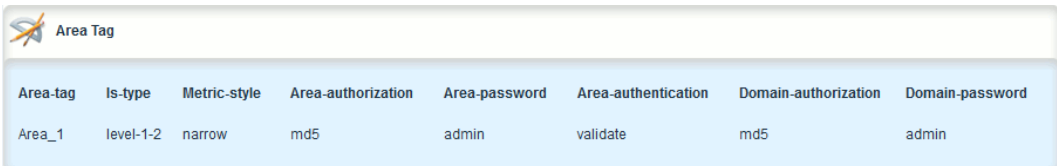
The following sections describe how to configure and manage area tags for IS-IS:

- [Section 5.17.5.1, “Viewing a List of Area Tags”](#)
- [Section 5.17.5.2, “Adding an Area Tag”](#)
- [Section 5.17.5.3, “Deleting an Area Tag”](#)

## Section 5.17.5.1

### Viewing a List of Area Tags

To view a list of area tags configured for dynamic IS-IS routes, navigate to **routing » dynamic » isis » area**. If area tags have been configured, the **Area Tag** table appears.



Area-tag	Is-type	Metric-style	Area-authorization	Area-password	Area-authentication	Domain-authorization	Domain-password
Area_1	level-1-2	narrow	md5	admin	validate	md5	admin

**Figure 425: Area Tag Table**

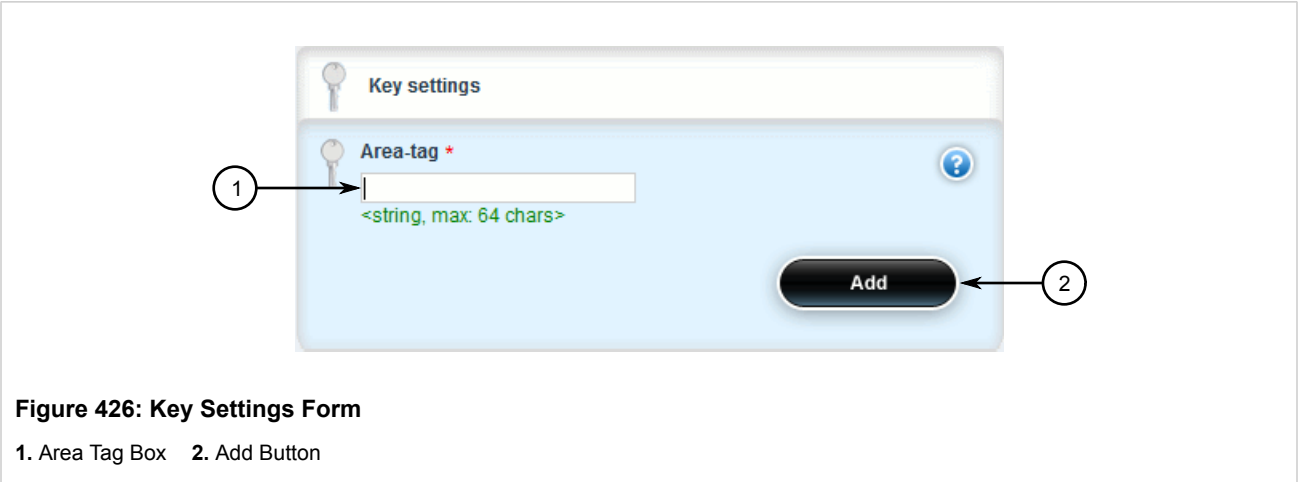
If no area tags have been configured, add area tags as needed. For more information, refer to [Section 5.17.5.2, “Adding an Area Tag”](#).

Section 5.17.5.2

Adding an Area Tag

To add an area tag for dynamic IS-IS routes, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *routing » dynamic » isis » area* and click **<Add area>**. The **Key Settings** form appears.



- 3. Configure the following parameter(s) as required:

Parameter	Description
Area Tag	<b>Synopsis:</b> A string 1 to 64 characters long Name for a routing process, must be unique among router processes for a given router. Mandatory field.

- 4. Click **Add** to create the new area tag. The **Area Tag** form appears.

**Figure 427: Area Tag Form**

1. IS Type List   2. Metric Style List   3. Area Authorization List   4. Area Password Box   5. Area Authentication List   6. Domain Authorization List   7. Domain Password Box   8. Domain Authentication List

5. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 } The IS type for this area: level-1-only, level-2-only or level-1-2. Level-1 routers have neighbors only on the same area. Level-2-only (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
Metric Style	<b>Synopsis:</b> { narrow, transition, wide } <b>Default:</b> wide The metric style Type Length Value (TLV) for this area: narrow, transition or wide. Default is wide.
Area Authorization	<b>Synopsis:</b> { clear, md5 } <b>Default:</b> clear

Parameter	Description
	The authorization type for the area password. Default is clear.
Area Password	<b>Synopsis:</b> A string 1 to 254 characters long The area password to be used for transmission of level-1 LSPs.
Area Authentication	<b>Synopsis:</b> { send-only, validate } <b>Default:</b> send-only The authentication option to be used with the area password on SNP PDUs. Default is send-only.
Domain Authorization	<b>Synopsis:</b> { clear, md5 } <b>Default:</b> clear The authorization type for the domain password. Default is clear.
Domain Password	<b>Synopsis:</b> A string 1 to 254 characters long The domain password to be used for transmission of level-2 LSPs.
Domain Authentication	<b>Synopsis:</b> { send-only, validate } <b>Default:</b> send-only The authentication option to be used with the domain password on SNP PDUs. Default is send-only.

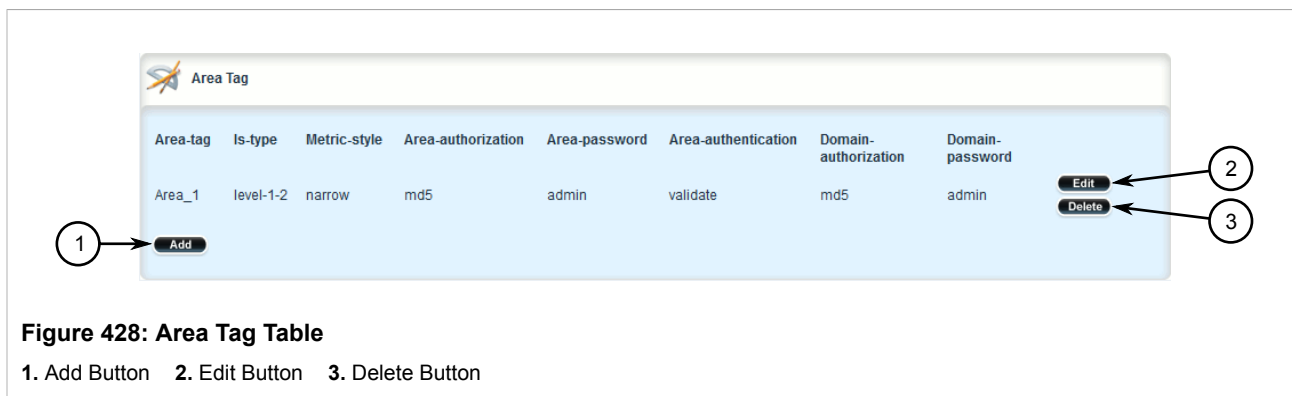
6. Add one or more Network Entity Titles (NETs). For more information, refer to [Section 5.17.11, “Managing Network Entity Titles \(NETs\)”](#)
7. If necessary, configure intervals for the generation of Link-State Packets (LSPs). The default is 30 seconds. For more information, refer to [Section 5.17.7, “Managing LSP Generation”](#).
8. If necessary, configure refresh intervals for Link-State Packets (LSPs). The default is 900 seconds. For more information, refer to [Section 5.17.10, “Managing LSP Refresh Intervals”](#).
9. If necessary, configure the minimum interval between consecutive SPF calculations. The default is 1 second. For more information, refer to [Section 5.17.8, “Managing SPF Calculations”](#).
10. If necessary, configure how long LSPs can reside in the device's Link State Database (LSDB) before they are refreshed. The default is 1200 seconds. For more information, refer to [Section 5.17.9, “Managing the Lifetime of LSPs”](#).
11. If necessary, define rules for redistributing static, RIP, BGP or OSPF routes. For more information, refer to [Section 5.17.12, “Managing Redistribution Metrics”](#)
12. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
13. Click **Exit Transaction** or continue making changes.

### Section 5.17.5.3

## Deleting an Area Tag

To delete an area tag for dynamic IS-IS routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis » area**. The **Area Tag** table appears.



3. Click **Delete** next to the chosen area tag.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.17.6

## Managing Interfaces

IS-IS transmits hello packets and Link-State Packets (LSPs) through IS-IS enabled interfaces.



#### NOTE

*IS-IS is only supported on Ethernet and WAN (HDLC-ETH) interfaces.*

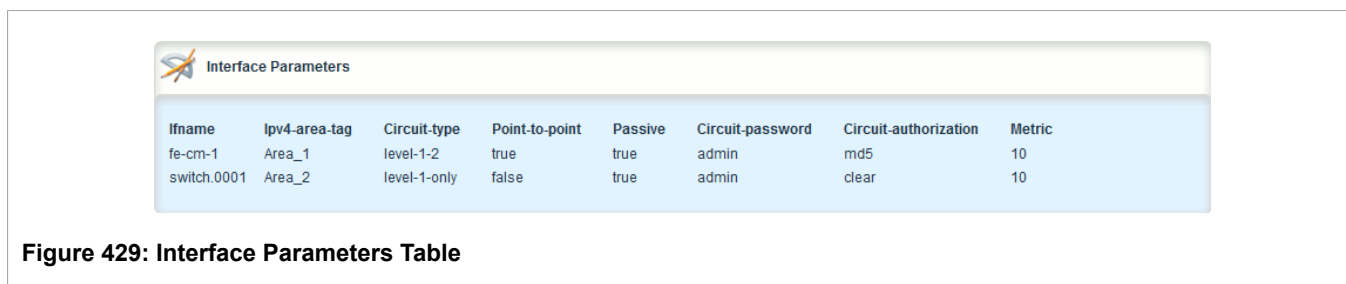
The following sections describe how to configure and manage interfaces for IS-IS:

- [Section 5.17.6.1, “Viewing a List of Interfaces”](#)
- [Section 5.17.6.2, “Configuring an Interface”](#)

#### Section 5.17.6.1

### Viewing a List of Interfaces

To view a list of interfaces for dynamic IS-IS routes, navigate to **routing » dynamic » isis » interface**. If interfaces have been configured, the **Interface Parameters** table appears.



Interfaces are added automatically when a VLAN is created. For more information about creating a VLAN, refer to [Section 5.36, “Managing VLANs”](#).

Section 5.17.6.2

## Configuring an Interface

When IS-IS is enabled, two interfaces are already configured: *fe-cm-01* and *switch.0001*.

To configure optional parameters for these and any other interfaces that have been added for IS-IS, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis » interface** and select an interface. The **Interface Parameters** form appears.

The screenshot shows the 'Interface Parameters' configuration window. It contains the following fields and their values:

- Ipv4-area-tag**: -- (Callout 1)
- Circuit-type**: -- (Callout 2)
- Point-to-point \***: ☐ Enabled (false) (Callout 3)
- Passive \***: ☒ Enabled (true) (Callout 4)
- Circuit-password**: -- (Callout 5)
- Circuit-authorization \***: clear (clear) (Callout 6)
- Metric \***: 10 (10) (Callout 7)
- Csnp-interval \***: 10 (10) (Callout 8)
- Hello-interval \***: 3 (3) (Callout 9)
- Hello-multiplier \***: 10 (10) (Callout 10)
- Psnp-interval \***: 2 (2) (Callout 11)

**Figure 430: Interface Parameters Form**

1. IPv4 Area Tag Box   2. Circuit Type List   3. Point-to-Point Check Box   4. Passive Check Box   5. Circuit Password Box  
6. Circuit Authorization List   7. Metric Box   8. CSNP Interval Box   9. Hello Interval Box   10. Hello Multiplier Box   11. PSNP Interval Box

3. Configure the following parameter(s) as required:



Parameter	Description
IPv4 Area Tag	Name of Area Tag to be used for IS-IS over IPv4.
Circuit Routing Type	<p><b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 }</p> <p>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.</p>
Point-to-Point	<p><b>Synopsis:</b> true or false <b>Default:</b> false</p> <p>Enable or disable point-to-point network communication</p>
passive	<p><b>Synopsis:</b> true or false <b>Default:</b> true</p> <p>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.</p>
Password	<p><b>Synopsis:</b> A string 1 to 254 characters long</p> <p>The value to be used as a transmit password in IIH PDUs transmitted by this Intermediate System.</p>
Authorization	<p><b>Synopsis:</b> { clear, md5 } <b>Default:</b> clear</p> <p>The authorization type to be associated with the transmit password in IIH PDUs transmitted by this Intermediate System.</p>
Metric	<p><b>Synopsis:</b> An integer between 1 and 16777214 <b>Default:</b> 10</p> <p>Metric assigned to the link, used to calculate the cost of the route. Value ranges from 1 to 16777214. Default is 10.</p>
CSNP Interval	<p><b>Synopsis:</b> An integer between 1 and 600 <b>Default:</b> 10</p> <p>CSNP interval in seconds, ranging from 1 to 600. Default is 10.</p>
Hello Interval	<p><b>Synopsis:</b> An integer between 1 and 600 <b>Default:</b> 3</p> <p>Hello interval in seconds, ranging from 1 to 600. Default is 3.</p>
Hello Multiplier	<p><b>Synopsis:</b> An integer between 2 and 100 <b>Default:</b> 10</p> <p>Multiplier for Hello holding time. Value ranges from 2 to 100. Default is 10.</p>
PSNP Interval	<p><b>Synopsis:</b> An integer between 1 and 120 <b>Default:</b> 2</p> <p>PSNP interval in seconds, ranging from 1 to 120. Default is 2.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.17.7

## 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.

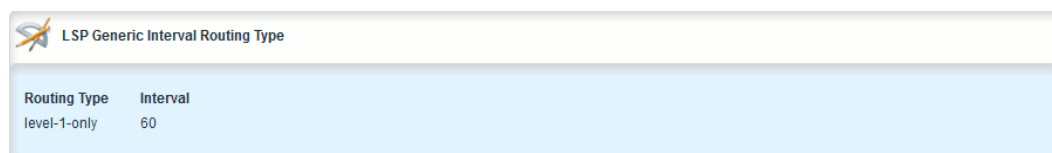
The following sections describe how to configure and manage generation intervals for LSPs:

- [Section 5.17.7.1, “Viewing a List of LSP Generation Intervals”](#)
- [Section 5.17.7.2, “Adding an LSP Generation Interval”](#)
- [Section 5.17.7.3, “Deleting an LSP Generation Interval”](#)

## Section 5.17.7.1

### Viewing a List of LSP Generation Intervals

To view a list of LSP generation intervals configured for an IS-IS area, navigate to **routing » dynamic » 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, the **LSP Generic Interval Routing Type** table appears.



The screenshot shows a web interface window titled "LSP Generic Interval Routing Type". Inside the window is a table with two columns: "Routing Type" and "Interval". There is one row of data with "level-1-only" under "Routing Type" and "60" under "Interval".

Routing Type	Interval
level-1-only	60

Figure 431: LSP Generic Interval Routing Type Table

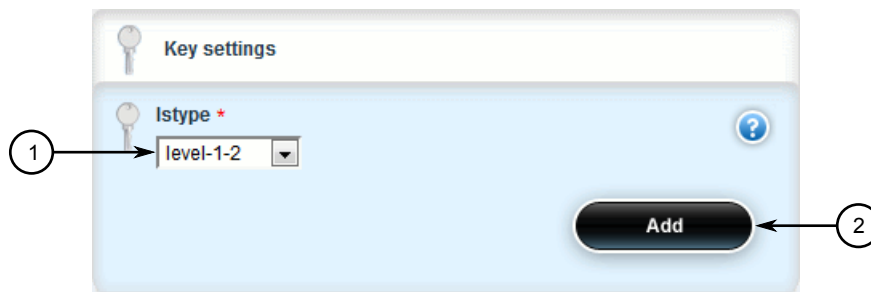
If no intervals have been configured, add intervals as needed. For more information, refer to [Section 5.17.7.2, “Adding an LSP Generation Interval”](#).

## Section 5.17.7.2

### Adding an LSP Generation Interval

To add an LSP generation interval to an IS-IS area, do the following:

1. Navigate to **routing » dynamic » isis » area » {name} » lsp-gen-interval**, where **{name}** is the unique name for a routing process that belongs to a specific router.
2. Click **<Add is-type>**. The **Key Settings** form appears.



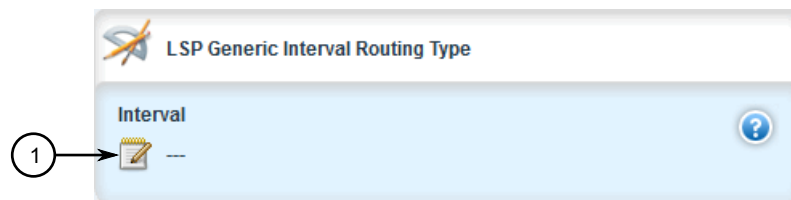
**Figure 432: Key Settings Form**

1. Routing Type List 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 } The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.

4. Click **Add** to create the new interval. The **LSP Generic Interval Routing Type** form appears.



**Figure 433: LSP Generic Interval Routing Type Form**

1. Interval Box

5. Configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 1 and 120 Minimum interval in seconds, ranging from 1 to 120. Default is 30.

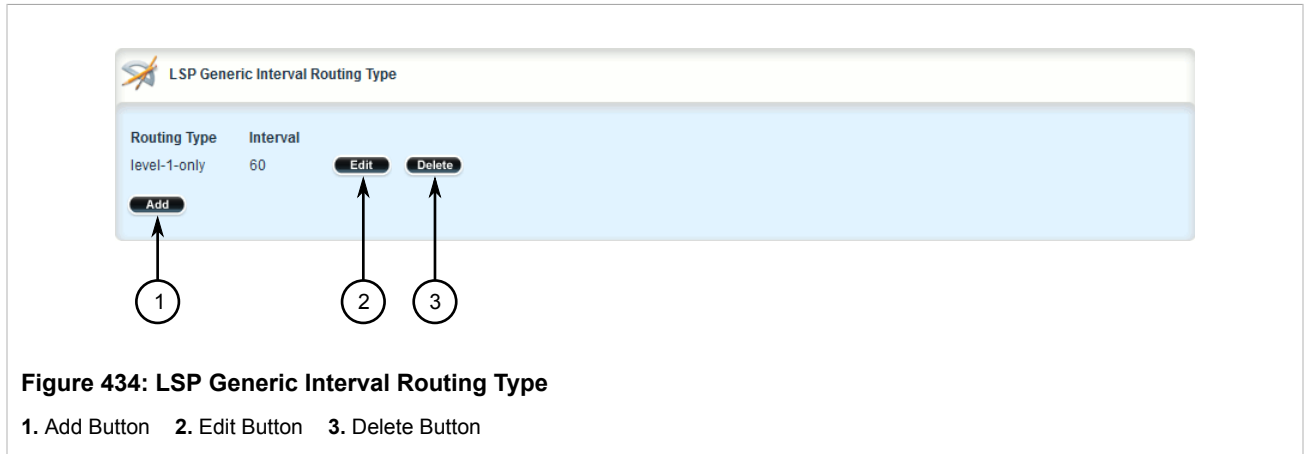
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.17.7.3

## Deleting an LSP Generation Interval

To delete an LSP generation interval for an IS-IS area, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis » area » {name} » lsp-gen-interval**, where **{name}** is the unique name for a routing process that belongs to a specific router. The **LSP Generic Interval Routing Type** table appears.



3. Click **Delete** next to the chosen interval.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.17.8

## 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.

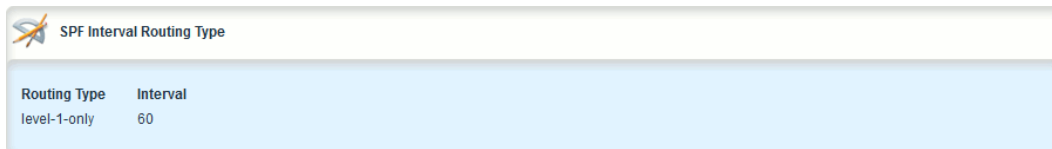
The following sections describe how to configure and manage SPF calculations for IS-IS areas:

- [Section 5.17.8.1, “Viewing a List of SPF Calculation Intervals”](#)
- [Section 5.17.8.2, “Adding an SPF Calculation Interval”](#)
- [Section 5.17.8.3, “Deleting an SPF Calculation Interval”](#)

#### Section 5.17.8.1

### Viewing a List of SPF Calculation Intervals

To view a list of SPF calculation intervals configured for an IS-IS area, navigate to **routing » dynamic » 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, the **SPF Interval Routing Type** table appears.



Routing Type	Interval
level-1-only	60

**Figure 435: SPF Interval Routing Type**

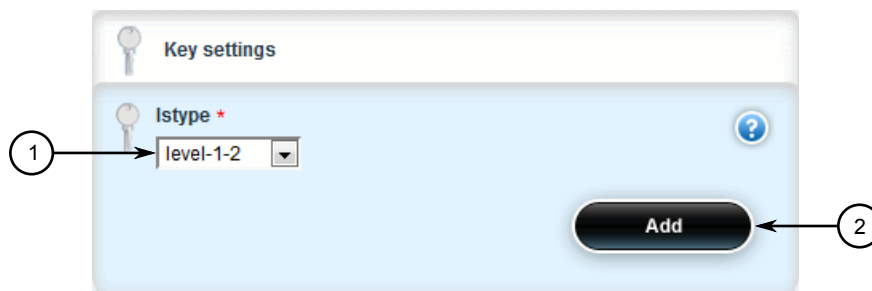
If no intervals have been configured, add intervals as needed. For more information, refer to [Section 5.17.8.2, “Adding an SPF Calculation Interval”](#).

### Section 5.17.8.2

## Adding an SPF Calculation Interval

To add an SPF calculation interval to an IS-IS area, do the following:

1. Navigate to **routing » dynamic » isis » area » {name} » spf-interval**, where **{name}** is the unique name for a routing process that belongs to a specific router.
2. Click **<Add is-type>**. The **Key Settings** form appears.



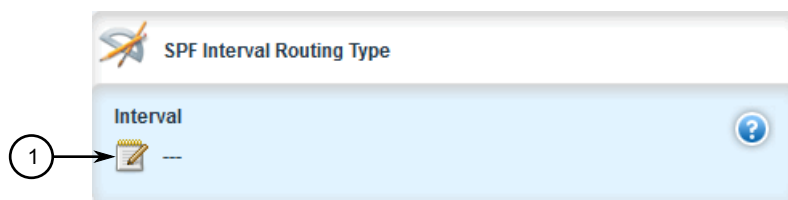
**Figure 436: Key Settings Form**

1. Routing Type List    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 } The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.

4. Click **Add** to create the new interval. The **SPF Interval Routing Type** form appears.



**Figure 437: SPF Interval Routing Type Form**

1. Interval Box

5. Configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 1 and 120 Minimum interval in seconds, ranging from from 1 to 120. Default is 1.

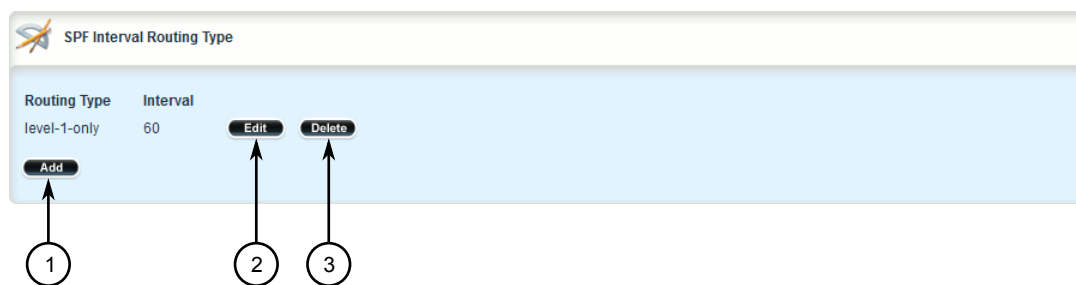
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.17.8.3

### Deleting an SPF Calculation Interval

To delete an SPF calculation interval for an IS-IS area, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis » area » {name} » spf-interval**, where **{name}** is the unique name for a routing process that belongs to a specific router. The **SPF Interval Routing Type** table appears.



**Figure 438: SPF Interval Routing Type**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen interval.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

5. Click **Exit Transaction** or continue making changes.

## Section 5.17.9

## Managing the Lifetime of LSPs

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, the maximum time limit is 1200 seconds. However, this interval can be customized for different routing types within the range of 350 to 65535 seconds if needed.

The lifetime interval is configurable for each area and routing type in the IS-IS network.

The following sections describe how to configure and manage LSP lifetime intervals for LSPs:

**NOTE**

*For information about configuring the refresh interval for an LSP, refer to [Section 5.17.10, “Managing LSP Refresh Intervals”](#).*

- [Section 5.17.9.1, “Viewing a List of LSP Lifetime Intervals”](#)
- [Section 5.17.9.2, “Adding an LSP Lifetime Interval”](#)
- [Section 5.17.9.3, “Deleting an LSP Lifetime Interval”](#)

## Section 5.17.9.1

### Viewing a List of LSP Lifetime Intervals

To view a list of LSP lifetime intervals configured for an IS-IS area, navigate to **routing » dynamic » 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, the **Maximum LSP Lifetime Routing Type** table appears.

Routing Type	Interval
level-1-only	60

**Figure 439: Maximum LSP Lifetime Routing Type**

If no intervals have been configured, add intervals as needed. For more information, refer to [Section 5.17.9.2, “Adding an LSP Lifetime Interval”](#).

## Section 5.17.9.2

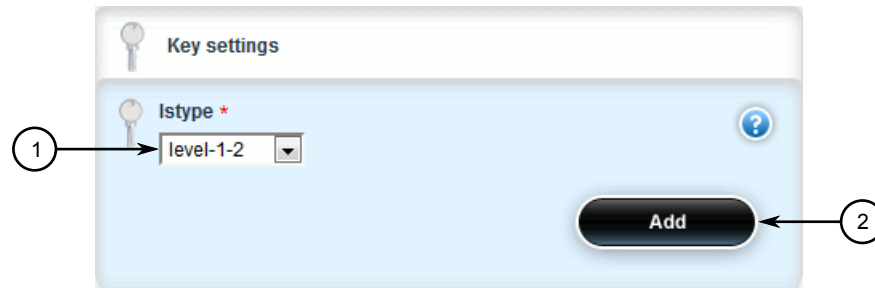
### Adding an LSP Lifetime Interval

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 5.17.10, “Managing LSP Refresh Intervals”](#).*

1. Navigate to **routing » dynamic » isis » area » {name} » max-lsp-lifetime**, where **{name}** is the unique name for a routing process that belongs to a specific router.
2. Click **<Add is-type>**. The **Key Settings** form appears.



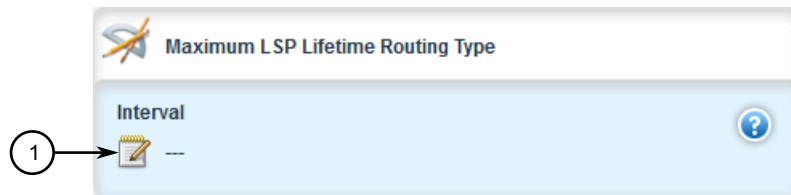
**Figure 440: Key Settings Form**

1. Routing Type List 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 } The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.

4. Click **Add** to create the new limit. The **Maximum LSP Lifetime Routing Type** form appears.



**Figure 441: Maximum LSP Lifetime Routing Type Form**

1. Interval Box

5. Configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 1 and 65535 Minimum interval in seconds, ranging from 350 to 65535 seconds. Default is 1200.

6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

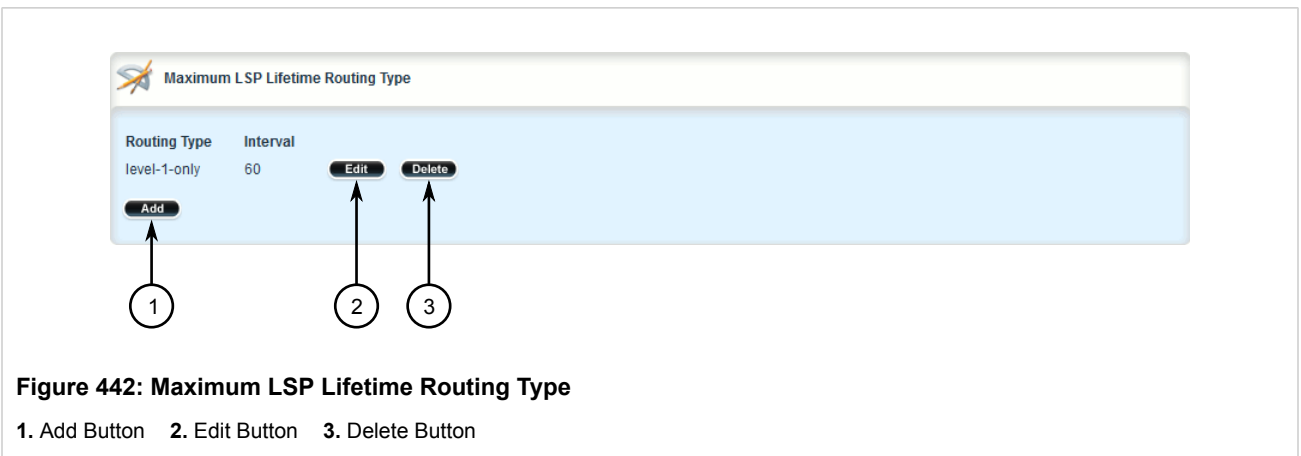


## Section 5.17.9.3

## Deleting an LSP Lifetime Interval

To delete an LSP lifetime interval for an IS-IS area, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis » area » {name} » max-lsp-lifetime**, where **{name}** is the unique name for a routing process that belongs to a specific router. The **Maximum LSP Lifetime Routing Type** table appears.



3. Click **Delete** next to the chosen interval.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.17.10

## 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.

The following sections describe how to configure and manage refresh intervals for LSPs:

**NOTE**

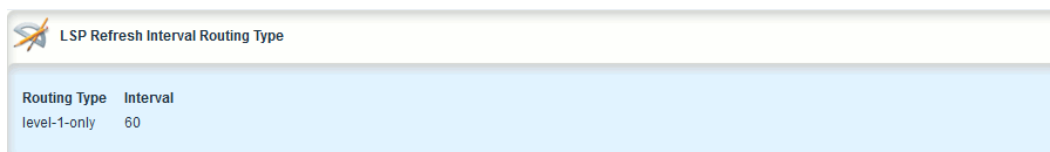
For information about configuring the lifetime of an LSP, refer to [Section 5.17.9, “Managing the Lifetime of LSPs”](#).

- [Section 5.17.10.1, “Viewing a List of LSP Refresh Intervals”](#)
- [Section 5.17.10.2, “Adding an LSP Refresh Interval”](#)
- [Section 5.17.10.3, “Deleting an LSP Refresh Interval”](#)

### Section 5.17.10.1

## Viewing a List of LSP Refresh Intervals

To view a list of LSP refresh intervals configured for an IS-IS area, navigate to **routing » dynamic » 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, the **LSP Refresh Interval Routing Type** table appears.



Routing Type	Interval
level-1-only	60

**Figure 443: LSP Refresh Interval Routing Type**

If no intervals have been configured, add intervals as needed. For more information, refer to [Section 5.17.10.2](#), “Adding an LSP Refresh Interval”.

### Section 5.17.10.2

## Adding an LSP Refresh Interval

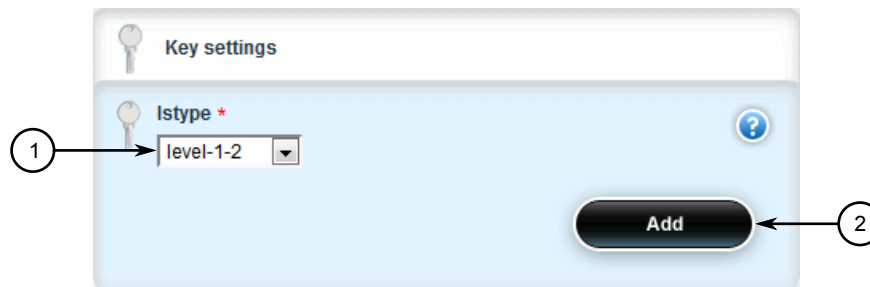
To add an LSP refresh interval to an IS-IS area, do the following:



### 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 5.17.9](#), “Managing the Lifetime of LSPs”.*

1. Navigate to **routing » dynamic » isis » area » {name} » lsp-refresh-interval**, where {name} is the unique name for a routing process that belongs to a specific router.
2. Click **<Add is-type>**. The **Key Settings** form appears.



**Figure 444: Key Settings Form**

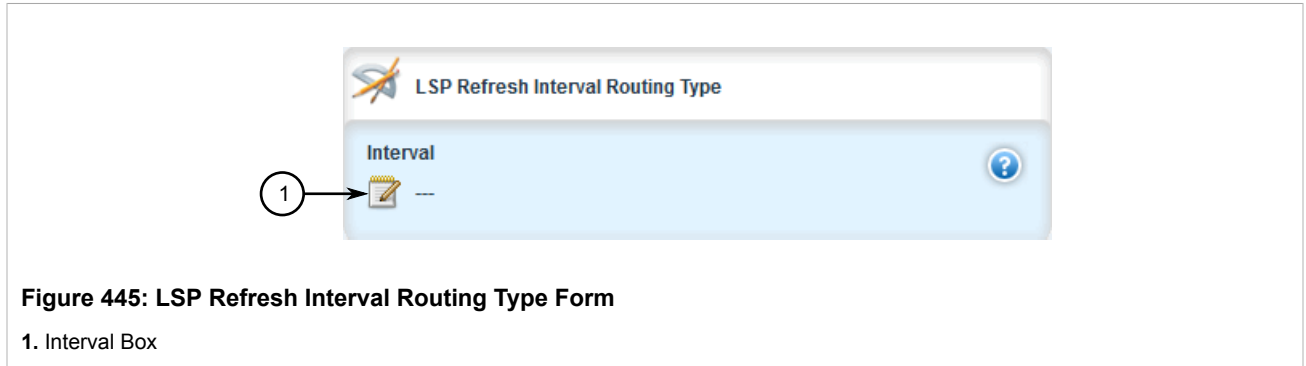
1. Routing Type List    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 }

Parameter	Description
	The IS type for this setting, specified as level-1-only, level-2-only or level-1-2.

- Click **Add** to create the new interval. The **LSP Refresh Interval Routing Type** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 1 and 65235 Minimum interval in seconds, ranging from LSP generating interval to Maximum LSP lifetime less 300 seconds. Default is 900.

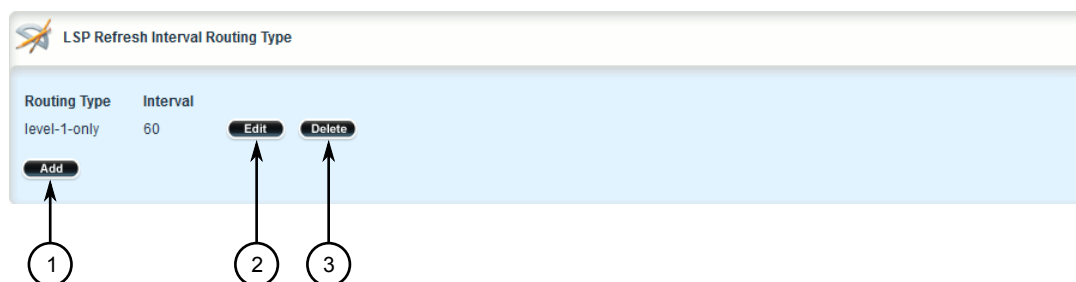
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.17.10.3

## Deleting an LSP Refresh Interval

To delete an LSP refresh interval for an IS-IS area, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » isis » area » {name} » lsp-refresh-interval**, where **{name}** is the unique name for a routing process that belongs to a specific router. The **LSP Refresh Interval Routing Type** table appears.



**Figure 446: LSP Refresh Interval Routing Type**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen interval.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.17.11

## 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 a 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 three two-byte numbers.
- 00 is the selector.



### IMPORTANT!

*The system identifier must be unique to the network.*

The following sections describe how to configure and manage NETs for IS-IS areas:

- [Section 5.17.11.1, "Viewing a List of NETs"](#)
- [Section 5.17.11.2, "Adding a NET"](#)

- [Section 5.17.11.3, “Deleting a NET”](#)

Section 5.17.11.1

Viewing a List of NETs

To view a list of NETs configured for an IS-IS area, navigate to *routing » dynamic » isis » area » {name} » net*, where **{name}** is the unique name for the area. The **Network Entity Title** table appears.

Network Entity Title	
Net-title	49.0001.1921.6800.1001.00

Figure 447: Network Entity Title Table

If no NETs have been configured, add NETs as needed. For more information, refer to [Section 5.17.11.2, “Adding a NET”](#).

Section 5.17.11.2

Adding a NET

To add a Network Entity Title (NET) for an IS-IS area, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *routing » dynamic » isis » area » {name} » net*, where **{name}** is the unique name for the area.
3. Click **<Add net>**. The **Key Settings** form appears.

Figure 448: Key Settings Form

1. Net-title Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Title	<b>Synopsis:</b> A string 20 to 50 characters long

Parameter	Description
	Network Entity Title (<OSI address>.<system Id>.00)

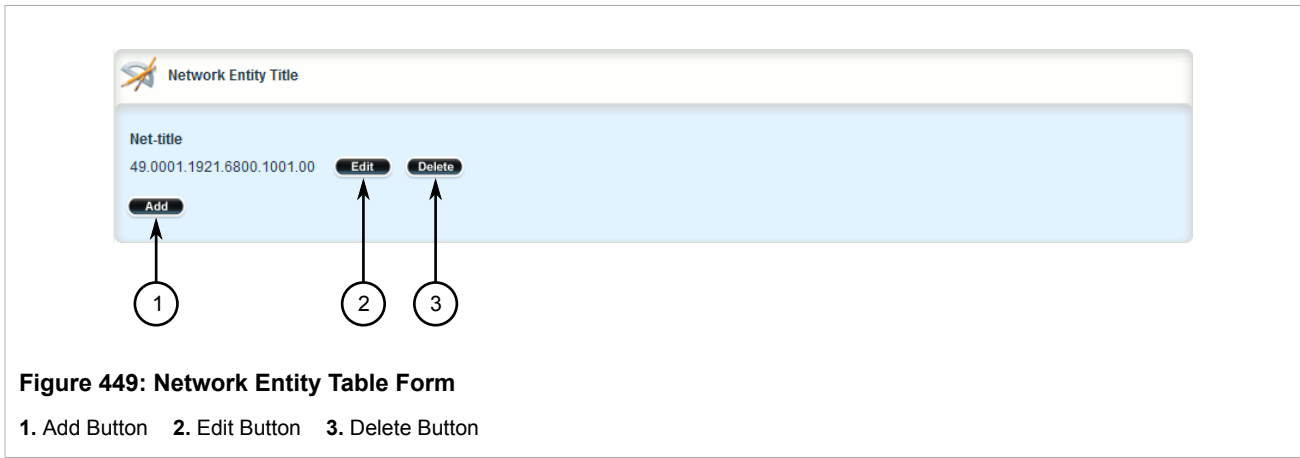
- Click **Add** to create the new NET.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.17.11.3

Deleting a NET

To delete a Network Entity Title (NET) for an IS-IS area, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to *routing » dynamic » isis » area » {name} » net*, where **{name}** is the unique name for the area. The **Network Entity Title** table appears.



- Click **Delete** next to the chosen area.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.17.12

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.


The following sections describe how to configure and manage redistribution metrics for IS-IS:

- [Section 5.17.12.1, “Viewing a List of Redistribution Metrics”](#)
- [Section 5.17.12.2, “Adding a Redistribution Metric”](#)
- [Section 5.17.12.3, “Deleting a Redistribution Metric”](#)

Section 5.17.12.1

## Viewing a List of Redistribution Metrics

To view a list of redistribution metrics defined for an IS-IS area, navigate to **routing » dynamic » isis » area » {name} » redistribute**, where {name} is the unique name for the area. The **Redistribute** table appears.



The screenshot shows a web interface window titled "Redistribute" with a table containing one row of data. The table has four columns: Source, Is-type, Metric-type, and Metric. The row contains the values: bgp, level-1-2, internal, and 10.

Source	Is-type	Metric-type	Metric
bgp	level-1-2	internal	10

Figure 450: Redistribute Table

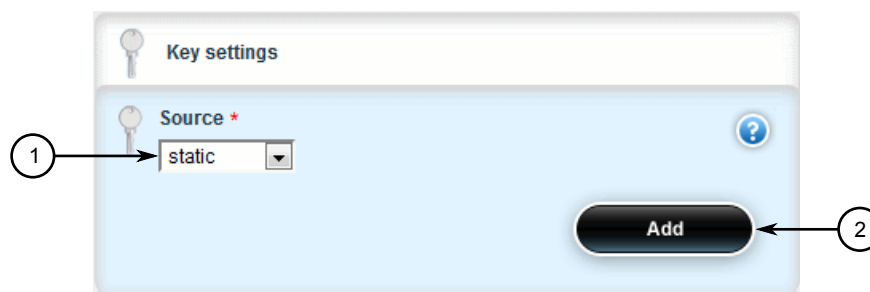
If no redistribution metrics have been configured, add metrics as needed. For more information, refer to [Section 5.17.12.2, “Adding a Redistribution Metric”](#).

Section 5.17.12.2

## Adding a Redistribution Metric

To add a redistribution metric for an IS-IS area, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » isis » area » {name} » redistribute**, where {name} is the unique name for the area.
3. Click **<Add redistribute>**. The **Key Settings** form appears.



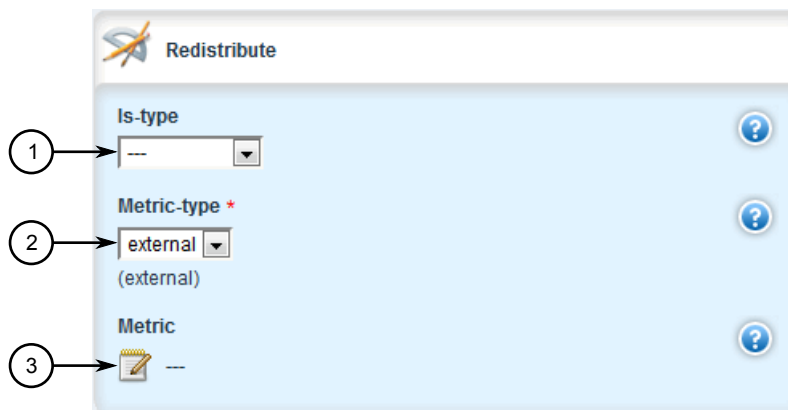
**Figure 451: Key Settings Form**

1. Source List 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Source	<b>Synopsis:</b> { bgp, connected, kernel, ospf, rip, static } Protocol that is source of IS-IS information.

5. Click **Add** to create the new metric. The **Redistribute** form appears>



**Figure 452: Redistribute Form**

1. IS-Type List 2. Metric-Type List 3. Metric Box

6. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	<b>Synopsis:</b> { level-1-only, level-2-only, level-1-2 } IS type of the IS-IS information, specified as level-1-only, level-2-only or level-1-2. If not provided, uses IS type from area.
Metric Type	<b>Synopsis:</b> { internal, external } <b>Default:</b> external The IS-IS metric type for redistributed routes. Default is external



Parameter	Description
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric for redistributed routes.

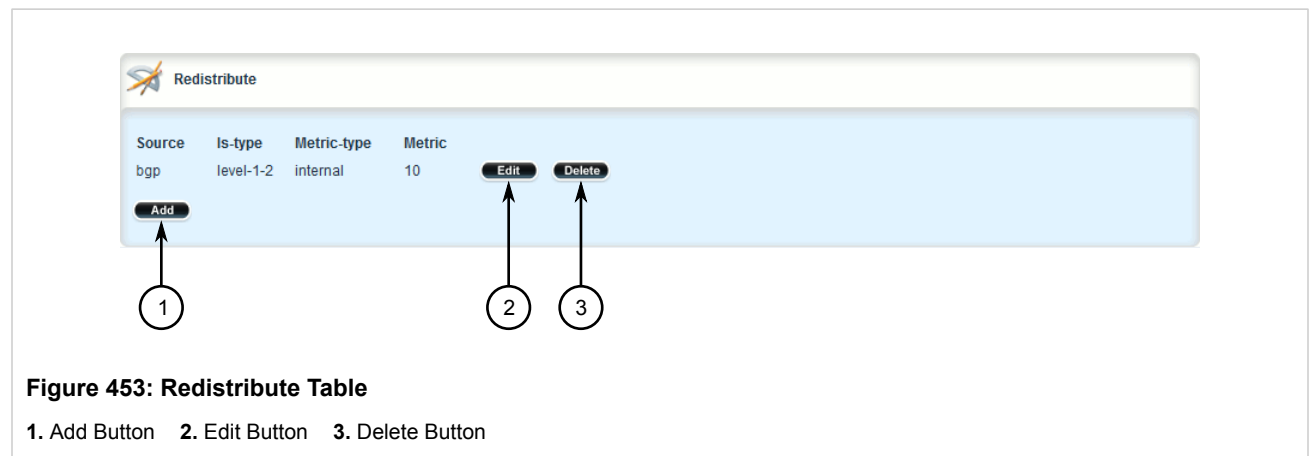
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.17.12.3

## Deleting a Redistribution Metric

To delete a redistribution metric for an IS-IS area, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » isis » area » {name} » redistribute**, where **{name}** is the unique name for the area. The **Redistribute** table appears.



- Click **Delete** next to the chosen metric.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.18

## Managing BGP

The Border Gateway Protocol (BGP) as defined by [RFC 4271](http://tools.ietf.org/rfc/rfc4271.txt) [http://tools.ietf.org/rfc/rfc4271.txt] is a robust and scalable routing protocol. BGP is designed to manage a routing table of up to 90000 routes. Therefore, it is used in large networks or among groups of networks which have common administrative and routing policies. External BGP (eBGP) is used to exchange routes between different Autonomous Systems (AS). Interior BGP (iBGP) is used to exchange routes within autonomous system (AS).

BGP is used by the bgpd daemon to handle communications with other routers. The daemon also determines which routers it prefers to forward traffic to for each known network route.



#### NOTE

*In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.*

The following sections describe how to configure and manage BGP:

- [Section 5.18.1, “Configuring BGP”](#)
- [Section 5.18.2, “Viewing the Status of Dynamic BGP Routes”](#)
- [Section 5.18.3, “Managing Route Maps”](#)
- [Section 5.18.4, “Managing Prepended and Excluded Autonomous System Paths”](#)
- [Section 5.18.5, “Managing Prefix Lists and Entries”](#)
- [Section 5.18.6, “Managing Autonomous System Paths and Entries”](#)
- [Section 5.18.7, “Managing Neighbors”](#)
- [Section 5.18.8, “Managing Networks”](#)
- [Section 5.18.9, “Managing Aggregate Addresses”](#)
- [Section 5.18.10, “Managing Aggregate Address Options”](#)
- [Section 5.18.11, “Managing Redistribution Metrics”](#)

#### Section 5.18.1

## Configuring BGP

To configure dynamic routing with BGP, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp**. The **Distance** and **BGP Configuration** forms appear.

Distance

1 → External Routes Distance

2 → Internal Routes Distance

3 → Local Routes Distance

**Figure 454: Distance Form**

1. External Routes Distance Box    2. Internal Routes Distance Box    3. Local Routes Distance Box

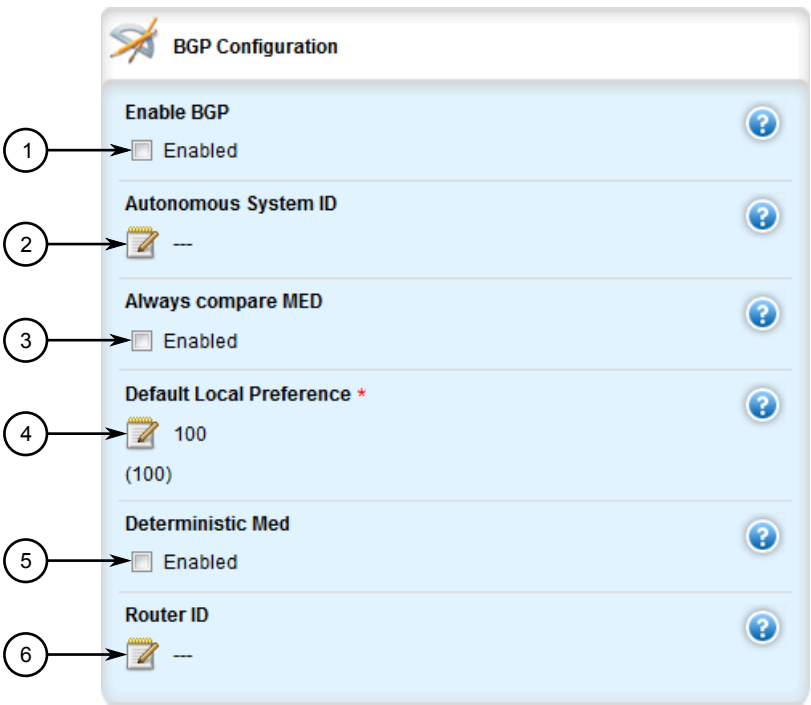


Figure 455: BGP Configuration

1. Enable BGP Check Box    2. Autonomous System ID Box    3. Always Compare MED Check Box    4. Default Local Preference Box    5. Deterministic MED Check Box    6. Router ID Box

3. In the **Distance** form, configure the following parameters:

Parameter	Description
External Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 Distance value for external routes. <b>Prerequisite:</b> external, internal and local must all be empty or all be configured.
Internal Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 Distance value for internal routes. <b>Prerequisite:</b> external, internal and local must all be empty or all be configured.
Local Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 Distance value for local routes. <b>Prerequisite:</b> external, internal and local must all be empty or all be configured.

4. In the **BGP Configuration** form, configure the following parameters:

Parameter	Description
Enable BGP	<b>Synopsis:</b> typeless Enables BGP.

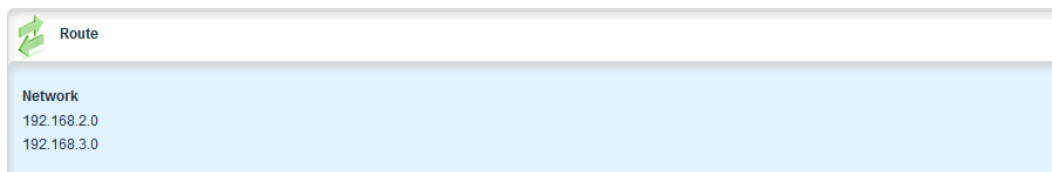
Parameter	Description
Autonomous System ID	<b>Synopsis:</b> An integer between 1 and 65535 Autonomous System ID.
Always compare MED	<b>Synopsis:</b> typeless Always comparing MED from different neighbors.
Default Local Preference	<b>Default:</b> 100 Default local preference value.
Deterministic Med	<b>Synopsis:</b> typeless Pick the best-MED path among paths advertised from neighboring AS.
Router ID	<b>Synopsis:</b> A string 7 to 15 characters long Router ID for BGP.

5. Configure autonomous system path filters. For more information, refer to [Section 5.18.6.3, “Adding an Autonomous System Path Filter”](#).
6. Configure prefix list filters. For more information, refer to [Section 5.18.5.3, “Adding a Prefix List”](#).
7. Configure route map filters. For more information, refer to [Section 5.18.3.3, “Adding a Route Map Filter”](#).
8. Configure a network. For more information, refer to [Section 5.18.8.2, “Adding a Network”](#).
9. Configure IP addresses for neighbors. For more information, refer to [Section 5.18.7.2, “Adding a Neighbor”](#).
10. Configure aggregate addresses. For more information, refer to [Section 5.18.9.2, “Adding an Aggregate Address”](#).
11. Configure redistribution metrics. For more information, refer to [Section 5.18.11.2, “Adding a Redistribution Metric”](#).
12. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
13. Click **Exit Transaction** or continue making changes.

## Section 5.18.2

# Viewing the Status of Dynamic BGP Routes

To view the status of the dynamic BGP routes configured on the device, navigate to **routing » status » bgp » route**. If BGP routes have been configured, the **Route** table appears.



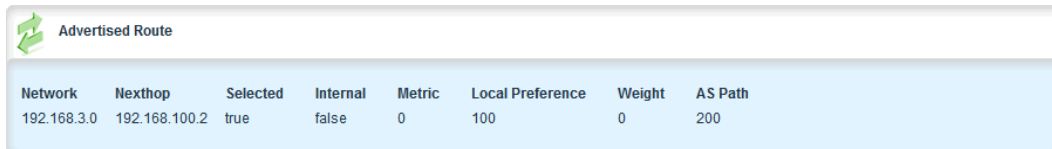
Route
Network
192.168.2.0
192.168.3.0

**Figure 456: Route Table**

The **Route** table provides the following information:

Parameter	Description
Network	<b>Synopsis:</b> A string Network.

To view the routing information advertised to the network, navigate to **routing » status » bgp » neighbor » advertised-route**. The **Advertised Route** table appears.



Advertised Route							
Network	Nexthop	Selected	Internal	Metric	Local Preference	Weight	AS Path
192.168.3.0	192.168.100.2	true	false	0	100	0	200

**Figure 457: Advertised Route Table**

The **Advertised Route** table provides the following information:

Parameter	Description
Network	<b>Synopsis:</b> A string Network.
Nexthop	<b>Synopsis:</b> A string Next-hop address.
Selected	<b>Synopsis:</b> true or false Selected next-hop for this route.
Internal	<b>Synopsis:</b> true or false Internal route.
Metric	Metric value.
Local Preference	<b>Synopsis:</b> A string Local preference.
Weight	Weight.
AS Path	<b>Synopsis:</b> A string Path.
Origin	<b>Synopsis:</b> A string Origin.

If no dynamic BGP routes have been configured, configure BGP and add routes as needed. For more information about configuring BGP, refer to [Section 5.18.1, “Configuring BGP”](#).

### Section 5.18.3

## 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.


The following sections describe how to configure and manage route maps for BGP:

- [Section 5.18.3.1, “Viewing a List of Route Map Filters”](#)
- [Section 5.18.3.2, “Viewing a List of Route Map Filter Entries”](#)
- [Section 5.18.3.3, “Adding a Route Map Filter”](#)
- [Section 5.18.3.4, “Adding a Route Map Filter Entry”](#)
- [Section 5.18.3.5, “Deleting a Route Map Filter”](#)
- [Section 5.18.3.6, “Deleting a Route Map Filter Entry”](#)
- [Section 5.18.3.7, “Configuring Match Rules”](#)
- [Section 5.18.3.8, “Configuring a Set”](#)

Section 5.18.3.1

Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic BGP, navigate to *routing » dynamic » bgp » filter » route-map*. If filters have been configured, the **Route Map** table appears.



The screenshot shows a web interface titled "Route Map" with a sub-header "Route Map Tag" and a single entry "route".

Route Map Tag
route

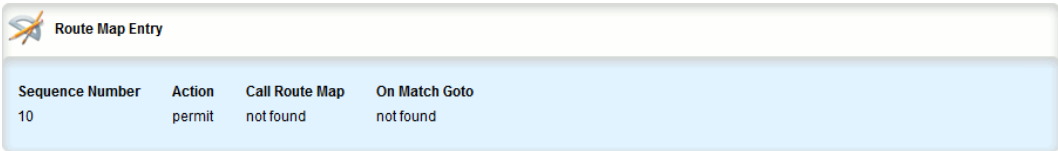
Figure 458: Route Map Table

If no filters have been configured, add filters as needed. For more information, refer to [Section 5.18.6.3, “Adding an Autonomous System Path Filter”](#).

Section 5.18.3.2

Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either BGP, navigate to *routing » dynamic » bgp » filter » route-map » {tag} » entry*, where {tag} is the tag for the route map filter. If entries have been configured, the **Route Map Entry** table appears.



The screenshot shows a web interface titled "Route Map Entry" with a table containing one entry. The table has four columns: Sequence Number, Action, Call Route Map, and On Match Goto.

Sequence Number	Action	Call Route Map	On Match Goto
10	permit	not found	not found

Figure 459: Route Map Entry Table

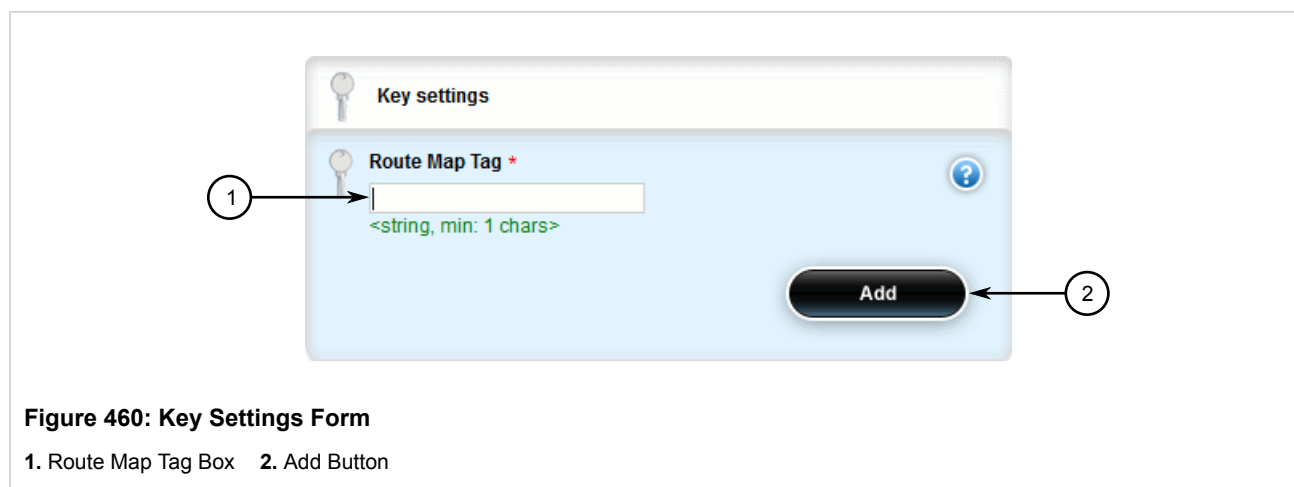
If no filters have been configured, add filters as needed. For more information, refer to [Section 5.18.6.3, “Adding an Autonomous System Path Filter”](#).

## Section 5.18.3.3

## Adding a Route Map Filter

To add a route map filter for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map** and click **<Add route-map>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Route Map Tag	<b>Synopsis:</b> A string 1 to 1024 characters long Route map tag.

4. Click **Add** to create the new filter.
5. Add one or more entries. For more information, refer to [Section 5.18.3.4, “Adding a Route Map Filter Entry”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 5.18.3.4

## Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map » {tag} » entry**, where *{tag}* is the tag for the route map filter.
3. Click **<Add entry>**. The **Key Settings** form appears.

**Figure 461: Key Settings Form**

1. Sequence Number Box 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 65535 The sequence number of the route-map entry.

5. Click **Add** to create the new entry. The **Route Map Entry** form appears.

**Figure 462: Route Map Entry Form**

1. Action List 2. Call Route Map List 3. On Match Goto List

6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { deny, permit } <b>Default:</b> permit Action.
Call Route Map	Jump to another route-map after match+set.
On Match Goto	Go to this entry on match.



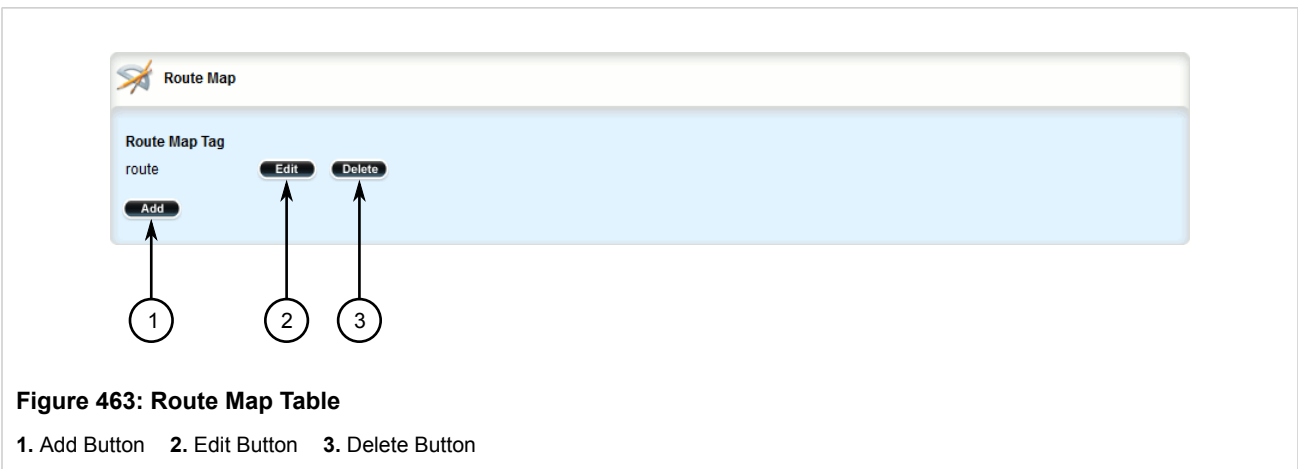
7. Configure the match rules for the route map filter. For more information, refer to [Section 5.18.3.7, “Configuring Match Rules”](#).
8. Configure a set for the route map filter. For more information, refer to [Section 5.18.3.8, “Configuring a Set”](#).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
10. Click **Exit Transaction** or continue making changes.

#### Section 5.18.3.5

### Deleting a Route Map Filter

To delete a route map filter for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map**. The **Route Map** table appears.



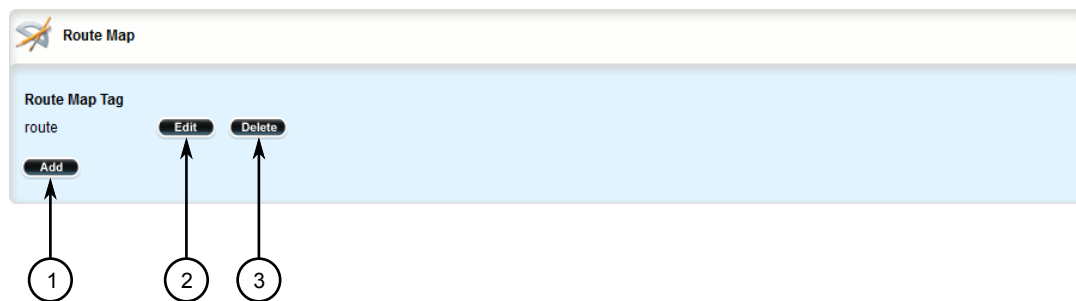
3. Click **Delete** next to the chosen filter.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.3.6

### Deleting a Route Map Filter Entry

To delete an entry for a route map filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map » {tag} » entry**, where {tag} is the tag for the route map filter. The **Route Map Entry** table appears.



**Figure 464: Route Map Entry Table**

1. Add Button 2. Edit Button 3. Delete Button

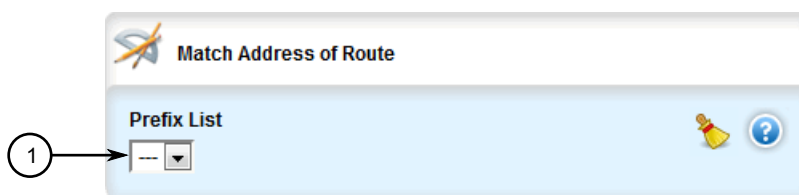
3. Click **Delete** next to the chosen entry.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.3.7

### Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » 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. The **Match Address of Route**, **Match Nexthop of Route**, **Match Advertising Source Address** and **Match** forms appear.



**Figure 465: Match Address of Route Form**

1. Prefix List List

The screenshot shows the 'Match Nexthop of Route' configuration form. It has a title bar with a router icon and the text 'Match Nexthop of Route'. Below the title bar is a light blue section labeled 'Prefix List'. Inside this section is a dropdown menu with a downward arrow. A callout circle with the number '1' points to this dropdown menu. To the right of the dropdown are a yellow bell icon and a blue circle with a question mark icon.

Figure 466: Match Nexthop of Route Form

1. Prefix List List

The screenshot shows the 'Match Advertising Source Address' configuration form. It has a title bar with a router icon and the text 'Match Advertising Source Address'. Below the title bar is a light blue section labeled 'Prefix List'. Inside this section is a dropdown menu with a downward arrow. A callout circle with the number '1' points to this dropdown menu. To the right of the dropdown are a yellow bell icon and a blue circle with a question mark icon.

Figure 467: Match Advertising Source Address Form

1. Prefix List List

The screenshot shows the 'Match' configuration form. It has a title bar with a router icon and the text 'Match'. Below the title bar are four light blue sections, each with a label and a field. A callout circle with the number '1' points to the 'AS Path Filter' dropdown. A callout circle with the number '2' points to the 'Metric' field. A callout circle with the number '3' points to the 'Peer Address' field. A callout circle with the number '4' points to the 'Origin' dropdown. Each field has a yellow bell icon and a blue circle with a question mark icon to its right.

Figure 468: Match Form

1. AS Path Filter List   2. Metric Box   3. Peer Address Box   4. Origin List

3. On the **Match Address of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	The prefix list name.

4. On the **Match Nexthop of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	The prefix list name.

5. On the **Match Advertising Source Address** form, configure the following parameters as required:

Parameter	Description
Prefix List	The prefix list name.

6. On the **Match** form, configure the following parameters as required:

Parameter	Description
AS Path Filter	Match the BGP AS path filter.
Metric	Match the route metric.
Peer Address	<b>Synopsis:</b> A string 7 to 15 characters long This parameter is not supported and any value is ignored by the system.s
Origin	<b>Synopsis:</b> { egp, igp, incomplete } Match the BGP origin code.

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.18.3.8

### Configuring a Set

To configure matched rules for a route map filter entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » 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. The **Aggregator**, **Metric** and **Set** forms appear.

The screenshot shows a web form titled '/routing/dynamic/bgp/filter/route-map/entry/set/aggregator'. It contains two input fields: 'AS Number' and 'IP Address'. Both fields have a question mark icon to their right. A circled '1' points to the 'AS Number' field, and a circled '2' points to the 'IP Address' field.

**Figure 469: Aggregator Form**

1. AS Number Box    2. IP Address Box

**Figure 470: Metric Form**  
1. Operation List    2. Value Box

**Figure 471: Set Form**  
1. Local Preference Box    2. Next Hop Box    3. Origin List    4. Originator ID Box    5. Weight Box

3. On the **Aggregator** form, configure the following parameters as required:

Parameter	Description
AS Number	<b>Synopsis:</b> An integer between 1 and 4294967295 AS number. <b>Prerequisite:</b> as must be empty when ip is not configured.
IP Address	<b>Synopsis:</b> A string 7 to 15 characters long IP address of aggregator. <b>Prerequisite:</b> ip must be empty when as is not configured.

4. On the **Metric** form, configure the following parameters as required:

Parameter	Description
operation	<b>Synopsis:</b> { set, add, sub } Set , add or subtract the metric value. <b>Prerequisite:</b> Operation must be empty when value is not configured.
value	Value. <b>Prerequisite:</b> value must be empty when operation is not configured.

5. On the **Set** form, configure the following parameters as required:

Parameter	Description
Local Preference	Local preference.
next-hop	<b>Synopsis:</b> { 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	<b>Synopsis:</b> { egp, igp, incomplete } The origin code.
originator-id	<b>Synopsis:</b> A string 7 to 15 characters long This parameter is not supported and any value is ignored by the system.
weight	Weight.

6. Add pre-pended and/or excluded autonomous system paths. For more information, refer to [Section 5.18.4.3, “Adding a Prepended Autonomous System Path Filter”](#) and/or [Section 5.18.4.4, “Adding an Excluded Autonomous System Path filter”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.18.4

## Managing Prepended and Excluded Autonomous System Paths

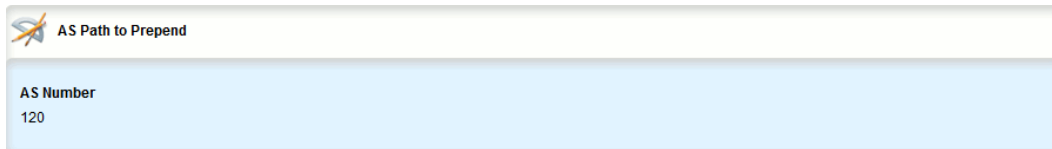
The following sections describe how to configure and manage prepended and excluded autonomous system paths:

- [Section 5.18.4.1, “Viewing a List of Prepended Autonomous System Path Filters”](#)
- [Section 5.18.4.2, “Viewing a List of Excluded Autonomous System Paths”](#)
- [Section 5.18.4.3, “Adding a Prepended Autonomous System Path Filter”](#)
- [Section 5.18.4.4, “Adding an Excluded Autonomous System Path filter”](#)
- [Section 5.18.4.5, “Deleting a Prepended Autonomous System Path Filter”](#)
- [Section 5.18.4.6, “Deleting an Excluded Autonomous System Path Filter”](#)

## Section 5.18.4.1

## Viewing a List of Prepended Autonomous System Path Filters

To view a list of prependded autonomous system path filters configured for a BGP route map entry, navigate to **routing » dynamic » bgp » filter » route-map » {name} » entry » {number} » set » as-path » prepend**, where {name} is the name of the route map and {number} is the entry number. If filters have been configured, the **AS Path to Prepend** table appears.



AS Path to Prepend
AS Number 120

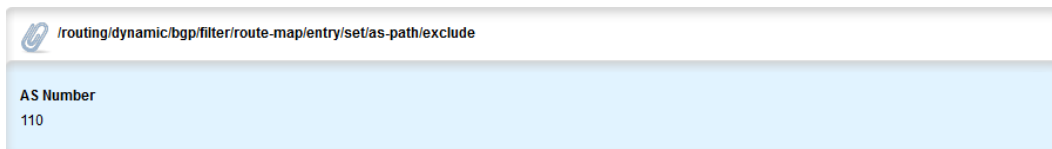
Figure 472: AS Path to Prepend Table

If no prependded autonomous system path filters have been configured, add filters as needed. For more information, refer to [Section 5.18.4.3, “Adding a Prepended Autonomous System Path Filter”](#).

## Section 5.18.4.2

## 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, navigate to **routing » dynamic » bgp » filter » route-map » {name} » entry » {number} » set » as-path » exclude**, where {name} is the name of the route map and {number} is the entry number. If filters have been configured, the **AS Path to Exclude** table appears.



/routing/dynamic/bgp/filter/route-map/entry/set/as-path/exclude
AS Number 110

Figure 473: AS Path to Exclude Table

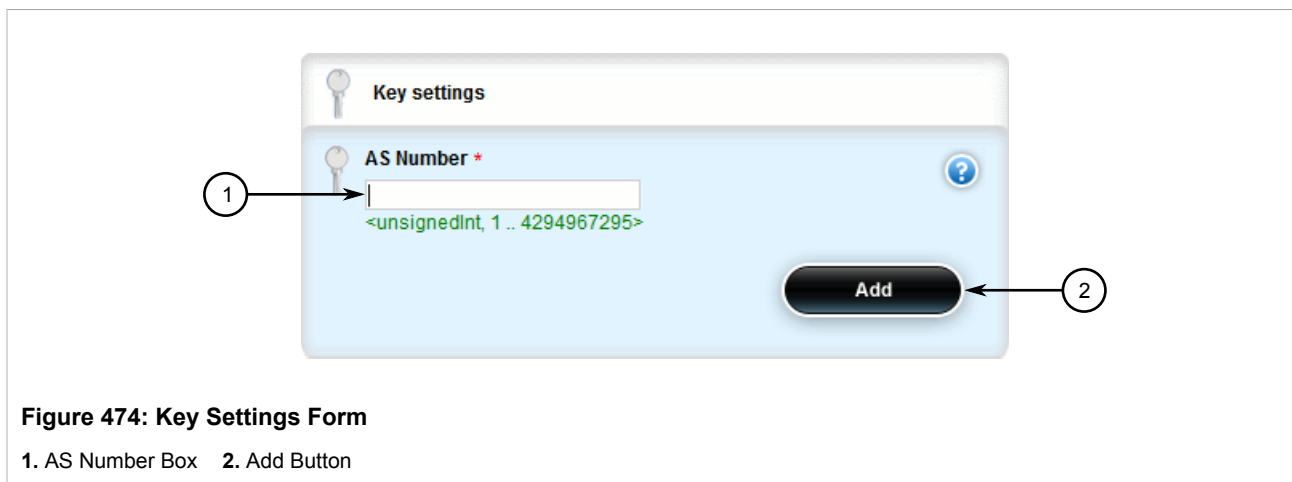
If no excluded autonomous system path filters have been configured, add filters as needed. For more information, refer to [Section 5.18.4.4, “Adding an Excluded Autonomous System Path filter”](#).

## Section 5.18.4.3

## Adding a Prepended Autonomous System Path Filter

To add a prependded autonomous system path filter to a BGP route map entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map » {name} » entry » {number} » set » as-path » prepend**, where {name} is the name of the route map and {number} is the entry number.
3. Click **<Add prepend>**. The **Key Settings** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
AS Number	<b>Synopsis:</b> An integer between 1 and 4294967295 AS number.

- Click **Add** to add the filter.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

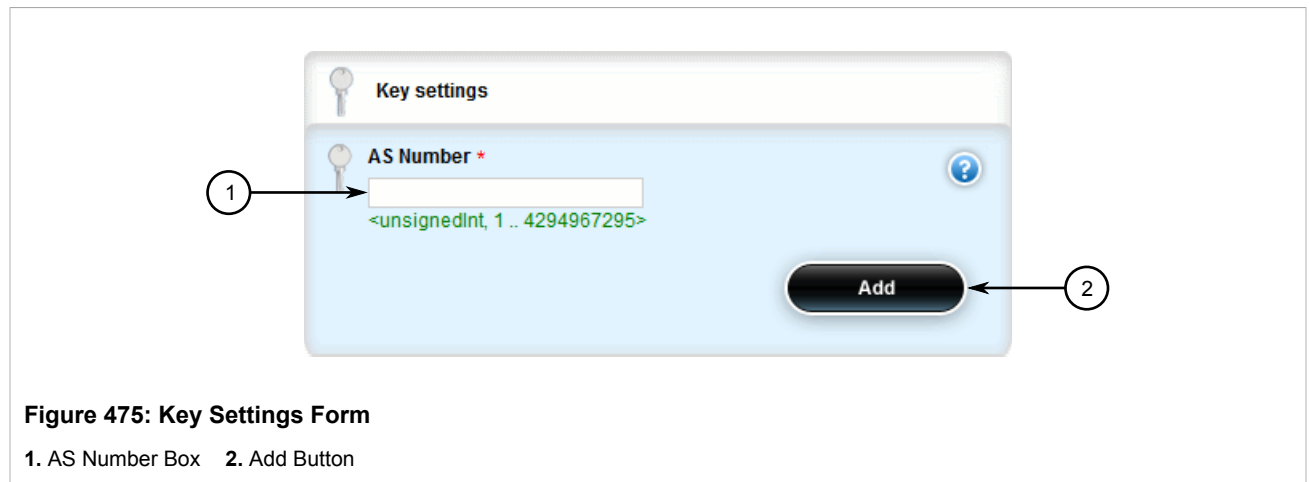
#### Section 5.18.4.4

### Adding an Excluded Autonomous System Path filter

To add an excluded autonomous system path filter to a BGP route map entry, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » bgp » filter » route-map » {name} » entry » {number} » set » as-path » exclude**, where {name} is the name of the route map and {number} is the entry number.
- Click **<Add prepend>**. The **Key Settings** form appears.





4. Configure the following parameter(s) as required:

Parameter	Description
AS Number	<b>Synopsis:</b> An integer between 1 and 4294967295 AS number.

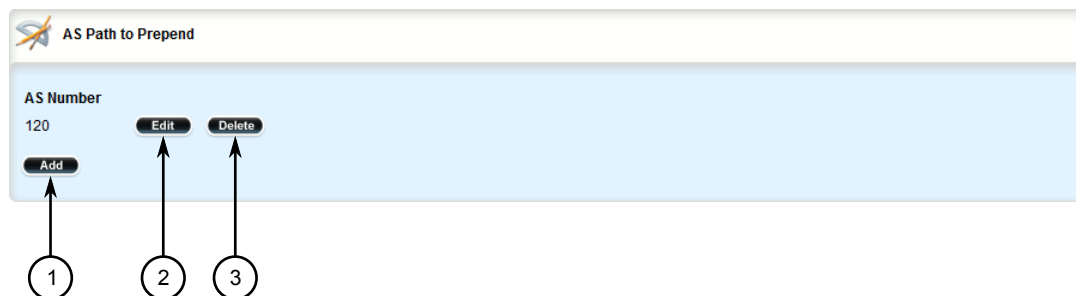
5. Click **Add** to add the filter.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.18.4.5

### Deleting a Prepended Autonomous System Path Filter

To delete a prepend autonomous system path filter from a BGP route map entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map » {name} » entry » {number} » set » as-path » prepend**, where {name} is the name of the route map and {number} is the entry number. The **AS Path to Prepend** table appears.



**Figure 476: AS Path to Prepend Table**

1. Add Button 2. Edit Button 3. Delete Button

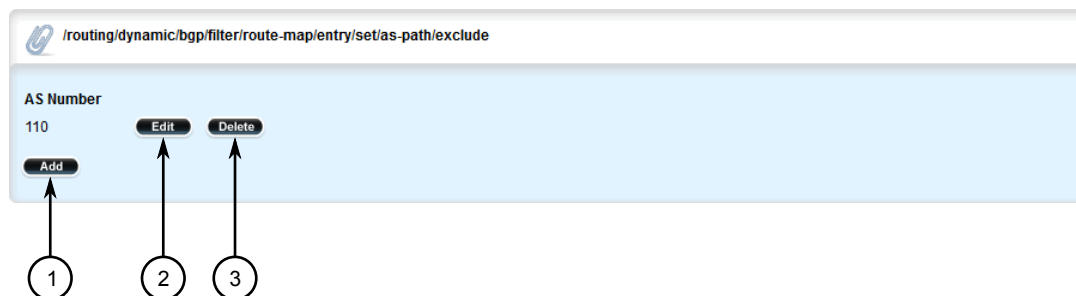
3. Click **Delete** next to the chosen filter.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.4.6

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » route-map » {name} » entry » {number} » set » as-path » exclude**, where {name} is the name of the route map and {number} is the entry number. The **AS Path to Exclude** table appears.



**Figure 477: AS Path to Exclude Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen filter.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.18.5

## 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.

The following sections describe how to configure and manage prefix lists and entries for dynamic BGP routes:

- [Section 5.18.5.1, “Viewing a List of Prefix Lists”](#)
- [Section 5.18.5.2, “Viewing a List of Prefix Entries”](#)
- [Section 5.18.5.3, “Adding a Prefix List”](#)
- [Section 5.18.5.4, “Adding a Prefix Entry”](#)
- [Section 5.18.5.5, “Deleting a Prefix List”](#)
- [Section 5.18.5.6, “Deleting a Prefix Entry”](#)

Section 5.18.5.1

### Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic BGP routes, navigate to one *routing » dynamic » bgp » filter » prefix-list*. If prefix lists have been configured, the **Prefix List** table appears.



The screenshot shows a web interface titled "Prefix List" with a table containing one entry. The table has two columns: "Prefix List" and "Description". The entry is "list-withdraw-33" with the description "not found".

Prefix List	Description
list-withdraw-33	not found

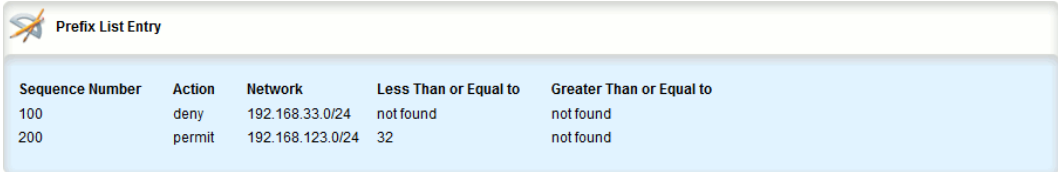
Figure 478: Prefix List Table

If no prefix lists have been configured, add lists as needed. For more information, refer to [Section 5.18.5.3, “Adding a Prefix List”](#).

Section 5.18.5.2

### Viewing a List of Prefix Entries

To view a list of entries for dynamic BGP prefix lists, navigate to *routing » dynamic » bgp » filter » {name} » entry*, where {name} is the name of the prefix list. If entries have been configured, the **Prefix List Entry** table appears.



The screenshot shows a web interface titled "Prefix List Entry" with a table containing two entries. The table has five columns: "Sequence Number", "Action", "Network", "Less Than or Equal to", and "Greater Than or Equal to".

Sequence Number	Action	Network	Less Than or Equal to	Greater Than or Equal to
100	deny	192.168.33.0/24	not found	not found
200	permit	192.168.123.0/24	32	not found

Figure 479: Prefix List Entry Table

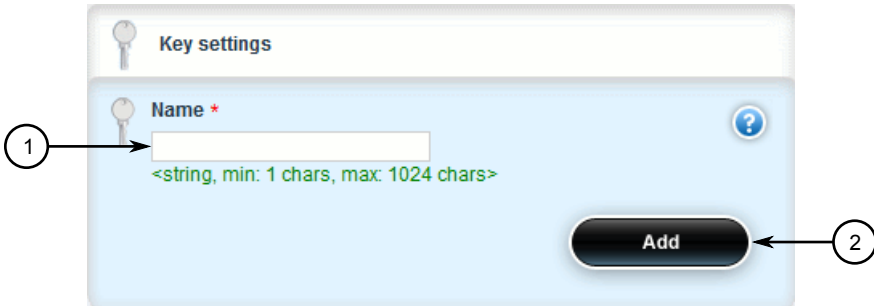
If no entries have been configured, add entries as needed. For more information, refer to [Section 5.18.5.4](#), “Adding a Prefix Entry”.

### Section 5.18.5.3

## Adding a Prefix List

To add a prefix list for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » prefix-list** and click **<Add prefix-list>**. The **Key Settings** form appears.



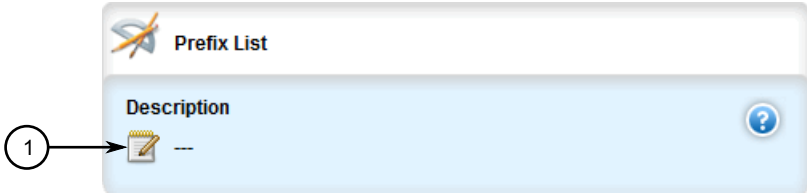
**Figure 480: Key Settings Form**

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 1024 characters long The name of the prefix list.

4. Click **Add** to create the new prefix-list. The **Prefix List** form appears.



**Figure 481: Prefix List Form**

1. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string 1 to 1024 characters long

Parameter	Description
	The description of the prefix list.

- Add prefix entries as needed. For more information, refer to [Section 5.18.5.4, “Adding a Prefix Entry”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.18.5.4

### Adding a Prefix Entry

To add an entry for a dynamic BGP prefix list, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Depending on the dynamic routing protocol being configured, navigate to **routing » dynamic » rip » filter » {name} » entry**, where *{name}* is the name of the prefix list.
- Click **<Add entry>**. The **Key Settings** form appears.

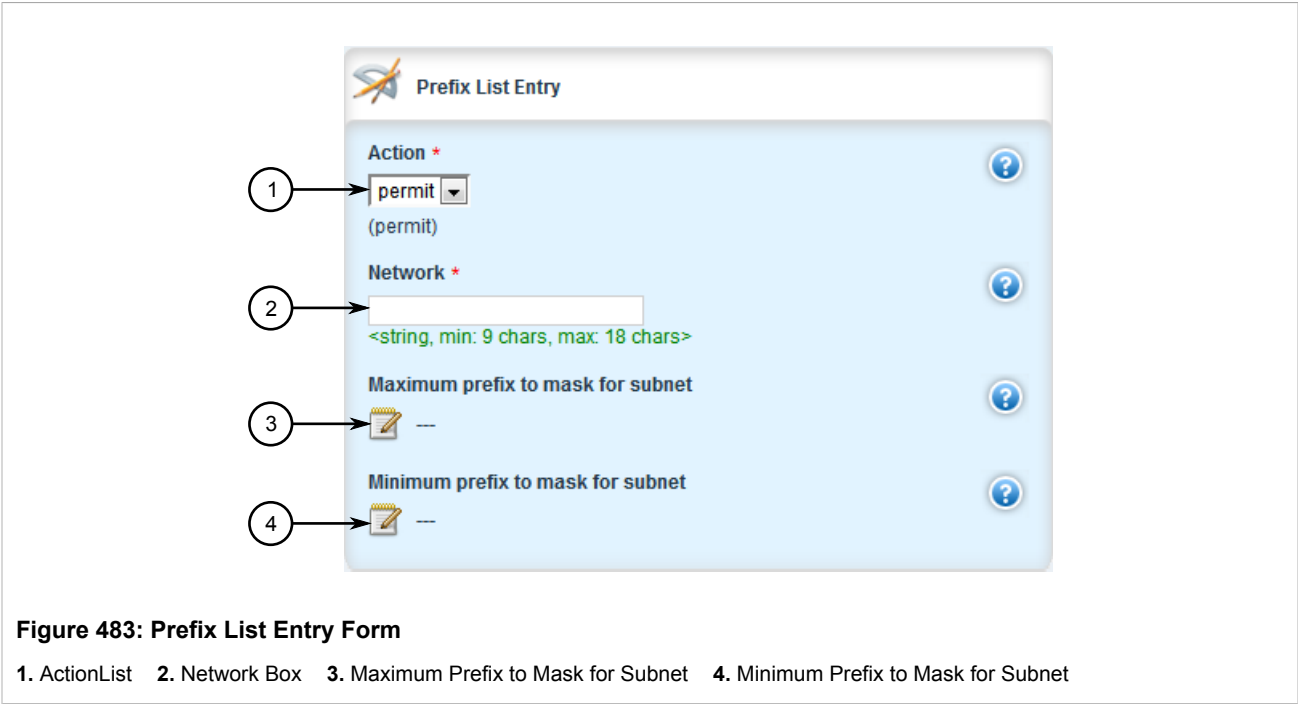
**Figure 482: Key Settings Form**

1. Sequence Number Box    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 4294967295 Sequence number of the entry.

- Click **Add** to create the new entry. The **Prefix List Entry** form appears.



**Figure 483: Prefix List Entry Form**

1. ActionList    2. Network Box    3. Maximum Prefix to Mask for Subnet    4. Minimum Prefix to Mask for Subnet

6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { deny, permit } <b>Default:</b> permit Action.
Network	<b>Synopsis:</b> A string 9 to 18 characters long Network (xxx.xxx.xxx.xxx/xx).
Maximum prefix to mask for subnet	<b>Synopsis:</b> An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
Minimum prefix to mask for subnet	<b>Synopsis:</b> An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

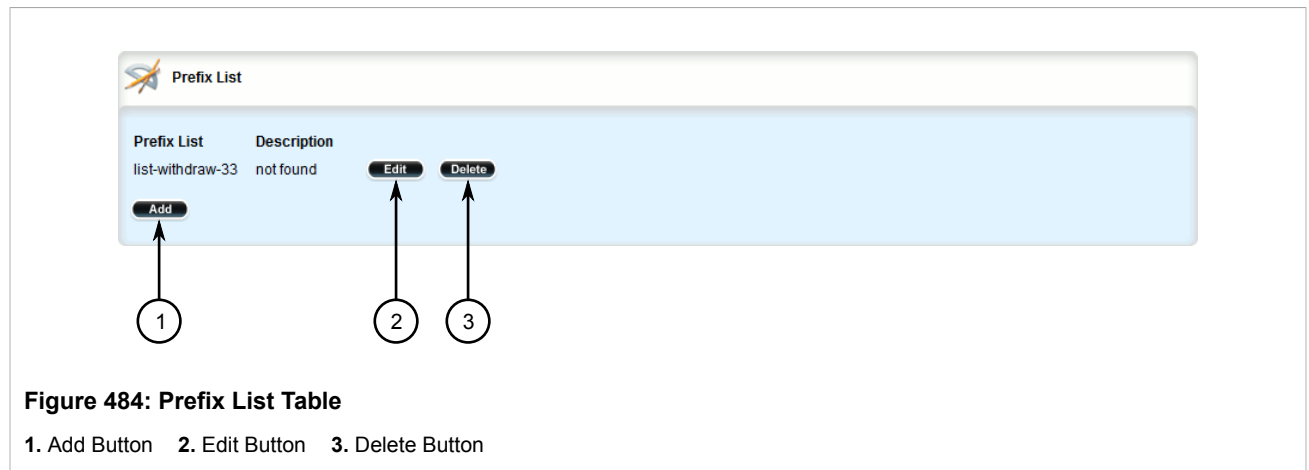
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 5.18.5.5

**Deleting a Prefix List**

To delete a prefix list for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *routing » dynamic » bgp » filter » prefix-list*. The **Prefix List** table appears.



#### NOTE

*Deleting a prefix list removes all associate prefix entries as well.*

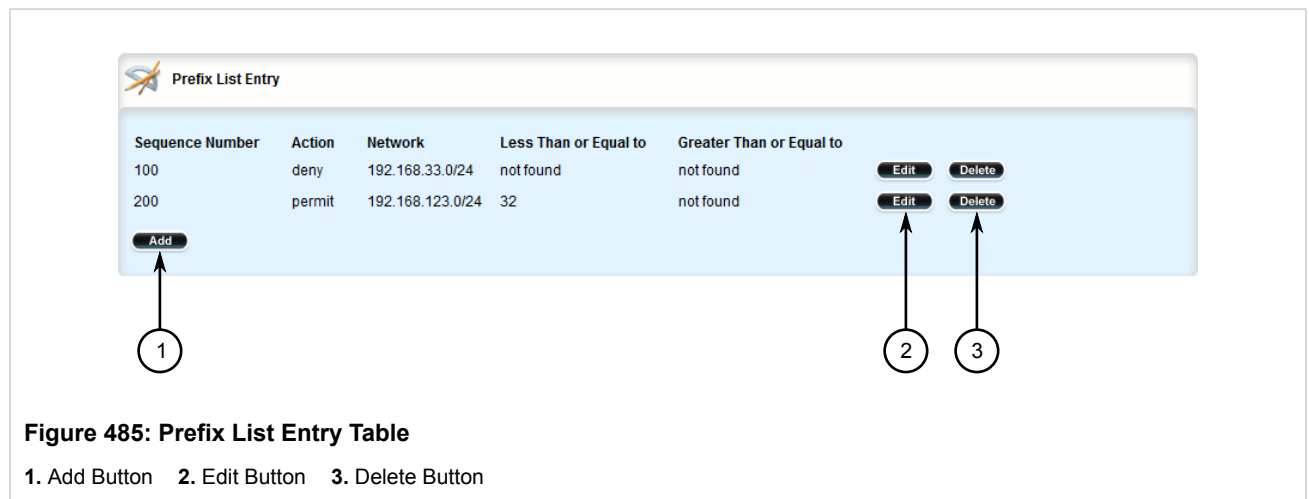
3. Click **Delete** next to the chosen prefix list.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.5.6

### Deleting a Prefix Entry

To delete an entry for a dynamic BGP prefix list, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Depending on the dynamic routing protocol being configured, navigate to **routing » dynamic » bgp » filter » {name} » entry**, where {name} is the name of the prefix list. The **Prefix List Entry** table appears.



3. Click **Delete** next to the chosen entry.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.18.6

## Managing Autonomous System Paths and Entries

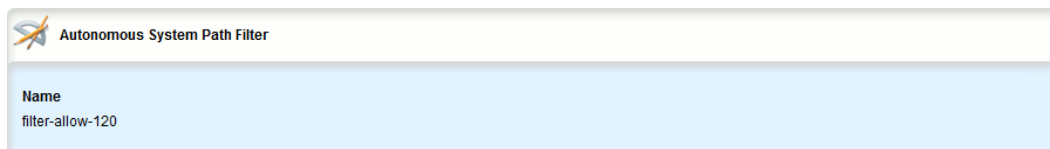
The following sections describe how to configure and manage autonomous system paths and entries for dynamic BGP routes:

- [Section 5.18.6.1, “Viewing a List of Autonomous System Paths”](#)
- [Section 5.18.6.2, “Viewing a List of Autonomous System Path Entries”](#)
- [Section 5.18.6.3, “Adding an Autonomous System Path Filter”](#)
- [Section 5.18.6.4, “Adding an Autonomous System Path Filter Entry”](#)
- [Section 5.18.6.5, “Deleting an Autonomous System Path”](#)
- [Section 5.18.6.6, “Deleting an Autonomous System Path Filter Entry”](#)

## Section 5.18.6.1

### Viewing a List of Autonomous System Paths

To view a list of autonomous system path filters for dynamic BGP routes, navigate to **routing » dynamic » bgp » filter » as-path**. If filters have been configured, the **Autonomous System Path Filter** table appears.



Name
filter-allow-120

**Figure 486: Autonomous System Path Filter Table**

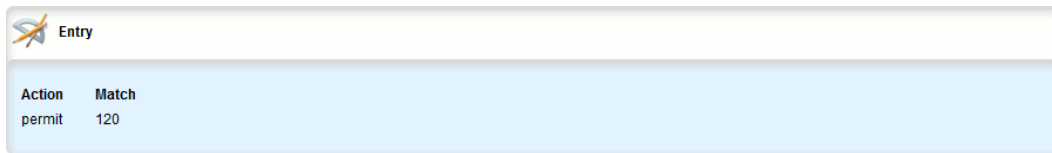
If no filters have been configured, add filters as needed. For more information, refer to [Section 5.18.6.3, “Adding an Autonomous System Path Filter”](#).

## Section 5.18.6.2

### Viewing a List of Autonomous System Path Entries

To view a list of entries for an autonomous system path filter, navigate to **routing » dynamic » bgp » filter » as-path » {name} » entry**, where {name} is the name of the autonomous system path filter. If entries have been configured, the **Entry** table appears.





Action	Match
permit	120

**Figure 487: Entry Table**

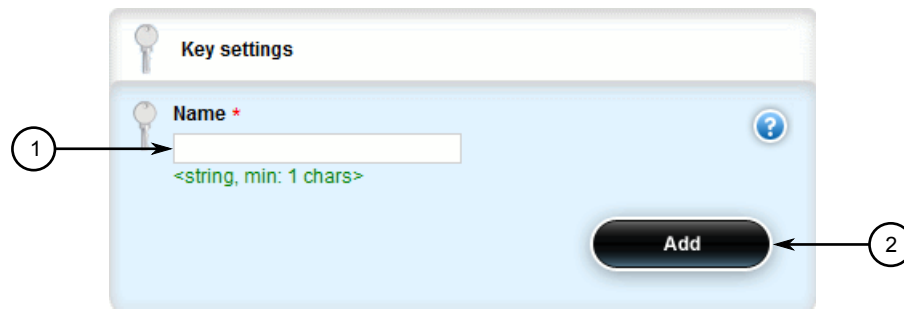
If no filters have been configured, add filters as needed. For more information, refer to [Section 5.18.6.3, “Adding an Autonomous System Path Filter”](#).

### Section 5.18.6.3

## Adding an Autonomous System Path Filter

To add an autonomous system path filter for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » as-path** and click **<Add as-path>**. The **Key Settings** form appears.

**Figure 488: Key Settings Form**

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 1024 characters long Name of the AS-path filter.

4. Click **Add** to create the new filter.
5. Add one or more entries. For more information, refer to [Section 5.18.6.4, “Adding an Autonomous System Path Filter Entry”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 5.18.6.4

## Adding an Autonomous System Path Filter Entry

Create an entry for an autonomous system path filter to match a string or integer value in AS path and then perform an action. The match criteria is defined using regular expressions. The following lists special characters that can be used in a regular expression:

Character	Description	Example
.	Matches any single character (e.g. .100, 100., .100.)	.100 100. .100.
*	Matches zero (0) or more occurrences of a pattern	100*
+	Matches 1 or more occurrences of a pattern	100+
?	Match 0 or 1 occurrences of a pattern	100?
^	Matches the beginning of the line	^100
\$	Matches the end of the line	100\$
()	Matches only the characters specified	(38a)
[]	Matches any character other than those specified	[^abc]
_ (underscore)	The underscore character has special meanings in an autonomous system path. It matches to: <ul style="list-style-type: none"><li>• Each space ( ) and comma (,)</li><li>• Each AS set delimiter (e.g. { and })</li><li>• Each AS confederation delimiter (e.g. ( and ))</li><li>• The beginning and end of the line</li></ul> Therefore, the underscore can be used to match AS values.	_100,100_, _100_

To add an entry for an autonomous system path filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » as-path » {name} » entry**, where {name} is the name of the autonomous system path filter.
3. Click **<Add entry>**. The **Key Settings** form appears.

**Figure 489: Key Settings Form**

1. Action List   2. Match Box   3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { deny, permit } Action.
Match	<b>Synopsis:</b> A string 1 to 1024 characters long The regular expression to match the BGP AS paths - for more information about regular expressions, refer to the User Guide.

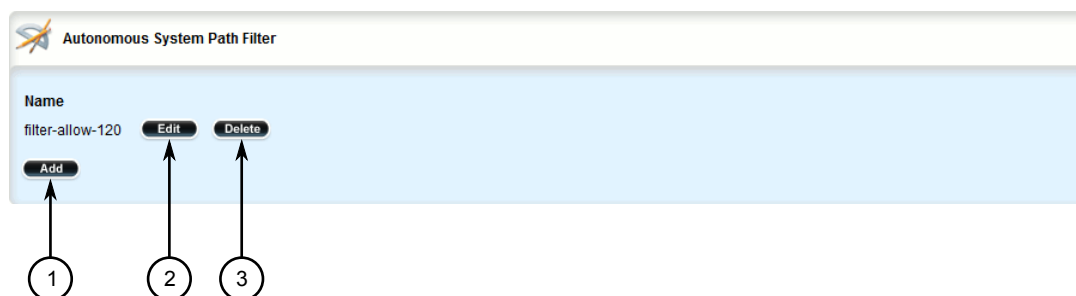
5. Click **Add** to create the new entry.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.18.6.5

### Deleting an Autonomous System Path

To delete an autonomous system path filter for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » as-path**. The **Autonomous System Path Filter** table appears.



**Figure 490: Autonomous System Path Filter Table**

1. Add Button 2. Edit Button 3. Delete Button

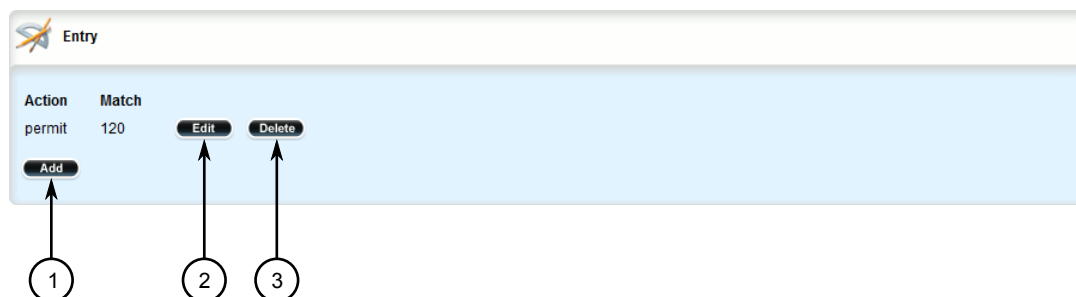
3. Click **Delete** next to the chosen filter.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.6.6

### Deleting an Autonomous System Path Filter Entry

To delete an entry for an autonomous system path filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » filter » as-path » {name} » entry**, where {name} is the name of the autonomous system path filter. The **Entry** table appears.



**Figure 491: Entry Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen entry.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.18.7

## 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 5.18.8, “Managing Networks”](#).*

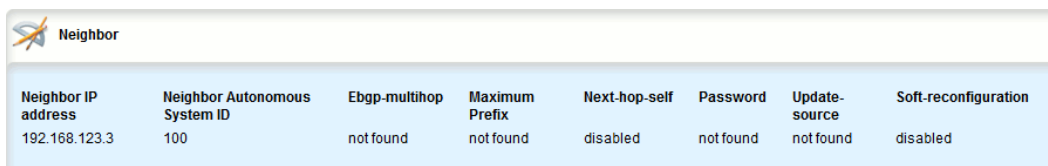
The following sections describe how to configure and manage neighbors for dynamic BGP routes:

- [Section 5.18.7.1, “Viewing a List of Neighbors”](#)
- [Section 5.18.7.2, “Adding a Neighbor”](#)
- [Section 5.18.7.3, “Configuring the Distribution of Prefix Lists”](#)
- [Section 5.18.7.4, “Tracking Commands for BGP Neighbors”](#)
- [Section 5.18.7.5, “Deleting a Neighbor”](#)

## Section 5.18.7.1

### Viewing a List of Neighbors

To view a list of neighbors configured for a BGP network, navigate to **routing » dynamic » bgp » neighbor**. If neighbors have been configured, the **Neighbor** table appears.



Neighbor IP address	Neighbor Autonomous System ID	Ebgp-multihop	Maximum Prefix	Next-hop-self	Password	Update-source	Soft-reconfiguration
192.168.123.3	100	not found	not found	disabled	not found	not found	disabled

**Figure 492: Neighbor Table**

If no neighbors have been configured, add neighbors as needed. For more information, refer to [Section 5.18.7.2, “Adding a Neighbor”](#).

## Section 5.18.7.2

### Adding a Neighbor

To add a neighbor for a BGP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » neighbor** and click **<Add neighbor>**. The **Key Settings** form appears.

**Figure 493: Key Settings Form**

1. Neighbor IP Address Box 2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string 7 to 15 characters long The neighbor IP address.

- Click **Add** to add the address. The **Route Map** and **Neighbor** forms appear.

**Figure 494: Route Map Form**

1. In List 2. Out List

Neighbor

Neighbor Autonomous System ID \*

1

<unsignedint, 1 .. 65535>

Ebgp-multihop

2

---

Maximum Prefix

3

---

Next-hop-self

4

☒

Enabled

Password

5

---

Update-source

6

---

Soft-reconfiguration

7

☒

Enabled

Weight

8

---

**Figure 495: Neighbor Form**

1. Neighbor Autonomous System ID Box    2. eBGP Multi-Hop Box    3. Maximum Prefix Box    4. Next Hop Self Check Box  
5. Password Box    6. Update Source Box    7. Soft Reconfiguration Check Box    8. Weight Box

5. On the **Route Map** form, configure the following parameter(s) as required:

Parameter	Description
in	Apply route map to incoming routes.
out	Apply route map to outbound routes.

6. On the **Neighbor** form, configure the following parameter(s) as required:

Parameter	Description
Neighbor Autonomous System ID	<b>Synopsis:</b> An integer between 1 and 65535 A BGP neighbor.
ebgp-multihop	<b>Synopsis:</b> An integer between 1 and 255 The maximum hop count. This allows EBGp neighbors not on directly connected networks.
Maximum Prefix	<b>Synopsis:</b> An integer between 1 and 4294967295

Parameter	Description
	The maximum prefix number accepted from this peer.
next-hop-self	<b>Synopsis:</b> typeless Disables the next hop calculation for this neighbor.
password	<b>Synopsis:</b> A string 1 to 1024 characters long Password.
update-source	<b>Synopsis:</b> A string 7 to 15 characters long Source IP address of routing updates.
disable-connected-check	<b>Synopsis:</b> typeless Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
soft-reconfiguration	<b>Synopsis:</b> typeless Per neighbor soft reconfiguration.
weight	The default weight for routes from this neighbor.

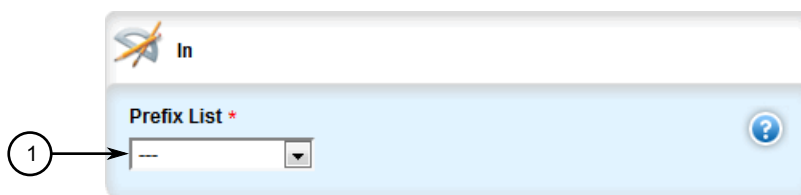
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.18.7.3

### Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in a BGP network, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Make sure the desired prefix list is configured for the BGP network. For more information, refer to [Section 5.18.5.3, "Adding a Prefix List"](#).
- Navigate to **routing » dynamic » bgp » neighbor » {address} » distribute-prefix-list**, where {address} is the IP address of the neighbor.
- Click the **+** symbol in the menu next to either **in** or **out**, depending on the direction of the route (incoming or outbound). The **In** or **Out** form appears.



**Figure 496: In Form (Example)**

1. Prefix List

- Select the desired prefix list.



6. If necessary, configure an event tracker to track network commands. For more information, refer to [Section 5.18.7.4, “Tracking Commands for BGP Neighbors”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

## Section 5.18.7.4

## 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 3.17, “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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » neighbor » {address} » distribute-prefix-list » in|out**, where **{address}** is the IP subnet address and prefix for the neighbor.
3. Click the **+** symbol in the menu next to **track**. The **Track** form appears

The screenshot shows a 'Track' form with two dropdown menus. The first dropdown, labeled 'Event \*', has a callout '1' pointing to it. The second dropdown, labeled 'Apply When \*', has 'up' selected and '(up)' below it, with a callout '2' pointing to it. Both dropdowns have a question mark icon to their right.

**Figure 497: Track Form**

1. Event List    2. Apply When List

4. Configure the following parameter(s) as required:

**NOTE**

For information about creating event trackers, refer to [Section 3.17.3, “Adding an Event Tracker”](#).

Parameter	Description
Event	Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state.
Apply When	<b>Synopsis:</b> { up, down } <b>Default:</b> up

Parameter	Description
	Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

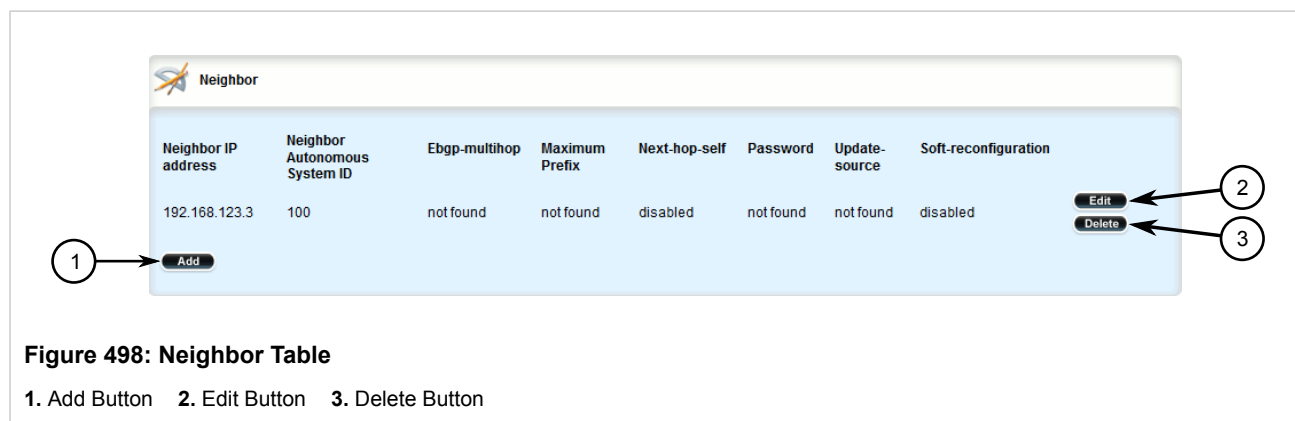
- Click **Add** to create the tracker.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.18.7.5

### Deleting a Neighbor

To delete a neighbor from a BGP network, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » bgp » neighbor**. The **Neighbor** table appears.



- Click **Delete** next to the chosen neighbor.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.18.8

### Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.



#### NOTE

For point-to-point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to [Section 5.18.7.2, "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 5.18.7, “Managing Neighbors”](#).

The following sections describe how to configure and manage networks:

- [Section 5.18.8.1, “Viewing a List of Networks”](#)
- [Section 5.18.8.2, “Adding a Network”](#)
- [Section 5.18.8.3, “Tracking Commands for a BGP Network”](#)
- [Section 5.18.8.4, “Deleting a Network”](#)

#### Section 5.18.8.1

### Viewing a List of Networks

To view a list of networks configured for the BGP protocol, navigate to **routing » dynamic » bgp » network**. If networks have been configured, the **BGP Network** table appears.

Subnet Address/Prefix
192.168.12.0/24
192.168.123.0/24

**Figure 499: BGP Network Table**

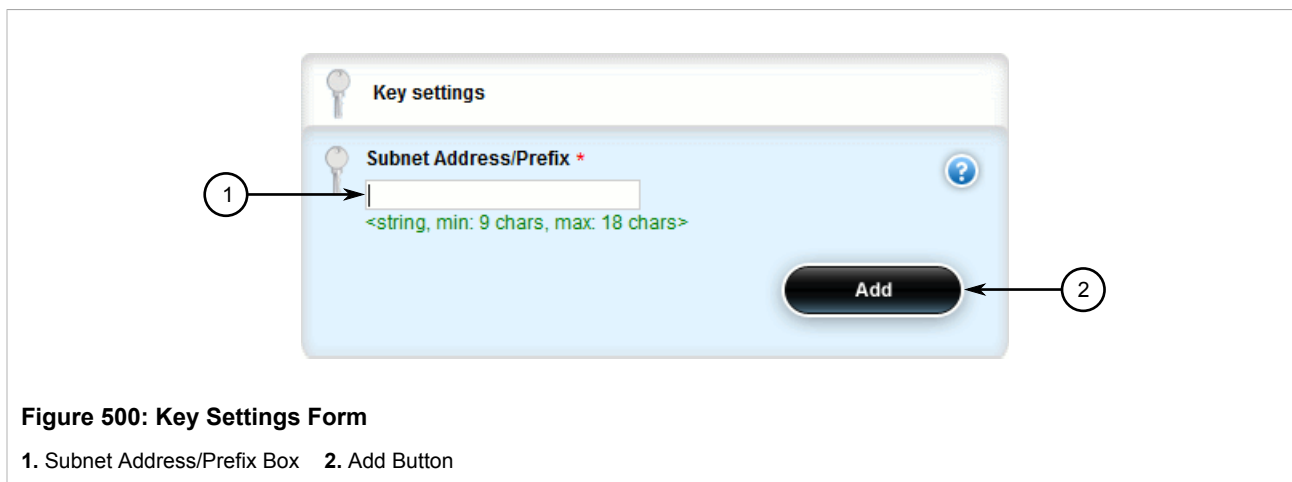
If no networks have been configured, add networks as needed. For more information, refer to [Section 5.18.8.2, “Adding a Network”](#).

#### Section 5.18.8.2

### Adding a Network

To add a network for the BGP protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » network** and click **<Add option82>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address/Prefix	<b>Synopsis:</b> A string 9 to 18 characters long IP address/prefix.

4. Click **Add** to create the network.
5. If necessary, configure an event tracker to track network commands. For more information, refer to [Section 5.18.8.3, "Tracking Commands for a BGP Network"](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.18.8.3

### 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 3.17, "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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » network » {address}**, where {address} is the IP subnet address and prefix for the network.
3. Click the **+** symbol in the menu next to **track**. The **Track** form appears

**Figure 501: Track Form**

1. Event List    2. Apply When List

4. Configure the following parameter(s) as required:



**NOTE**

For information about creating event trackers, refer to [Section 3.17.3, “Adding an Event Tracker”](#).

Parameter	Description
Event	Select an event.
Apply When	<p><b>Synopsis:</b> { up, down }</p> <p><b>Default:</b> up</p> <p>Advertises the network when the tracked event state goes UP or stops advertising the network when the tracked event goes DOWN.</p>

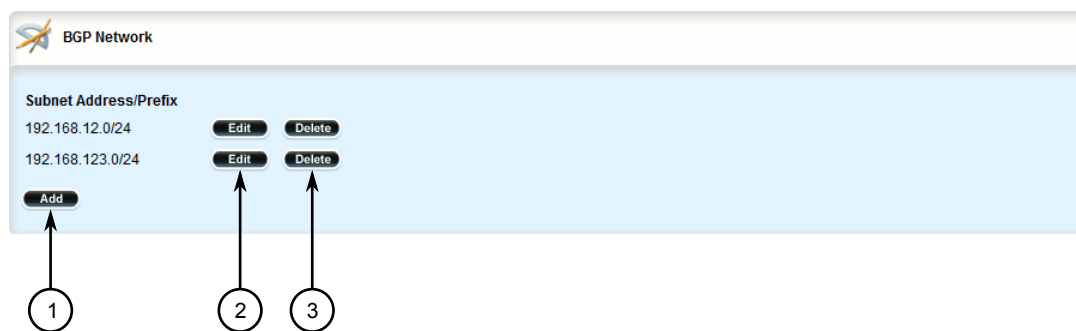
5. Click **Add** to create the tracker.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.18.8.4

### Deleting a Network

To delete a network configured for the BGP protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » network**. The **BGP Network** table appears.



**Figure 502: BGP Network Table**

1. Add Button   2. Edit Button   3. Delete Button

3. Click **Delete** next to the chosen network.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.9

## Managing Aggregate Addresses

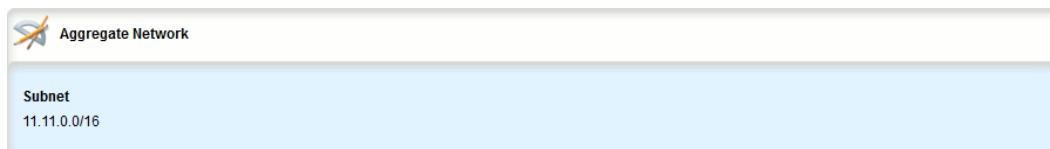
The following sections describe how to configure and manage aggregate addresses:

- [Section 5.18.9.1, “Viewing a List of Aggregate Addresses”](#)
- [Section 5.18.9.2, “Adding an Aggregate Address”](#)
- [Section 5.18.9.3, “Deleting an Aggregate Address”](#)

#### Section 5.18.9.1

### Viewing a List of Aggregate Addresses

To view a list of aggregate addresses for dynamic BGP routes, navigate to **routing » dynamic » bgp » aggregate-address**. If addresses have been configured, the **Aggregate Network** table appears.



**Figure 503: Aggregate Network Table**

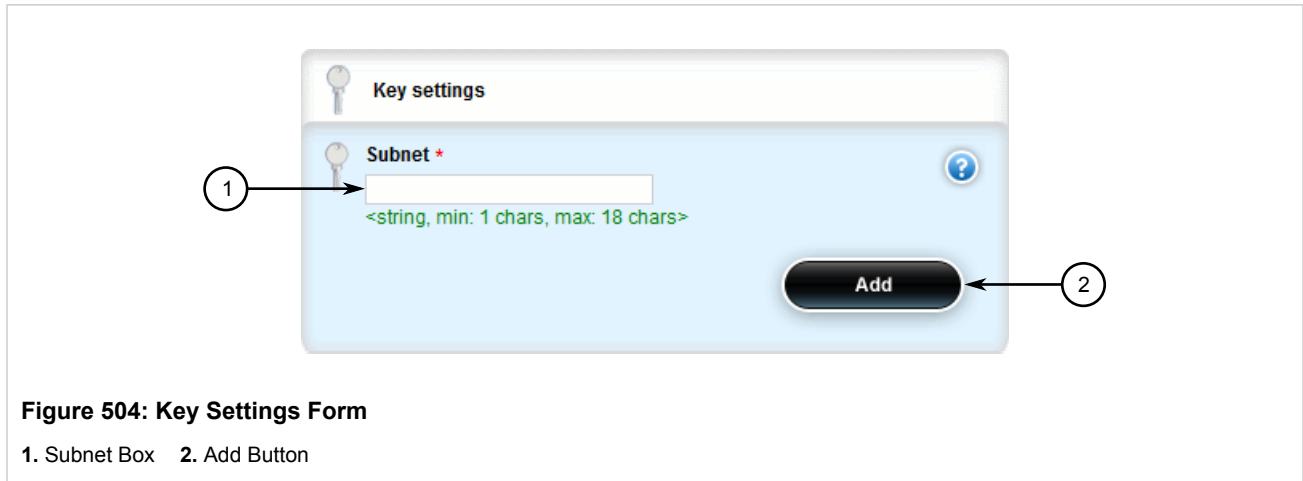
If no aggregate addresses have been configured, add addresses as needed. For more information, refer to [Section 5.18.9.2, “Adding an Aggregate Address”](#).

## Section 5.18.9.2

## Adding an Aggregate Address

To add an aggregate address for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » aggregate-address** and click **<Add aggregate-address>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
subnet	<b>Synopsis:</b> A string 9 to 18 characters long subnet (xxx.xxx.xxx.xxx/xx).

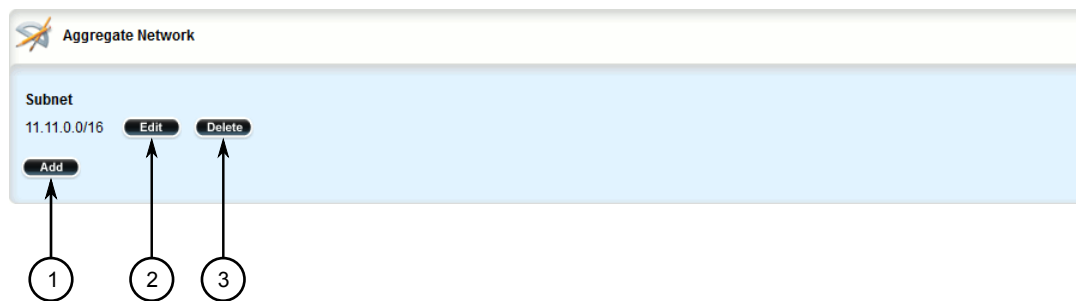
4. Click **Add** to add the address.
5. If necessary, configure options for the address. For more information, refer to [Section 5.18.10.2, “Adding an Aggregate Address Option”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 5.18.9.3

## Deleting an Aggregate Address

To delete an aggregate address for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » aggregate-address**. The **Aggregate Network** table appears.



**Figure 505: Aggregate Network Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.18.10

## Managing Aggregate Address Options

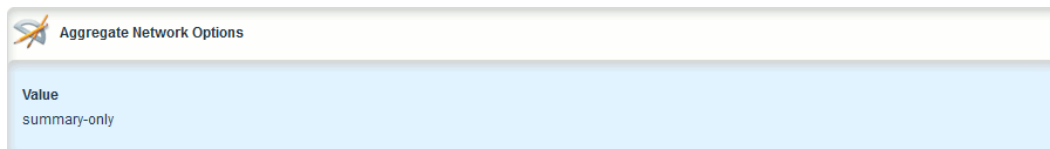
The following sections describe how to configure and manage options for aggregate addresses:

- [Section 5.18.10.1, “Viewing a List of Aggregate Address Options”](#)
- [Section 5.18.10.2, “Adding an Aggregate Address Option”](#)
- [Section 5.18.10.3, “Deleting an Aggregate Address Option”](#)

#### Section 5.18.10.1

### Viewing a List of Aggregate Address Options

To view a list of options for an aggregate address, navigate to **routing » dynamic » bgp » aggregate-address » {address} » options**, where **{address}** is the subnet address and prefix for the aggregate address. If options have been configured, the **Aggregate Network Options** table appears.



**Figure 506: Aggregate Network Options Table**

If no options have been configured, add options as needed. For more information, refer to [Section 5.18.10.2, “Adding an Aggregate Address Option”](#).

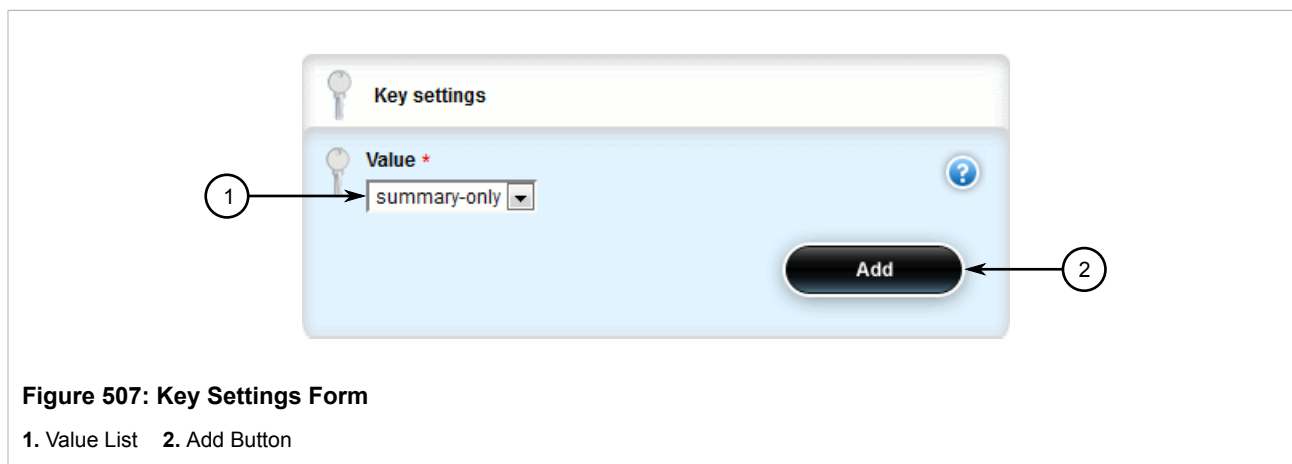


## Section 5.18.10.2

## Adding an Aggregate Address Option

To add an option for an aggregate address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » aggregate-address » {address} » options**, where {address} is the subnet address and prefix for the aggregate address.
3. Click **<Add options>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
value	<b>Synopsis:</b> { as-set, summary-only } Aggregate address option.

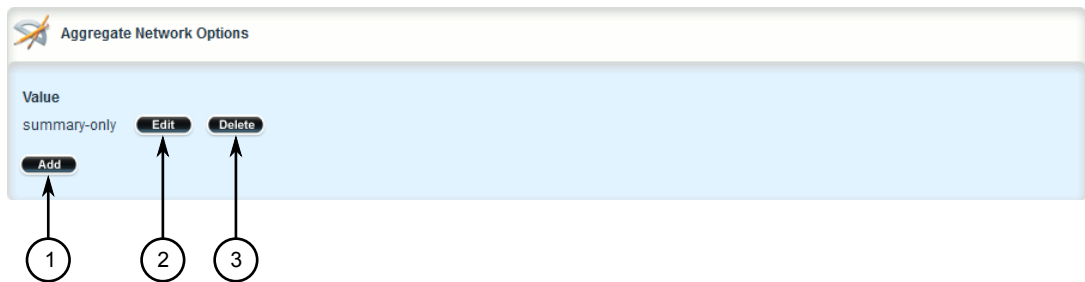
5. Click **Add** to add the option.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 5.18.10.3

## Deleting an Aggregate Address Option

To delete an option for an aggregate address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » aggregate-address » {address} » options**, where {address} is the subnet address and prefix for the aggregate address. The **Aggregate Network Options** table appears.



**Figure 508: Aggregate Network Options Table**

1. Add Button   2. Edit Button   3. Delete Button

3. Click **Delete** next to the chosen option.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.18.11

## 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.

The following sections describe how to configure and manage redistribution metrics for BGP:

- [Section 5.18.11.1, “Viewing a List of Redistribution Metrics”](#)
- [Section 5.18.11.2, “Adding a Redistribution Metric”](#)
- [Section 5.18.11.3, “Deleting a Redistribution Metric”](#)

Section 5.18.11.1

### Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic BGP routes, navigate to **routing » dynamic » bgp » redistribute**. If metrics have been configured, the **Redistribute Route from Other Protocols** table appears.

Redistribute Route From	Metric
rip	not found

**Figure 509: Redistribute Route from Other Protocols Table**

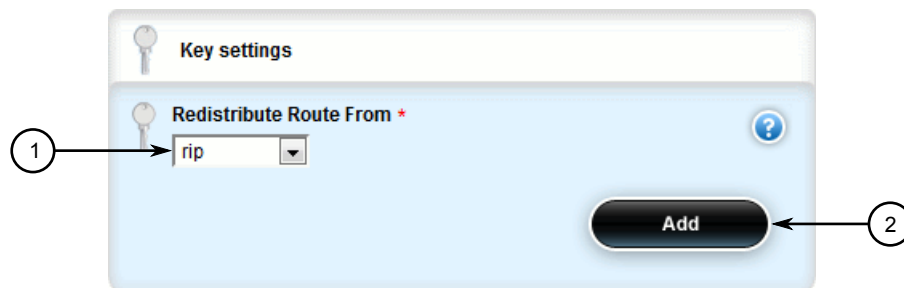
If no redistribution metrics have been configured, add metrics as needed. For more information, refer to [Section 5.18.11.2, “Adding a Redistribution Metric”](#).

Section 5.18.11.2

## Adding a Redistribution Metric

To add a redistribution metric for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » redistribute** and click **<Add redistribute>**. The **Key Settings** form appears.



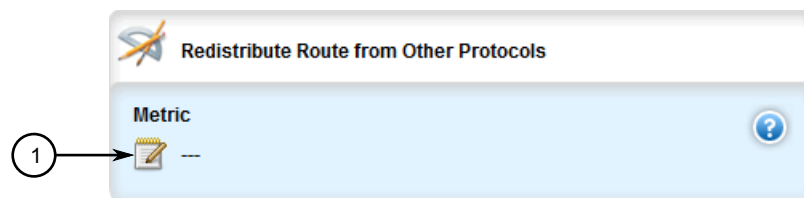
**Figure 510: Key Settings Form**

1. Redistribute Route From List 2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Route From	<b>Synopsis:</b> { kernel, static, connected, ospf, rip } Redistribute route type.

4. Click **Add** to add the metric. The **Redistribute Route From Other Protocols** form appears.



**Figure 511: Redistribute Route From Other Protocols Form**

1. Metric Box

5. Configure the following parameter(s) as required:

Parameter	Description
Metric	Metric value for redistributed routes.

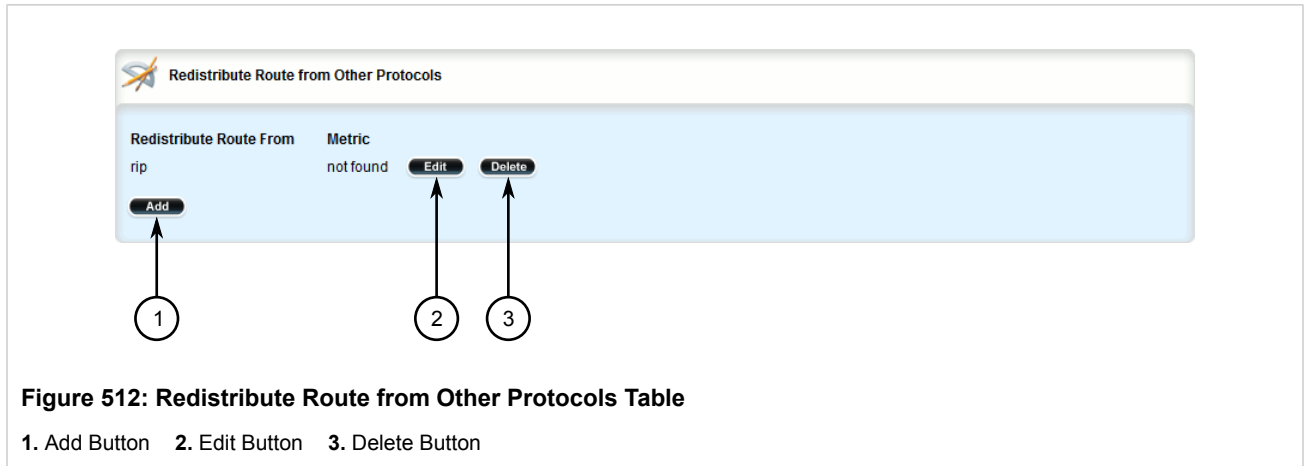
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.18.11.3

## Deleting a Redistribution Metric

To delete a redistribution metric for dynamic BGP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » redistribute**. The **Redistribute Route from Other Protocols** table appears.



3. Click **Delete** next to the chosen metric.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.19

## Managing RIP

The Routing Information Protocol (RIP) determines the best path for routing IP traffic over a TCP/IP network based on the number of hops between any two routers. It uses the shortest route available to a given network as the route to use for sending packets to that network.

The RUGGEDCOM ROX II RIP daemon is an [RFC 1058](http://tools.ietf.org/rfc/rfc1058.txt) [http://tools.ietf.org/rfc/rfc1058.txt] compliant implementation of RIP that supports RIP version 1 and 2. RIP version 1 is limited to obsolete class-based networks, while RIP version 2 supports subnet masks, as well as simple authentication for controlling which routers to accept route exchanges with.

RIP uses network and neighbor entries to control which routers it will exchange routes with. A network is either a subnet or a physical (broadcast-capable) network interface. Any router that is part of that subnet or connected to that interface may exchange routes. A neighbor is a specific router, specified by its IP address, to exchange routes with. For point to point links (i.e. T1/E1 links), neighbor entries must be used to add other routers to exchange routes with. The maximum number of hops between two points on a RIP network is 15, placing a limit on network size.

Link failures will eventually be noticed when using RIP, although it is not unusual for RIP to take many minutes for a dead route to disappear from the whole network. Large RIP networks could take over an hour to converge when link or route changes occur. For fast convergence and recovery, OSPF is recommended. For more information about OSPF, refer to [Section 5.20, "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.*

The following sections describe how to configure and manage RIP:

- [Section 5.19.1, “Configuring RIP”](#)
- [Section 5.19.2, “Viewing the Status of Dynamic RIP Routes”](#)
- [Section 5.19.3, “Managing Prefix Lists and Entries”](#)
- [Section 5.19.4, “Managing Networks”](#)
- [Section 5.19.5, “Managing Network IP Address”](#)
- [Section 5.19.6, “Managing Network Interfaces”](#)
- [Section 5.19.7, “Managing Neighbors”](#)
- [Section 5.19.8, “Managing the Prefix List Distribution”](#)
- [Section 5.19.9, “Managing Key Chains and Keys”](#)
- [Section 5.19.10, “Managing Redistribution Metrics”](#)
- [Section 5.19.11, “Managing Routing Interfaces”](#)

#### Section 5.19.1

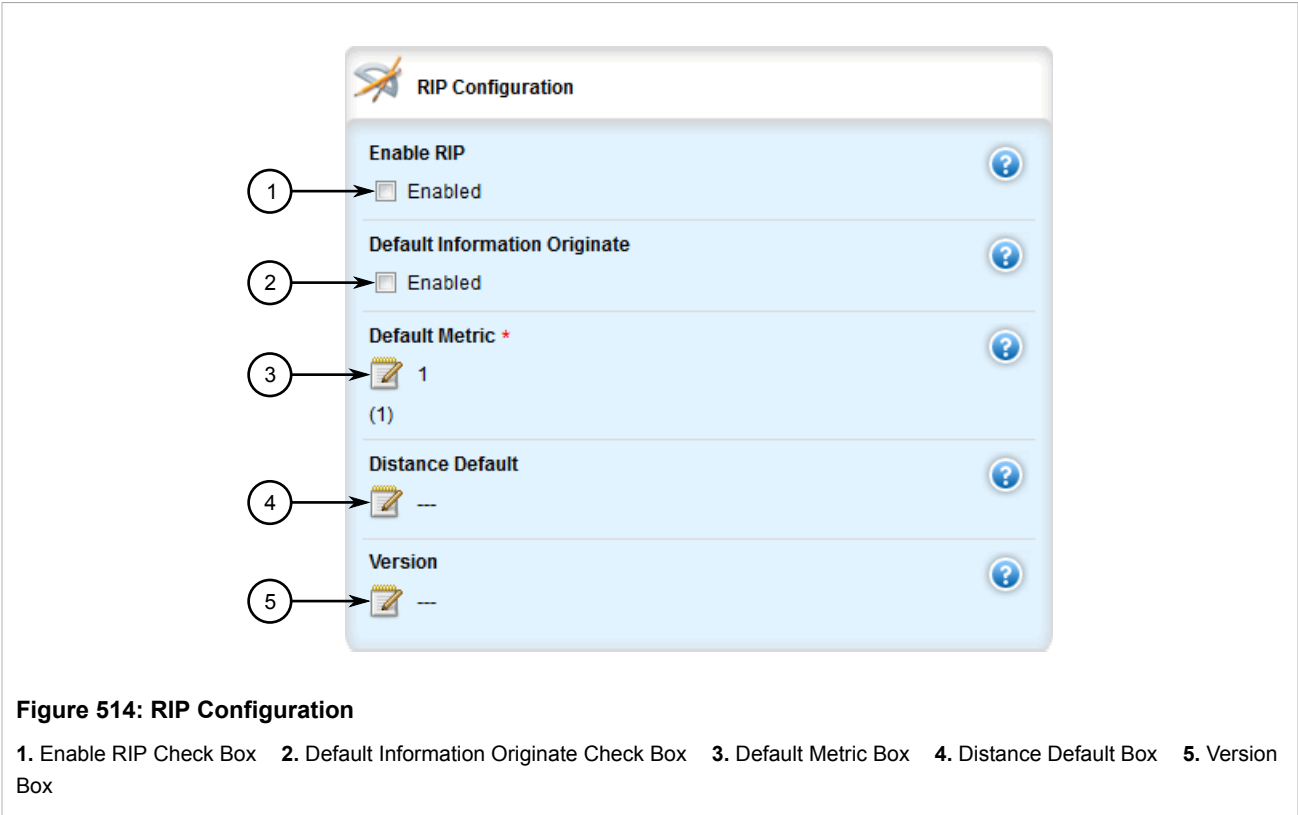
## Configuring RIP

To configure dynamic routing using the Routing Information Protocol (RIP) daemon, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip**. The **Routing Timers** and **RIP Configuration** forms appear.

**Figure 513: Routing Timers Form**

1. Update Timer Box    2. Timeout Timer Box    3. Garbage Collection Timer Box



3. In the **Routing Timers** form, configure the following parameters:

Parameter	Description
Update Timer	<b>Synopsis:</b> An integer between 5 and 2147483647 <b>Default:</b> 30 The routing table update timer (in seconds).
Timeout Timer	<b>Synopsis:</b> An integer between 5 and 2147483647 <b>Default:</b> 180 The routing information timeout timer (in seconds).
Garbage Collection Timer	<b>Synopsis:</b> An integer between 5 and 2147483647 <b>Default:</b> 120 The garbage collection timer (in seconds).

4. In the **RIP Configuration** form, configure the following parameters:

Parameter	Description
Enable RIP	<b>Synopsis:</b> typeless Enables the RIP dynamic routing protocol.
Default Information Originate	<b>Synopsis:</b> typeless The route element makes a static route only inside RIP. This element should be used only by advanced users who are particularly knowledgeable about the RIP protocol. In most cases, we recommend creating a static route and redistributing it in RIP using the redistribute element with static type.
Default Metric	<b>Synopsis:</b> An integer between 1 and 16

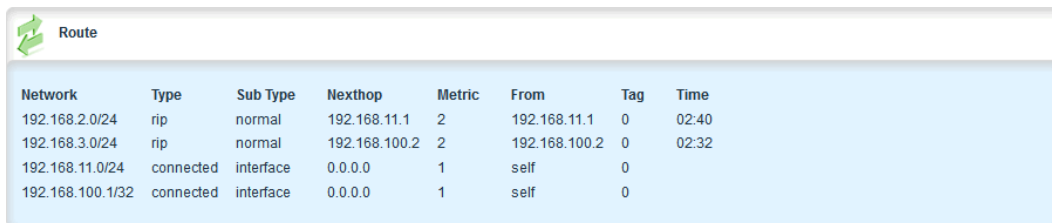
Parameter	Description
	<b>Default:</b> 1 Sets the default metric. With the exception of connected route types, the default metric is advertised when a metric has not been configured for a redistributed route. For connected route types, the default metric is 1 despite the value of this parameter.
Distance Default	<b>Synopsis:</b> An integer between 1 and 255 Sets the default RIP distance.
Version	<b>Synopsis:</b> An integer between 1 and 2 Set the RIP version to accept for reads and send. The version can be either 1 or 2. Disabling RIPv1 by specifying version 2 is STRONGLY encouraged.

5. Configure prefix lists. For more information, refer to [Section 5.19.3.3, “Adding a Prefix List”](#).
6. Configure a network. For more information, refer to [Section 5.19.4.1, “Configuring a Network”](#).
7. Configure the prefix list distribution. For more information, refer to [Section 5.19.8.2, “Adding a Prefix List Distribution Path”](#).
8. Configure key chains. For more information, refer to [Section 5.19.9.3, “Adding a Key Chain”](#).
9. Configure redistribution metrics. For more information, refer to [Section 5.19.10.2, “Adding a Redistribution Metric”](#).
10. Configure interfaces. For more information, refer to [Section 5.19.11.2, “Configuring a Routing Interface”](#).
11. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
12. Click **Exit Transaction** or continue making changes.

## Section 5.19.2

## Viewing the Status of Dynamic RIP Routes

To view the status of the dynamic RIP routes configured on the device, navigate to **routing » status » rip » route**. If RIP routes have been configured, the **Route** table appears.



Network	Type	Sub Type	Nexthop	Metric	From	Tag	Time
192.168.2.0/24	rip	normal	192.168.11.1	2	192.168.11.1	0	02:40
192.168.3.0/24	rip	normal	192.168.100.2	2	192.168.100.2	0	02:32
192.168.11.0/24	connected	interface	0.0.0.0	1	self	0	
192.168.100.1/32	connected	interface	0.0.0.0	1	self	0	

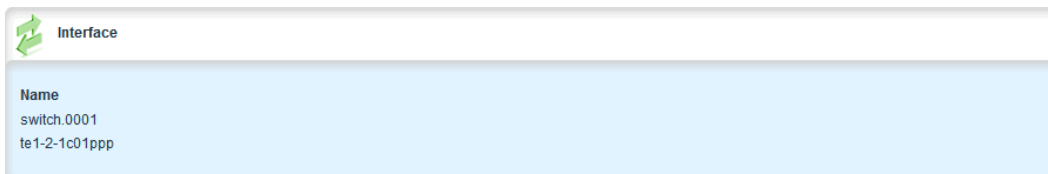
Figure 515: Route Table

The **Route** table provides the following information:

Parameter	Description
Network	<b>Synopsis:</b> A string

Parameter	Description
	The network.
Type	<b>Synopsis:</b> A string The route type.
Sub Type	<b>Synopsis:</b> A string The route sub type.
Nexthop	<b>Synopsis:</b> A string The next hop.
Metric	The metric value.
From	<b>Synopsis:</b> A string Where this route comes from.
Tag	<b>Synopsis:</b> A string Tag.
Time	<b>Synopsis:</b> A string The route update time.

To view the name of the interface associated with the route, navigate to **routing » status » rip » interface**. The **Interface** table appears.



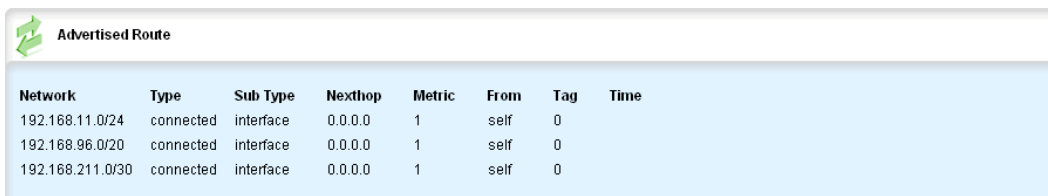
Interface
Name switch.0001 te1-2-1c01ppp

Figure 516: Interface Table

The **Interface** table provides the following information:

Parameter	Description
Name	<b>Synopsis:</b> A string The name of the interface.

To view the routing information advertised to the network, navigate to **routing » status » rip » route**. The **Advertised Route** table appears.



Network	Type	Sub Type	Nexthop	Metric	From	Tag	Time
192.168.11.0/24	connected	interface	0.0.0.0	1	self	0	
192.168.96.0/20	connected	interface	0.0.0.0	1	self	0	
192.168.211.0/30	connected	interface	0.0.0.0	1	self	0	

Figure 517: Advertised Route Table

The **Advertised Route** table provides the following information:



Parameter	Description
Network	<b>Synopsis:</b> A string The network.
Type	<b>Synopsis:</b> A string The route type.
Sub Type	<b>Synopsis:</b> A string The route sub type.
Nexthop	<b>Synopsis:</b> A string Next hop.
Metric	The metric value.
From	<b>Synopsis:</b> A string Where this route comes from.
Tag	<b>Synopsis:</b> A string Tag.
Time	<b>Synopsis:</b> A string The route update time.

If no dynamic RIP routes have been configured, configure RIP and add routes as needed. For more information about configuring RIP, refer to [Section 5.19.1, “Configuring RIP”](#).

### Section 5.19.3

## 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.


The following sections describe how to configure and manage prefix lists and entries for dynamic RIP routes:

- [Section 5.19.3.1, “Viewing a List of Prefix Lists”](#)
- [Section 5.19.3.2, “Viewing a List of Prefix Entries”](#)
- [Section 5.19.3.3, “Adding a Prefix List”](#)
- [Section 5.19.3.4, “Adding a Prefix Entry”](#)
- [Section 5.19.3.5, “Deleting a Prefix List”](#)
- [Section 5.19.3.6, “Deleting a Prefix Entry”](#)

### Section 5.19.3.1

## Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic RIP routes, navigate to one ***routing » dynamic » rip » filter***. If prefix lists have been configured, the **Prefix List** table appears.



The image shows a screenshot of a web interface titled "Prefix List". It contains a table with two columns: "Name" and "Description". The table lists two entries: "list-permit-lan-22" and "list-withdraw-lan-11", both with a description of "not found".

Name	Description
list-permit-lan-22	not found
list-withdraw-lan-11	not found

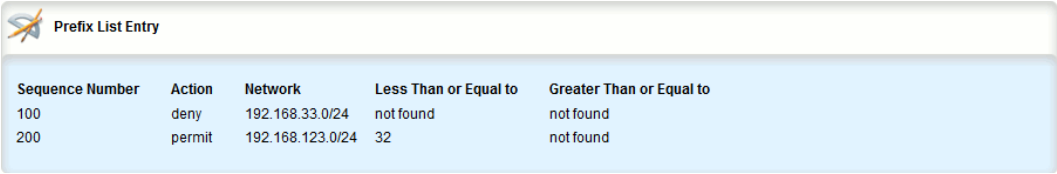
Figure 518: Prefix List Table

If no prefix lists have been configured, add lists as needed. For more information, refer to [Section 5.19.3.3](#), “Adding a Prefix List”.

Section 5.19.3.2

Viewing a List of Prefix Entries

To view a list of entries for dynamic RIP prefix lists, navigate to *routing » dynamic » rip » filter » {name} » entry*, where {name} is the name of the prefix list. If entries have been configured, the **Prefix List Entry** table appears.



The image shows a screenshot of a web interface titled "Prefix List Entry". It contains a table with five columns: "Sequence Number", "Action", "Network", "Less Than or Equal to", and "Greater Than or Equal to". The table lists two entries: "100" and "200".

Sequence Number	Action	Network	Less Than or Equal to	Greater Than or Equal to
100	deny	192.168.33.0/24	not found	not found
200	permit	192.168.123.0/24	32	not found

Figure 519: Prefix List Entry Table

If no entries have been configured, add entries as needed. For more information, refer to [Section 5.19.3.4](#), “Adding a Prefix Entry”.

Section 5.19.3.3

Adding a Prefix List

To add a prefix list for dynamic RIP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *routing » dynamic » rip » filter* and click **<Add prefix-list>**. The **Key Settings** form appears.

A screenshot of a web form titled "Key settings" with a key icon. Below the title is a "Name \*" field with a key icon and a blue question mark icon. The field contains the text "<string, min: 1 chars>". A circled number "1" with an arrow points to the text input area. To the right of the field is a dark "Add" button. A circled number "2" with an arrow points to the "Add" button.

Figure 520: Key Settings Form

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 1024 characters long The name of the prefix list.

4. Click **Add** to create the new prefix-list. The **Prefix List** form appears.

A screenshot of a web form titled "Prefix List" with a pencil icon. Below the title is a "Description" field with a notepad icon and a blue question mark icon. The field contains a dashed line "--". A circled number "1" with an arrow points to the text input area.

Figure 521: Prefix List Form

1. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string 1 to 1024 characters long The description of the prefix list.

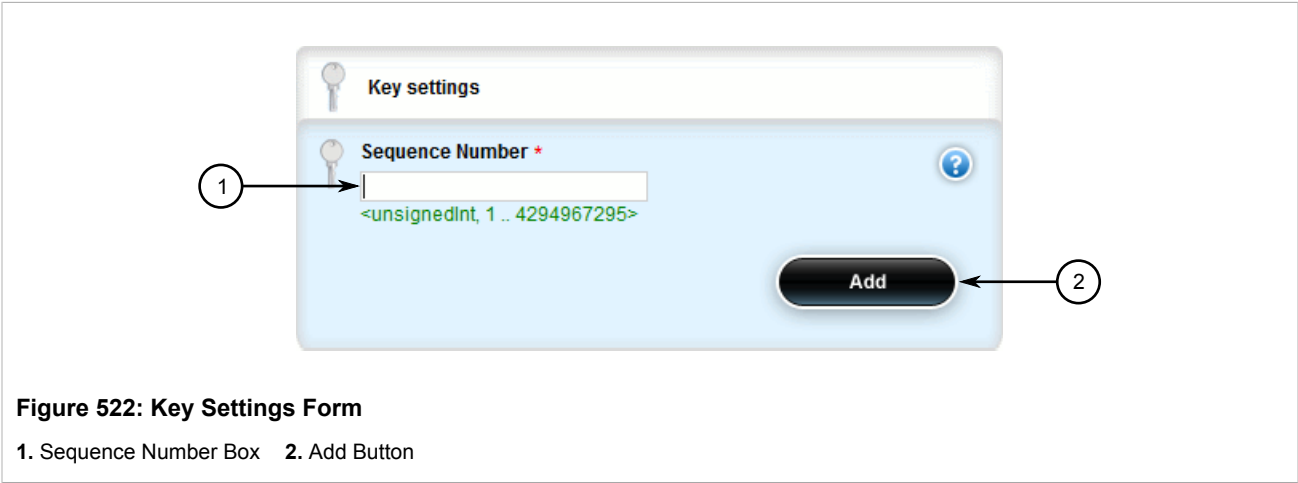
6. Add prefix entries as needed. For more information, refer to [Section 5.19.3.4, “Adding a Prefix Entry”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 5.19.3.4

# Adding a Prefix Entry

To add an entry for a dynamic RIP prefix list, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Depending on the dynamic routing protocol being configured, navigate to *routing » dynamic » rip » filter » {name} » entry*, where {name} is the name of the prefix list.
3. Click **<Add entry>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 4294967295 The sequence number of the entry.

5. Click **Add** to create the new entry. The **Prefix List Entry** form appears.

**Figure 523: Prefix List Entry Form**

1. ActionList   2. Network Box   3. Maximum Prefix to Mask for Subnet   4. Minimum Prefix to Mask for Subnet

6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { deny, permit } <b>Default:</b> permit The action that will be performed.
Network	<b>Synopsis:</b> A string 9 to 18 characters long The IPv4 network address and prefix.
Less Than or Equal to	<b>Synopsis:</b> An integer between 1 and 32 The maximum prefix length to be matched.
Greater Than or Equal to	<b>Synopsis:</b> An integer between 1 and 32 The minimum prefix length to be matched.

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.19.3.5

### Deleting a Prefix List

To delete a prefix list for dynamic RIP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » filter**. The **Prefix List** table appears.

Name	Description		
list-permit-lan-22	not found	Edit	Delete
list-withdraw-lan-11	not found	Edit	Delete

Add

1. Add Button 2. Edit Button 3. Delete Button

**Figure 524: Prefix List Table**

1. Add Button 2. Edit Button 3. Delete Button



#### NOTE

*Deleting a prefix list removes all associate prefix entries as well.*

- Click **Delete** next to the chosen prefix list.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.19.3.6

### Deleting a Prefix Entry

To delete an entry for a dynamic RIP prefix list, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Depending on the dynamic routing protocol being configured, navigate to **routing » dynamic » rip » filter » {name} » entry**, where {name} is the name of the prefix list. The **Prefix List Entry** table appears.

Sequence Number	Action	Network	Less Than or Equal to	Greater Than or Equal to		
100	deny	192.168.33.0/24	not found	not found	Edit	Delete
200	permit	192.168.123.0/24	32	not found	Edit	Delete

Add

1. Add Button 2. Edit Button 3. Delete Button

**Figure 525: Prefix List Entry Table**

1. Add Button 2. Edit Button 3. Delete Button

- Click **Delete** next to the chosen entry.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.19.4

## Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

**NOTE**

*For point to point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to [Section 5.19.7.2, "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 5.19.7, "Managing Neighbors"](#).*

The following sections describe how to configure and manage networks:

- [Section 5.19.4.1, "Configuring a Network"](#)
- [Section 5.19.4.2, "Tracking Commands"](#)

## Section 5.19.4.1

### Configuring a Network

To configure a network for the RIP protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Add one or more network IP addresses. For more information, refer to [Section 5.19.5.2, "Adding a Network IP Address"](#).
3. Add one or more network interfaces. For more information, refer to [Section 5.19.6.2, "Adding a Network Interface"](#).
4. Add one or more neighbors. For more information, refer to [Section 5.19.7.2, "Adding a Neighbor"](#).

## Section 5.19.4.2

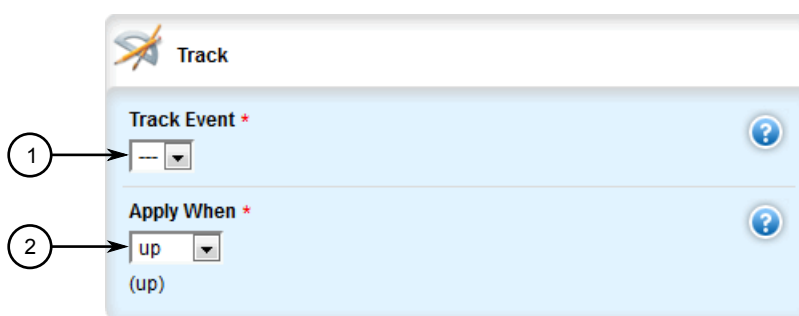
### Tracking Commands

Network commands can be tracked using event trackers configured under **global » tracking**. For more information about event trackers, refer to [Section 3.17, "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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure a prefix list distribution path has been configured. For more information, refer to [Section 5.19.8, "Managing the Prefix List Distribution"](#).
3. Navigate to **routing » dynamic » rip » distribute-prefix-list » {direction} » {interface}**, where: *{direction}* is the direction (incoming or outgoing) in which to filter routing updates and *{interface}* is the name of the interface.
4. Click the **+** symbol in the menu next to **track**. The **Track** form appears



**Figure 526: Track Form**

1. Track Event List   2. Apply When List

5. Configure the following parameter(s) as required:

Parameter	Description
Track Event	Selects an event to track. The distribute-prefix-list is applied only when the tracked event is in the UP state.
Apply When	<b>Synopsis:</b> { up, down } <b>Default:</b> up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

6. Click **Add** to create the tracker.
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.19.5

## Managing Network IP Address

The following sections describe how to configure and manage network IP addresses for dynamic RIP routes:

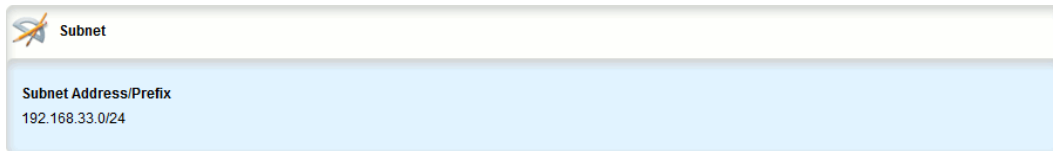


- [Section 5.19.5.1, “Viewing a List of Network IP Addresses”](#)
- [Section 5.19.5.2, “Adding a Network IP Address”](#)
- [Section 5.19.5.3, “Deleting a Network IP Address”](#)

#### Section 5.19.5.1

### Viewing a List of Network IP Addresses

To view a list of IP addresses configured for a RIP network, navigate to **routing » dynamic » rip » network » ip**. If addresses have been configured, the **Subnet** table appears.



Subnet Address/Prefix
192.168.33.0/24

**Figure 527: Subnet Table**

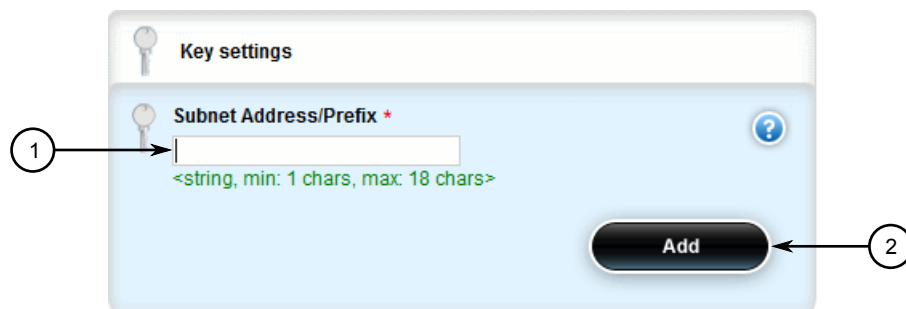
If no IP addresses have been configured, add addresses as needed. For more information, refer to [Section 5.19.5.2, “Adding a Network IP Address”](#).

#### Section 5.19.5.2

### Adding a Network IP Address

To add an IP address for a RIP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » network » ip** and click **<Add ip>**. The **Key Settings** form appears.



**Figure 528: Key Settings Form**

1. Subnet Address/Prefix Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address/Prefix	<b>Synopsis:</b> A string 9 to 18 characters long

Parameter	Description
	The IPv4 network address and prefix.

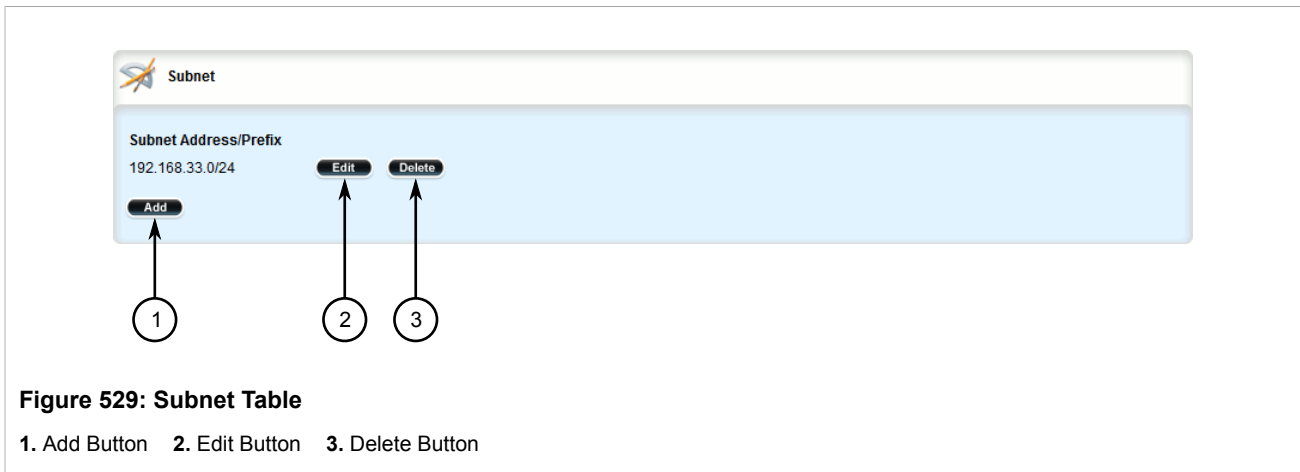
- Click **Add** to add the IP address.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.19.5.3

## Deleting a Network IP Address

To delete an IP address from a RIP network, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » rip » network » ip**. The **Subnet** table appears.



- Click **Delete** next to the chosen IP address.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.19.6

## Managing Network Interfaces


The following sections describe how to configure and manage interfaces for a RIP network:

- [Section 5.19.6.1, “Viewing a List of Network Interfaces”](#)
- [Section 5.19.6.2, “Adding a Network Interface”](#)
- [Section 5.19.6.3, “Deleting a Network Interface”](#)

### Section 5.19.6.1

## Viewing a List of Network Interfaces

To view a list of interfaces configured for a RIP network, navigate to **routing » dynamic » rip » network » interface**. If interfaces have been configured, the **Interface** table appears.



Interface Name
switch.4084

**Figure 530: Interface Table**

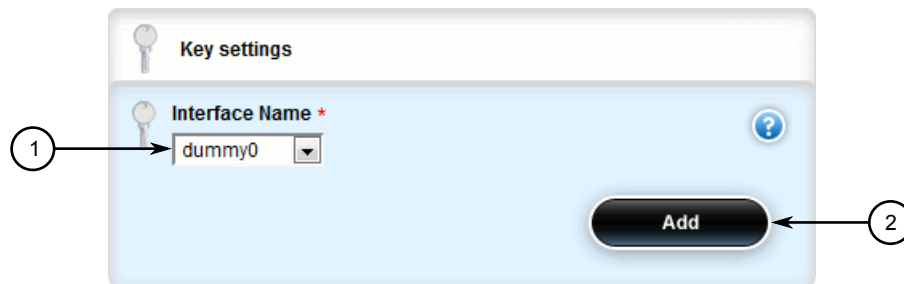
If no interfaces have been configured, add neighbors as needed. For more information, refer to [Section 5.19.7.2, “Adding a Neighbor”](#).

### Section 5.19.6.2

## Adding a Network Interface

To add an interface for a RIP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » network » interface** and click **<Add interface>**. The **Key Settings** form appears.



**Figure 531: Key Settings Form**

1. Interface Name List    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	Interface name.

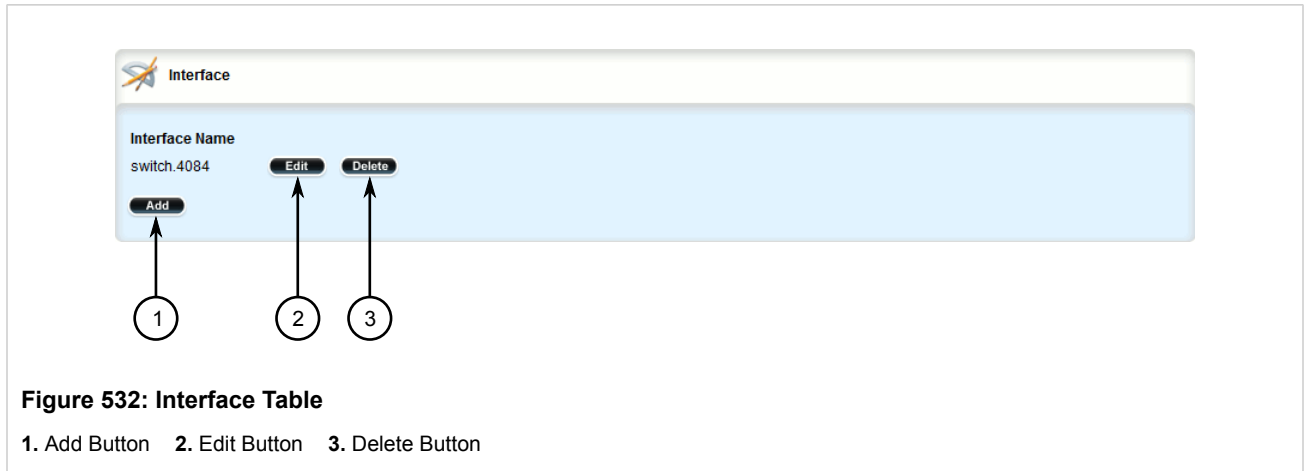
4. Click **Add** to add the interface.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.19.6.3

## Deleting a Network Interface

To delete an interface from a RIP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » network » interface**. The **Interface** table appears.



3. Click **Delete** next to the chosen interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.19.7

## Managing Neighbors

Neighbors are other routers with which to exchange routes.

The following sections describe how to configure and manage neighbor IP addresses for dynamic RIP routes:

- [Section 5.19.7.1, “Viewing a List of Neighbors”](#)
- [Section 5.19.7.2, “Adding a Neighbor”](#)
- [Section 5.19.7.3, “Deleting a Neighbor”](#)

### Section 5.19.7.1

## Viewing a List of Neighbors

To view a list of neighbors configured for a RIP network, navigate to **routing » dynamic » rip » network » neighbor**. If neighbors have been configured, the **Neighbor** table appears.

Neighbor	
Neighbor IP Address	192.168.33.2

**Figure 533: Neighbor Table**

If no neighbors have been configured, add neighbors as needed. For more information, refer to [Section 5.19.7.2, “Adding a Neighbor”](#).

### Section 5.19.7.2

## Adding a Neighbor

To add a neighbor for a RIP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *routing » dynamic » rip » network » neighbor* and click **<Add neighbor>**. The **Key Settings** form appears.

**Figure 534: Key Settings Form**

1. Neighbor IP Address Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the neighbor.

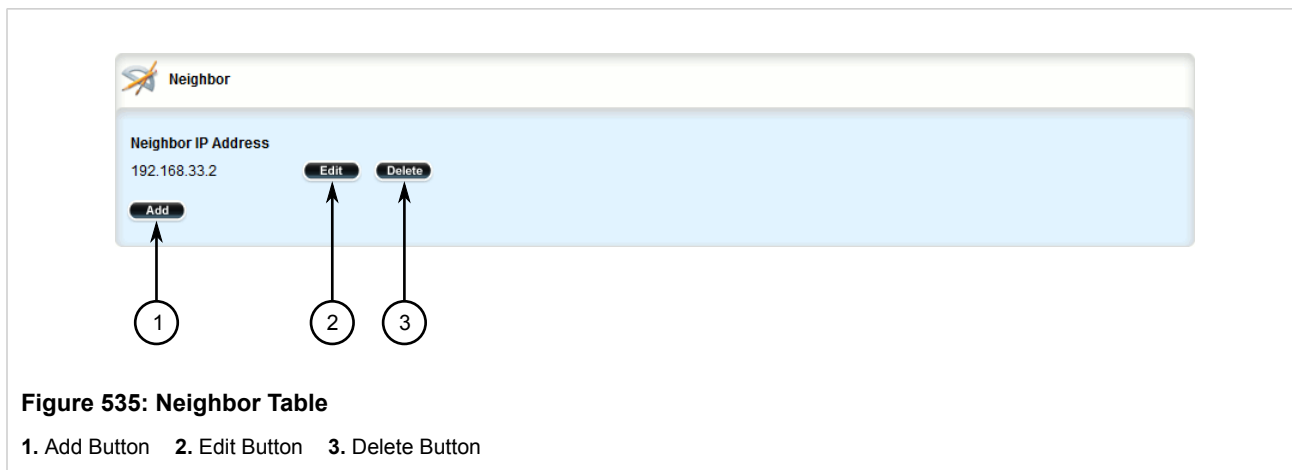
4. Click **Add** to add the address.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.19.7.3

## Deleting a Neighbor

To delete a neighbor from a RIP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » network » neighbor**. The **Neighbor** table appears.



3. Click **Delete** next to the chosen neighbor.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.19.8

## Managing the Prefix List Distribution

The following sections describe how to configure and manage the prefix list distribution:

- [Section 5.19.8.1, “Viewing a List of Prefix List Distribution Paths”](#)
- [Section 5.19.8.2, “Adding a Prefix List Distribution Path”](#)
- [Section 5.19.8.3, “Deleting a Prefix List Distribution Path”](#)

### Section 5.19.8.1

## Viewing a List of Prefix List Distribution Paths

To view a list of prefix list distribution paths for dynamic RIP routes, navigate to **routing » dynamic » rip » distribute-prefix-list**. If distribution paths have been configured, the **Distribute Prefix List** table appears.

Distribute Prefix List		
Direction	Interface Name	Prefix List
out		list-permit-lan-22

Figure 536: Distribute Prefix List Table

If no prefix list distribution paths have been configured, add distribution paths as needed. For more information, refer to [Section 5.19.8.2, “Adding a Prefix List Distribution Path”](#).

Section 5.19.8.2

Adding a Prefix List Distribution Path

To add a prefix list distribution path for dynamic RIP routes, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *routing » dynamic » rip » distribute-prefix-list* and click **<Add distribute-prefix-list>**. The **Key Settings** form appears.

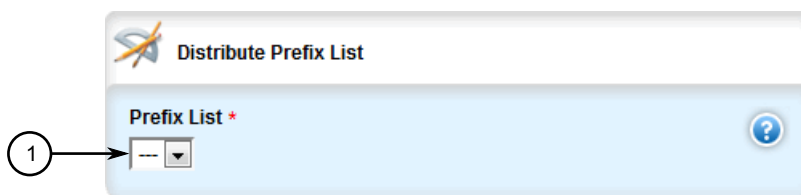
Figure 537: Key Settings Form

1. Direction List    2. Interface Name Box    3. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
Direction	<b>Synopsis:</b> { in, out } Filters incoming or outgoing routing updates.
Interface Name	<b>Synopsis:</b> A string 1 to 15 characters long The name of the interface. This parameter is optional.

- 4. Click **Add** to add the path. The **Distribute Prefix List** form appears.



**Figure 538: Distribute Prefix List Form**

1. Prefix List List

5. Configure the following parameter(s) as required:

Parameter	Description
Prefix List	The name of the prefix list.

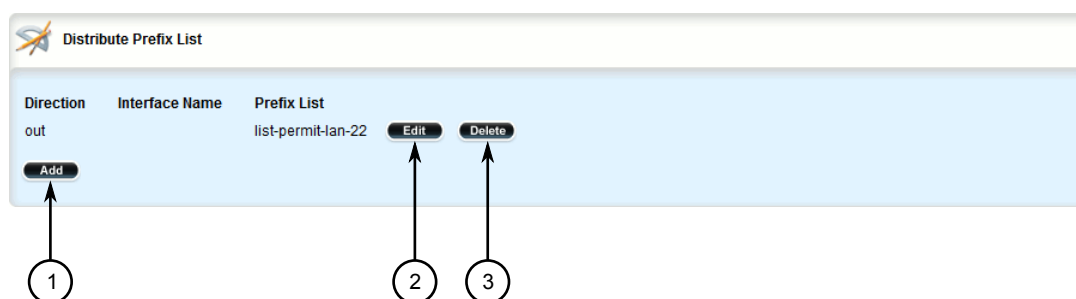
6. If necessary, configure an event tracker to track network commands. For more information, refer to [Section 5.19.4.2, "Tracking Commands"](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.19.8.3

## Deleting a Prefix List Distribution Path

To delete a prefix list distribution path for dynamic RIP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » distribute-prefix-list**. The **Distribute Prefix List** table appears.



**Figure 539: Distribute Prefix List Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen path.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.



Section 5.19.9

# 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.


The following sections describe how to configure and manage key chains and keys:

- [Section 5.19.9.1, “Viewing a List of Key Chains”](#)
- [Section 5.19.9.2, “Viewing a List of Keys”](#)
- [Section 5.19.9.3, “Adding a Key Chain”](#)
- [Section 5.19.9.4, “Adding a Key”](#)
- [Section 5.19.9.5, “Deleting a Key Chain”](#)
- [Section 5.19.9.6, “Deleting a Key”](#)

Section 5.19.9.1

## Viewing a List of Key Chains

To view a list of key chains for dynamic RIP routes, navigate to **routing » dynamic » rip » key-chain**. If key chains have been configured, the **Key Chain Management** table appears.



Key Chain Name
key-1

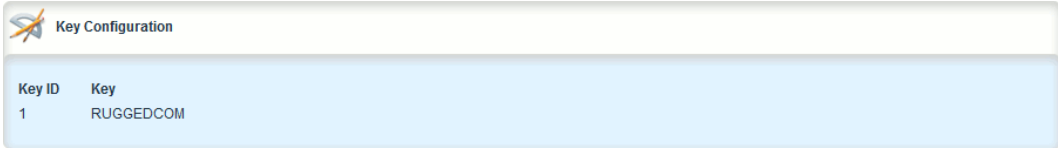
Figure 540: Key Chain Management Table

If no key chains have been configured, add key chains as needed. For more information, refer to [Section 5.19.9.3, “Adding a Key Chain”](#).

Section 5.19.9.2

## Viewing a List of Keys

To view a list of keys in a key chain, navigate to **routing » dynamic » rip » key-chain » {name} » key**, where {name} is the name of the key chain. If keys have been configured, the **Key Configuration** table appears.



Key ID	Key
1	RUGGEDCOM

Figure 541: Key Configuration Table

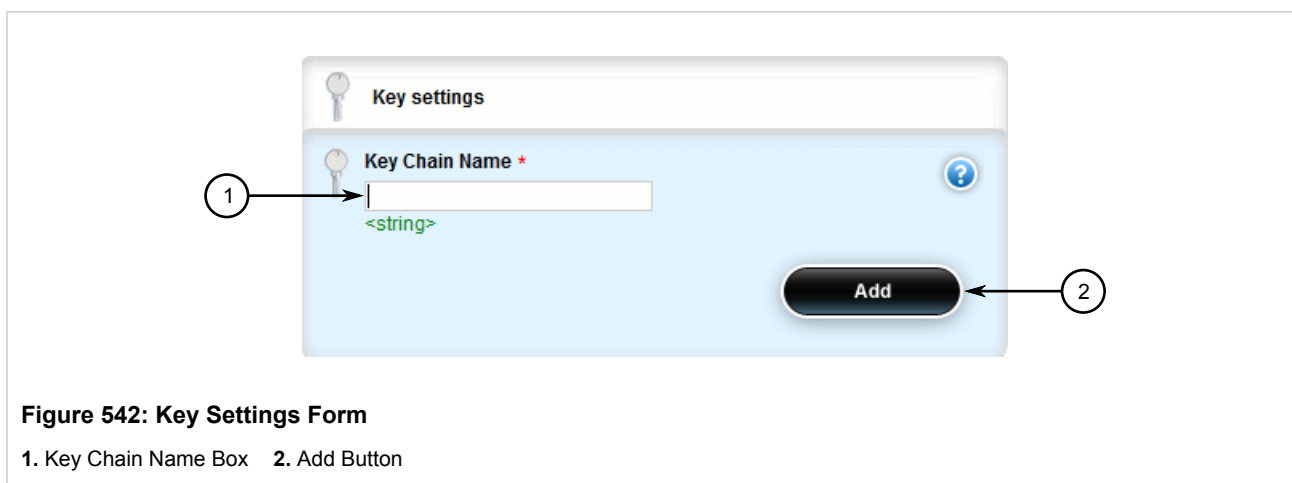
If no keys have been configured, add keys as needed. For more information, refer to [Section 5.19.9.4, “Adding a Key”](#).

## Section 5.19.9.3

## Adding a Key Chain

To add a key chain for dynamic RIP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » key-chain** and click **<Add key-chain>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Key Chain Name	<b>Synopsis:</b> A string 1 to 1024 characters long The name of the key chain.

4. Click **Add** to add the key chain.
5. Configure one or more keys for the key chain. For more information, refer to [Section 5.19.9.4, “Adding a Key”](#).
6. Configure a routing interface to use the key chain for authentication purposes. For more information, refer to [Section 5.19.11.2, “Configuring a Routing Interface”](#)
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

## Section 5.19.9.4

## Adding a Key

Keys (or shared secrets) are used to authenticate communications over a RIP network. To maintain network stability, each key is assigned an accept and send lifetime.

The *accept* lifetime is the time period in which the key is accepted by the device.

The *send* lifetime is the time period in which the key can be sent to other devices.

This is referred to as hitless authentication key rollover, a method for seamlessly updating authentication keys without having to reset network sessions.

To add a key to a key chain, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » key-chain » {name} » key**, where {name} is the name of the key chain.
3. Click **<Add key>**. The **Key Settings** form appears.

**Figure 543: Key Settings Form**

1. Key ID Box 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Key ID	The key identifier number.

5. Click **Add** to add the key chain. The **Key Configuration**, **Accept Life Time** and **Send Life Time** forms appear.

**Figure 544: Key Configuration Form**

1. Key Box

1. Time to Start  
2013-01-01T01:01:01-00:00

2. Expire Time  
2022-01-01T01:01:01-00:00

**Figure 545: Accept Life Time Form**  
1. Time to Start Box    2. Expire Time Box

1. Time to Start  
2013-01-01T01:01:01-00:00

2. Expire Time  
2022-01-01T01:01:01-00:00

**Figure 546: Send Life Time Form**  
1. Time to Start Box    2. Expire Time Box

6. On the **Key Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Key	<b>Synopsis:</b> A string 1 to 1024 characters long Sets the key string.

7. On the **Accept Life Time** form, configure the following parameter(s) as required:

Parameter	Description
Time to Start	<b>Synopsis:</b> A string The beginning time in which the key is considered valid. <b>Prerequisite:</b> The start time cannot be configured unless the expire time is configured.
Expire Time	<b>Synopsis:</b> { infinite } or a string Expire time. <b>Prerequisite:</b> The expire time cannot be configured unless the start time is configured.

8. On the **Send Life Time** form, configure the following parameter(s) as required:

Parameter	Description
Time to Start	<p><b>Synopsis:</b> A string</p> <p>Sets the time period in which the key on the key chain is considered valid.</p> <p><b>Prerequisite:</b> The start time cannot be configured unless the expire time is configured.</p>
Expire Time	<p><b>Synopsis:</b> { infinite } or a string</p> <p>The time at which the key expires.</p> <p><b>Prerequisite:</b> The expire time cannot be configured unless the start time is configured.</p>

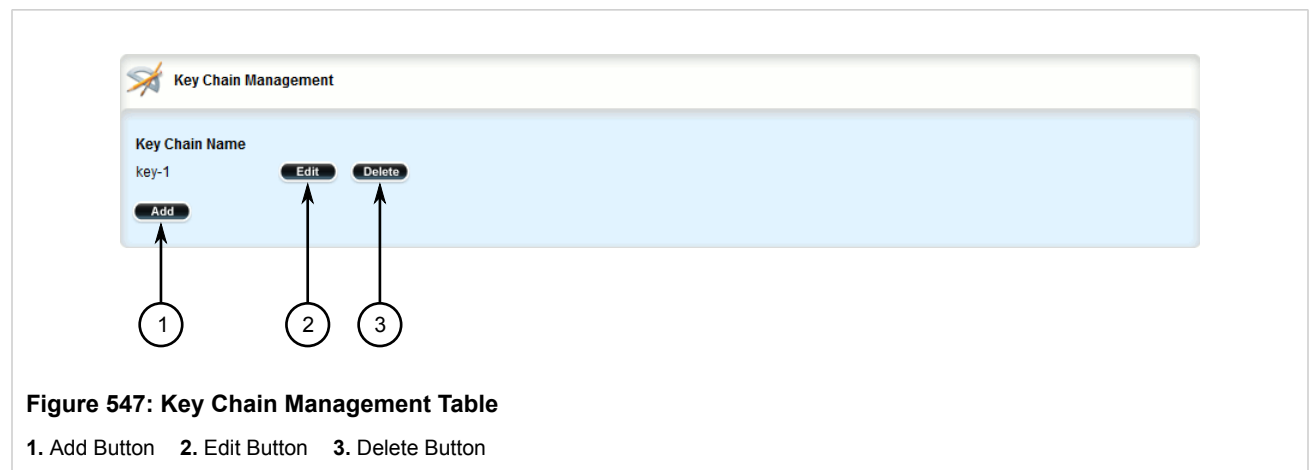
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.19.9.5

### Deleting a Key Chain

To delete a key chain for dynamic RIP routes, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » rip » key-chain**. The **Key Chain Management** table appears.



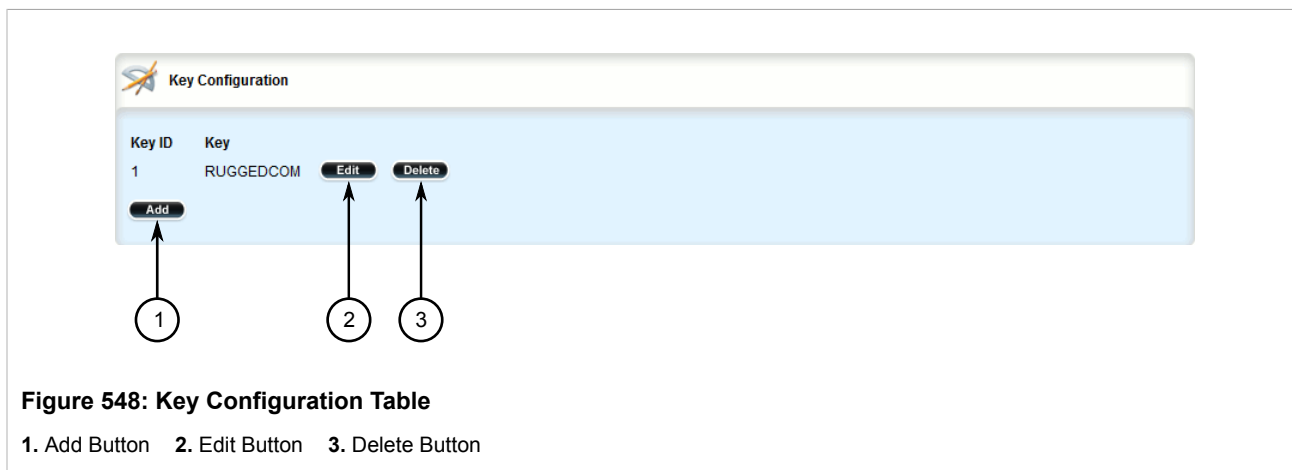
- Click **Delete** next to the chosen key chain.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.19.9.6

### Deleting a Key

To delete a key from a key chain, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » key-chain » {name} » key**, where {name} is the name of the key chain. The **Key Configuration** table appears.



3. Click **Delete** next to the chosen key.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.19.10

## 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.

The following sections describe how to configure and manage redistribution metrics:

- [Section 5.19.10.1, “Viewing a List of Redistribution Metrics”](#)
- [Section 5.19.10.2, “Adding a Redistribution Metric”](#)
- [Section 5.19.10.3, “Deleting a Redistribution Metric”](#)

#### Section 5.19.10.1

### Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic RIP routes, navigate to **routing » dynamic » rip » redistribute**. If metrics have been configured, the **Redistribute Route from Other Protocols** table appears.

Redistribute Route from Other Protocols	
Redistribute Type	Metric
bgp	not found

Figure 549: Redistribute Route from Other Protocols Table

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to [Section 5.19.10.2, “Adding a Redistribution Metric”](#).

Section 5.19.10.2

Adding a Redistribution Metric

To add a redistribution metric for dynamic RIP routes, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *routing » dynamic » rip » redistribute* and click **<Add redistribute>**. The **Key Settings** form appears.

Key settings

Redistribute Type \*

1 → bgp

?

Add

2 →

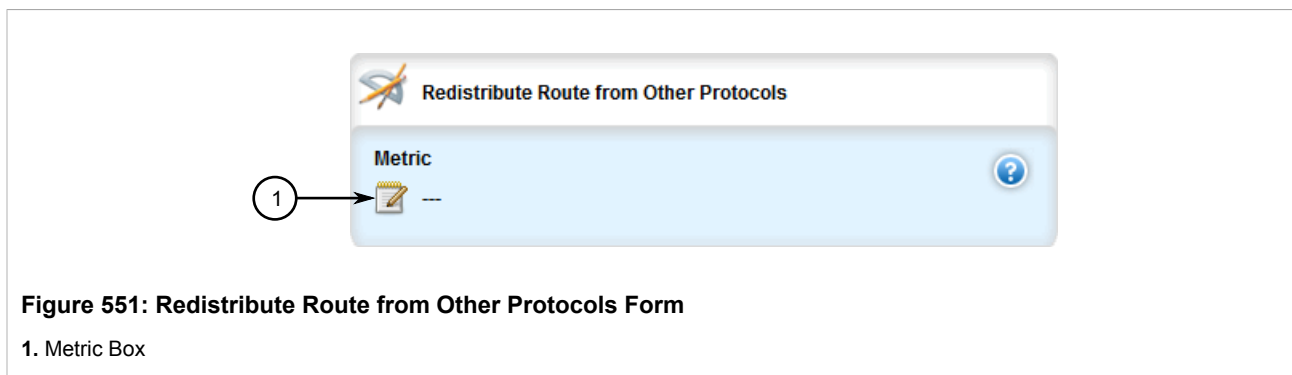
Figure 550: Key Settings Form

1. Redistribute Type List    2. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Type	<b>Synopsis:</b> { kernel, static, connected, ospf, bgp } Redistribute route type.

- 4. Click **Add** to add the metric. The **Redistribute Route from Other Protocols** form appears.



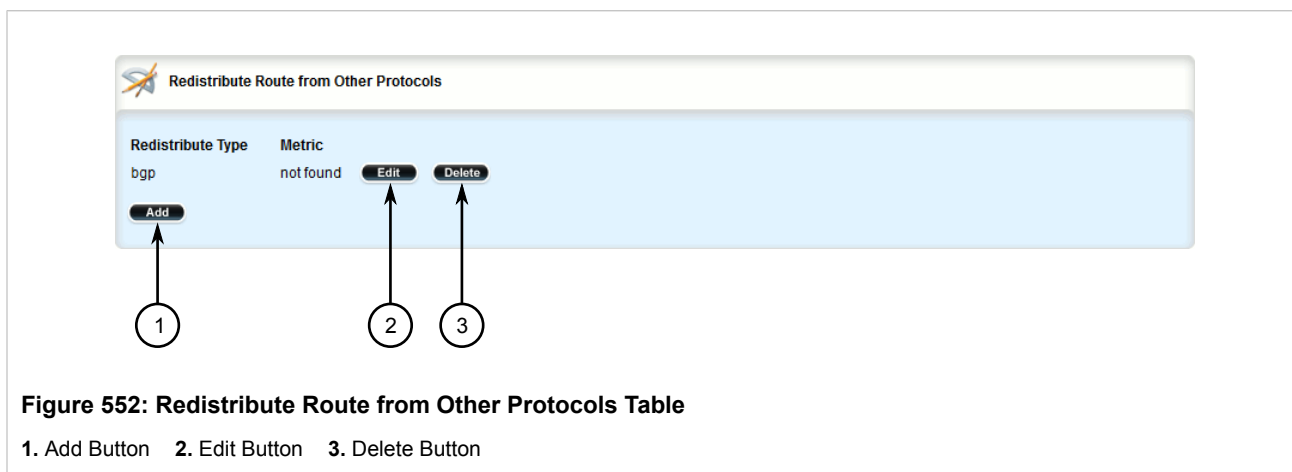
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 5.19.10.3

### Deleting a Redistribution Metric

To delete a redistribution metric for dynamic RIP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » redistribute**. The **Redistribute Route from Other Protocols** table appears.



3. Click **Delete** next to the chosen metric.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.



## Section 5.19.11

## Managing Routing Interfaces

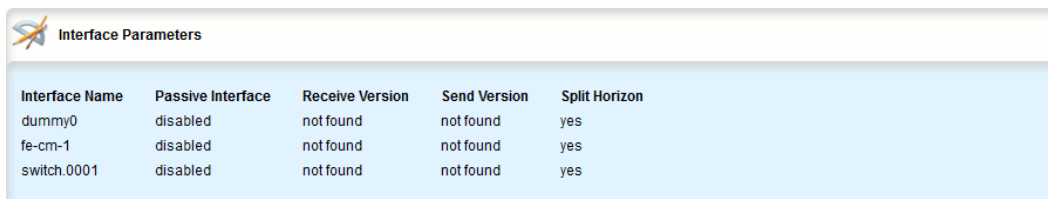
The following sections describe how to configure and manage routing interfaces for dynamic RIP routes:

- [Section 5.19.11.1, “Viewing a List of Routing Interfaces”](#)
- [Section 5.19.11.2, “Configuring a Routing Interface”](#)

## Section 5.19.11.1

### Viewing a List of Routing Interfaces

To view a list of routing interfaces for a RIP network, navigate to **routing » dynamic » rip » interface**. The **Interface Parameters** table appears.



Interface Name	Passive Interface	Receive Version	Send Version	Split Horizon
dummy0	disabled	not found	not found	yes
fe-cm-1	disabled	not found	not found	yes
switch.0001	disabled	not found	not found	yes

Figure 553: Interface Parameters Table

## Section 5.19.11.2

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » rip » interface » {name}**, where **{name}** is the name of the interface. The **Authentication** and **Interface Parameters** forms appear.

**Figure 554: Authentication Form**

1. Mode List   2. Key Chain List   3. String Box

**Figure 555: Interface Parameters Form**

1. Passive Interface Check Box   2. Receive Version List   3. Send Version List   4. Split Horizon List

- On the **Authentication** form, configure the following parameter(s) as required:

Parameter	Description
Mode	<b>Synopsis:</b> { md5-rfc, md5-old-ripd, text, none } The authentication mode.
Key Chain	The authentication key chain.
String	<b>Synopsis:</b> A string 1 to 16 characters long The authentication string.

- On the **Interface Parameters** form, configure the following parameter(s) as required:

Parameter	Description
Passive Interface	<b>Synopsis:</b> typeless The specified interface is set to passive mode. In passive mode, all received packets are processed normally and RIPd sends neither multicast nor unicast RIP packets except to RIP neighbors specified with a neighbor element.
Receive Version	<b>Synopsis:</b> { 1, 2, 1,2, 2,1 } The version of RIP packets that will be accepted on this interface. By default, version 1 and version 2 packets will be accepted.
Send Version	<b>Synopsis:</b> { 1, 2, 1,2, 2,1 } The version of RIP to send packets with. By default, version 2 packets will be sent.
Split Horizon	<b>Synopsis:</b> { yes, no, poisoned-reverse } <b>Default:</b> yes A split horizon.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.20

## Managing OSPF

The Open Shortest Path First (OSPF) protocol determines the best path for routing IP traffic over a TCP/IP network based on link cost and quality. Unlike static routing, OSPF takes link failures and other network topology changes into account. OSPF also differs from RIP in that it provides less router to router update traffic.

The RUGGEDCOM ROX II OSPF daemon (ospfd) is an [RFC 2178](http://tools.ietf.org/html/rfc2178) [http://tools.ietf.org/html/rfc2178] compliant implementation of OSPF version 2. The daemon also adheres to the Opaque LSA ([RFC 2370](http://tools.ietf.org/html/rfc2370) [http://tools.ietf.org/html/rfc2370]) and ABR-Types ([RFC 3509](http://tools.ietf.org/html/rfc3509) [http://tools.ietf.org/html/rfc3509]) extensions.

OSPF network design usually involves partitioning a network into a number of self-contained areas. The areas are chosen to minimize intra-area router traffic, making more manageable and reducing the number of advertised routes. Area numbers are assigned to each area. All routers in the area are known as Area routers. If traffic must flow between two areas a router with links in each area is selected to be an Area Border router, and serves as a gateway.

**NOTE**

The **Router ID** parameter defines the ID of the router. By default this is the highest IP assigned to the router. It is recommended to configure this value manually to avoid the ID changing if interfaces are added or deleted from the router. During elections for the master router, the ID is one of the values used to pick the winner. Keeping the ID fixed will avoid any unexpected changes in the election of the master router.

**NOTE**

In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.



#### NOTE

*Specific routes for Virtual Routing and Forwarding (VRF) interfaces can be configured. For more information about VRF, refer to [Section 5.21, “Managing Virtual Routing and Forwarding \(VRF\)”](#).*

The following sections describe how to configure and manage OSPF:

- [Section 5.20.1, “OSPF Concepts”](#)
- [Section 5.20.2, “Configuring OSPF”](#)
- [Section 5.20.3, “Viewing the Status of Dynamic OSPF Routes”](#)
- [Section 5.20.4, “Managing Prefix Lists and Entries”](#)
- [Section 5.20.5, “Managing Areas”](#)
- [Section 5.20.6, “Managing Route Maps”](#)
- [Section 5.20.7, “Managing Incoming Route Filters”](#)
- [Section 5.20.8, “Managing Redistribution Metrics”](#)
- [Section 5.20.9, “Managing Routing Interfaces”](#)
- [Section 5.20.10, “Managing Message Digest Keys”](#)

#### Section 5.20.1

## 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 5.20.2

## Configuring OSPF

To configure dynamic routing using the Open Shortest Path First (OSPF) daemon, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » ospf**. The **Distance OSPF** and **OSPF Configuration** forms appear.

The image shows a web interface for configuring OSPF distances. The form is titled "Distance OSPF" and contains three sections, each with a pencil icon, a dashed line, and a help icon. The sections are labeled "External Routes Distance", "Inter Area Routes Distance", and "intra Area Routes Distance". Numbered callouts 1, 2, and 3 point to the pencil icons in each section respectively.

Section	Icon	Value	Help
External Routes Distance	Pencil	---	?
Inter Area Routes Distance	Pencil	---	?
intra Area Routes Distance	Pencil	---	?

**Figure 556: Distance OSPF Form**

1. External Routes Distance Box   2. Inter Area Routes Distance Box   3. Intra Area Routes Distance Box

1

2

3

4

5

6

7

8

9

10

11

OSPF Configuration

Enable OSPF

☐ Enabled

?

ABR Type \*

cisco

(cisco)

?

Auto Cost Reference Bandwidth \*

100

(100)

?

Compatible with RFC1583

☐ Enabled

?

Default Information Originate

☐ Enabled

?

Default Metric

--

?

Distance

--

?

Enable Opaque-L SA capability

☐ Enabled

?

Passive Default \*

☒ Enabled

(true)

?

Refresh Timer \*

10

(10)

?

Router ID

--

?

**Figure 557: OSPF Configuration Form**

1. Enable OSPF Check Box   2. ABR Type List   3. Auto Cost Reference Bandwidth Box   4. Compatible with RFC1583 Check Box   5. Default Information Originate Check Box   6. Default Metric Box   7. Distance Box   8. Enable Opaque LSA Capability Box   9. Passive Default Check Box   10. Refresh Timer Box   11. Router ID Box

3. In the **Distance OSPF** form, configure the following parameters:

Parameter	Description
External Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for external routes.

Parameter	Description
Inter Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for inter-area routes.
intra Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for intra-area routes.

4. In the **OSPF Configuration** form, configure the following parameters:

Parameter	Description
Enable OSPF	<b>Synopsis:</b> typeless Enables the OSPF dynamic routing protocol.
ABR Type	<b>Synopsis:</b> { cisco, ibm, shortcut, standard } <b>Default:</b> cisco The OSPF ABR type.
Auto Cost Reference Bandwidth	<b>Synopsis:</b> An integer between 1 and 4294967 <b>Default:</b> 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
Compatible with RFC1583	<b>Synopsis:</b> typeless Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
Default Information Originate	<b>Synopsis:</b> typeless Advertises the default route.
Default Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The default metric of redistribute routes.
Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance.
Enable Opaque-LSA capability	<b>Synopsis:</b> typeless Enables the Opaque-LSA capability (RFC2370).
Passive Default	<b>Synopsis:</b> true or false <b>Default:</b> true Default passive value for new interface.
Refresh Timer	<b>Synopsis:</b> An integer between 10 and 1800 <b>Default:</b> 10 The refresh timer.
Router ID	<b>Synopsis:</b> A string 7 to 15 characters long The Router ID for OSPF.

5. If **Default Information Originate Check Box** was selected on the **OSPF Configuration** form, the **Default Information Originate** form appears.

**Figure 558: Default Information Originate Form**

1. Always Advertise Default Route Enable Check Box    2. Metric Box    3. Metric Type Box    4. Route Map List

6. In the **Default Information Originate** form, configure the following parameters:

Parameter	Description
Always Advertise Default Route	<b>Synopsis:</b> true or false <b>Default:</b> false Always advertise default route even when there is no default route present in routing table.
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric value for default route.
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 <b>Default:</b> 2 The metric type for default route.
Route Map	The route map name.

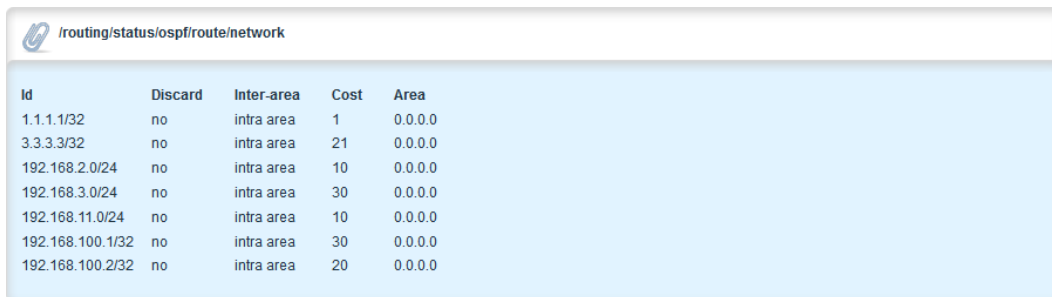
7. Configure prefix list filters. For more information, refer to [Section 5.20.4.3, “Adding a Prefix List”](#).
8. Configure areas. For more information, refer to [Section 5.20.5.2, “Adding an Area”](#).
9. Configure route map filters. For more information, refer to [Section 5.20.6.3, “Adding a Route Map Filter”](#).
10. Configure redistribution metrics. For more information, refer to [Section 5.20.8.2, “Adding a Redistribution Metric”](#).
11. Configure interfaces. For more information, refer to [Section 5.20.9.2, “Configuring a Routing Interface”](#).
12. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
13. Click **Exit Transaction** or continue making changes.



## Section 5.20.3

## Viewing the Status of Dynamic OSPF Routes

To view the status of the dynamic OSPF routes configured on the device, navigate to **routing » status » ospf » route » network**. If OSPF routes have been configured, the **Network** table appears.



The screenshot shows a web interface window titled "/routing/status/ospf/route/network". Inside, there is a table with the following data:

Id	Discard	Inter-area	Cost	Area
1.1.1.1/32	no	intra area	1	0.0.0.0
3.3.3.3/32	no	intra area	21	0.0.0.0
192.168.2.0/24	no	intra area	10	0.0.0.0
192.168.3.0/24	no	intra area	30	0.0.0.0
192.168.11.0/24	no	intra area	10	0.0.0.0
192.168.100.1/32	no	intra area	30	0.0.0.0
192.168.100.2/32	no	intra area	20	0.0.0.0

Figure 559: Network Table

The **Network** table provides the following information:

Parameter	Description
id	<b>Synopsis:</b> A string Network Prefix.
discard	<b>Synopsis:</b> A string This entry is discarded entry.
inter-area	<b>Synopsis:</b> A string Is path type inter area.
cost	<b>Synopsis:</b> A string Cost.
area	<b>Synopsis:</b> A string Area.

If no dynamic OSPF routes have been configured, configure OSPF and add routes as needed. For more information about configuring OSPF, refer to [Section 5.20.2, “Configuring OSPF”](#).

## Section 5.20.4

## 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.

The following sections describe how to configure and manage prefix lists and entries for dynamic OSPF routes:

- [Section 5.20.4.1, “Viewing a List of Prefix Lists”](#)
- [Section 5.20.4.2, “Viewing a List of Prefix Entries”](#)
- [Section 5.20.4.3, “Adding a Prefix List”](#)
- [Section 5.20.4.4, “Adding a Prefix Entry”](#)

- [Section 5.20.4.5, “Deleting a Prefix List”](#)
- [Section 5.20.4.6, “Deleting a Prefix Entry”](#)

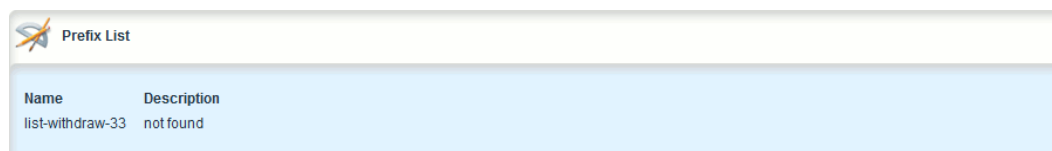
## Section 5.20.4.1

## Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic OSPF routes, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » prefix-list*
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » prefix-list*, where:
  - {vrf} is the chosen VRF

If prefix lists have been configured, the **Prefix List** table appears.



Name	Description
list-withdraw-33	not found

**Figure 560: Prefix List Table**

If no prefix lists have been configured, add lists as needed. For more information, refer to [Section 5.20.4.3, “Adding a Prefix List”](#).

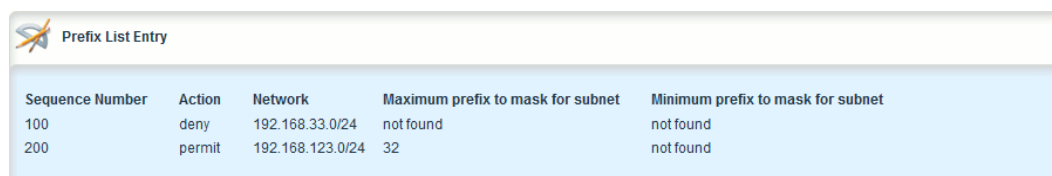
## Section 5.20.4.2

## Viewing a List of Prefix Entries

To view a list of entries for dynamic OSPF prefix lists, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » {name} » entry*, where:
  - {name} is the name of the prefix list
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » {name} » entry*, where:
  - {vrf} is the chosen VRF

If entries have been configured, the **Prefix List Entry** table appears.



Sequence Number	Action	Network	Maximum prefix to mask for subnet	Minimum prefix to mask for subnet
100	deny	192.168.33.0/24	not found	not found
200	permit	192.168.123.0/24	32	not found

**Figure 561: Prefix List Entry Table**

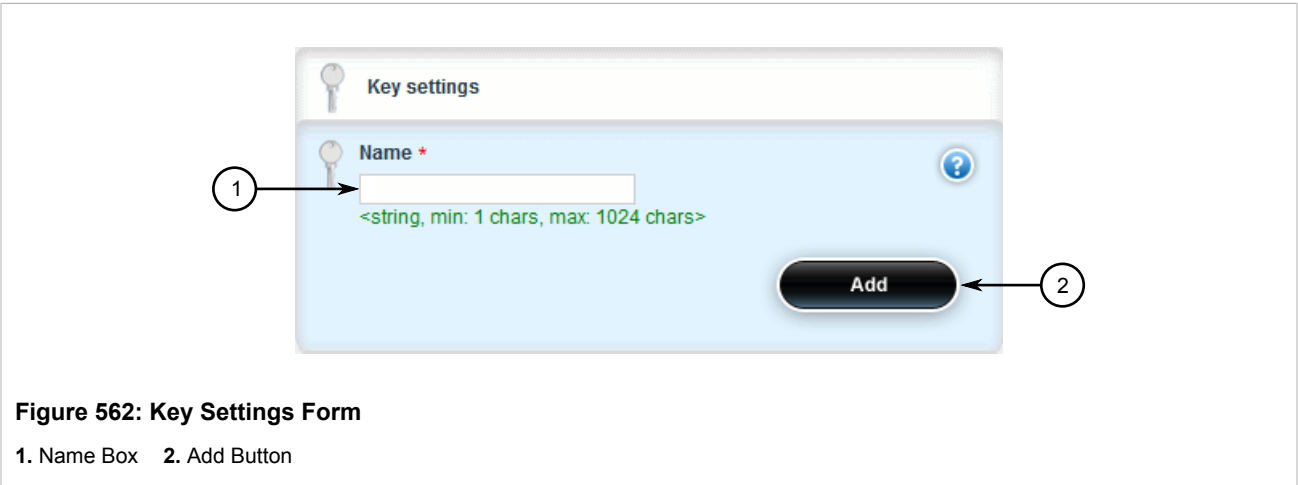
If no entries have been configured, add entries as needed. For more information, refer to [Section 5.20.4.4](#), “Adding a Prefix Entry”.

Section 5.20.4.3

## Adding a Prefix List

To add a prefix list for dynamic OSPF routes, do the following:

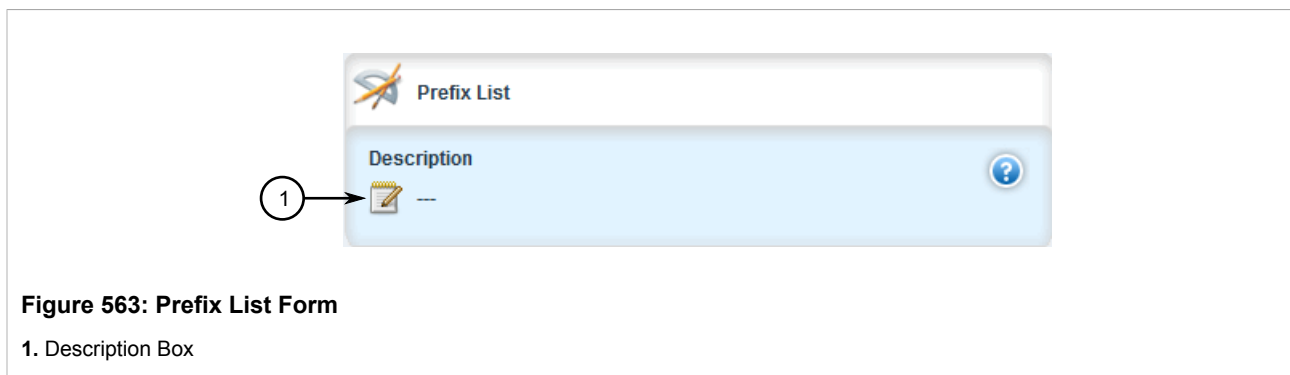
1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » prefix-list*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » prefix-list*, where:
    - {vrf} is the chosen VRF
3. Click **<Add prefix-list>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 1024 characters long The name of the prefix list.

5. Click **Add** to create the new prefix-list. The **Prefix List** form appears.



6. Configure the following parameter(s) as required:

Parameter	Description
Description	<b>Synopsis:</b> A string 1 to 1024 characters long The description of the prefix list.

7. Add prefix entries as needed. For more information, refer to [Section 5.20.4.4, “Adding a Prefix Entry”](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

#### Section 5.20.4.4

### Adding a Prefix Entry

To add an entry for a dynamic OSPF prefix list, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » {name} » entry*, where:
    - {name} is the name of the prefix list
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » {name} » entry*, where:
    - {vrf} is the chosen VRF
3. Click **<Add entry>**. The **Key Settings** form appears.

The image shows a 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a section with a key icon and the text 'Sequence Number \*'. There is a text input field for the sequence number, with a help icon (question mark in a circle) to its right. Below the input field is the text '<unsignedInt, 1 .. 4294967295>'. At the bottom right of the form is a black button with the text 'Add'. A circled number '1' with an arrow points to the sequence number input field. A circled number '2' with an arrow points to the 'Add' button.

Figure 564: Key Settings Form

1. Sequence Number Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 4294967295 Sequence number of the entry.

5. Click **Add** to create the new entry. The **Prefix List Entry** form appears.

The image shows a 'Prefix List Entry' form. It has a title bar with a pencil icon and the text 'Prefix List Entry'. Below the title bar are four sections, each with a help icon (question mark in a circle) to its right. The first section is 'Action \*' with a dropdown menu showing 'permit' and '(permit)'. The second section is 'Network \*' with a text input field and the text '<string, min: 9 chars, max: 18 chars>'. The third section is 'Maximum prefix to mask for subnet' with a text input field and a help icon. The fourth section is 'Minimum prefix to mask for subnet' with a text input field and a help icon. A circled number '1' with an arrow points to the 'Action' dropdown. A circled number '2' with an arrow points to the 'Network' input field. A circled number '3' with an arrow points to the 'Maximum prefix to mask for subnet' input field. A circled number '4' with an arrow points to the 'Minimum prefix to mask for subnet' input field.

Figure 565: Prefix List Entry Form

1. ActionList    2. Network Box    3. Maximum Prefix to Mask for Subnet    4. Minimum Prefix to Mask for Subnet

6. Configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { deny, permit } <b>Default:</b> permit Action.

Parameter	Description
Network	<b>Synopsis:</b> A string 9 to 18 characters long Network (xxx.xxx.xxx.xxx/xx).
Maximum prefix to mask for subnet	<b>Synopsis:</b> An integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
Minimum prefix to mask for subnet	<b>Synopsis:</b> An integer between 1 and 32 The minimum prefix length to match ipaddress within subnet.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

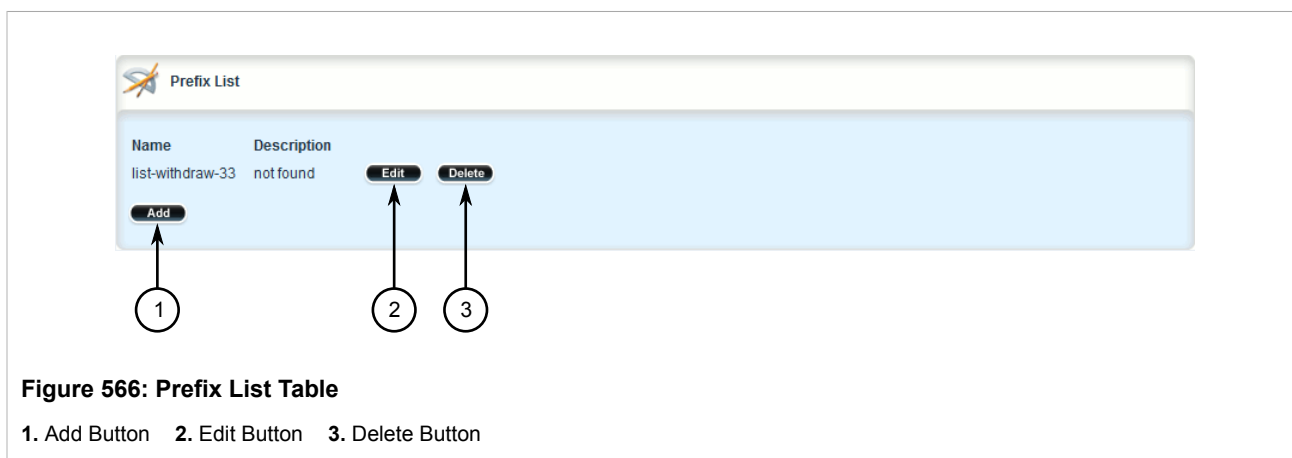
#### Section 5.20.4.5

### Deleting a Prefix List

To delete a prefix list for dynamic OSPF routes, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » prefix-list*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » prefix-list*, where:
    - {vrf} is the chosen VRF

The **Prefix List** table appears.



#### NOTE

*Deleting a prefix list removes all associate prefix entries as well.*

- Click **Delete** next to the chosen prefix list.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

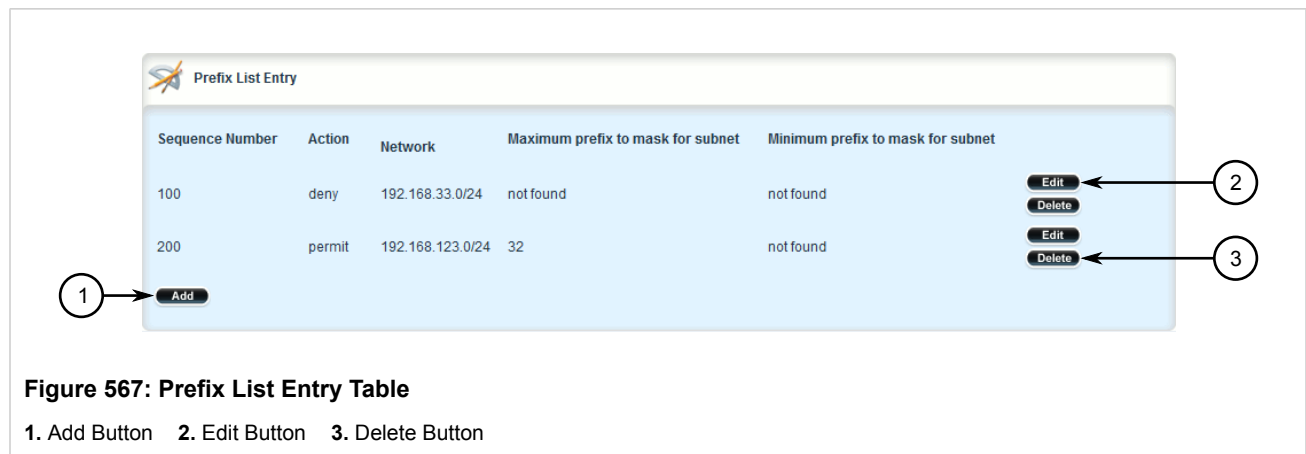
#### Section 5.20.4.6

### Deleting a Prefix Entry

To delete an entry for a dynamic OSPF prefix list, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » {name} » entry*, where:
    - {name} is the name of the prefix list
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » {name} » entry*, where:
    - {vrf} is the chosen VRF

The **Prefix List Entry** table appears.



**Figure 567: Prefix List Entry Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen entry.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.20.5

### 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).

The following sections describe how to configure and manage network areas for dynamic OSPF routes:

- [Section 5.20.5.1, “Viewing a List of Areas”](#)
- [Section 5.20.5.2, “Adding an Area”](#)
- [Section 5.20.5.3, “Deleting an Area”](#)

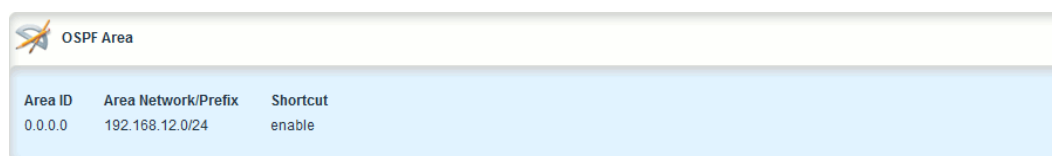
#### Section 5.20.5.1

### Viewing a List of Areas

To view a list of areas configured for dynamic OSPF routes, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » area*
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » area*, where:
  - {vrf} is the chosen VRF

If areas have been configured, the **OSPF Area** table appears.



Area ID	Area Network/Prefix	Shortcut
0.0.0.0	192.168.12.0/24	enable

**Figure 568: OSPF Area Table**

If no areas have been configured, add areas as needed. For more information, refer to [Section 5.20.5.2, “Adding an Area”](#).

#### Section 5.20.5.2

### Adding an Area

To add an area for dynamic OSPF routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » area*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » area*, where:
    - {vrf} is the chosen VRF
3. Click **<Add area>**. The **Key Settings** form appears.



Figure 569: Key Settings Form

1. Area ID Box    2. Area Network/Prefix Box    3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Area ID	<b>Synopsis:</b> A string 7 to 15 characters long The OSPF Area ID (format: A.B.C.D).
Area Network/Prefix	<b>Synopsis:</b> A string 9 to 18 characters long The OSPF area network/prefix.

5. Click **Add** to create the new area. The **OSPF Area** form appears.



**IMPORTANT!**  
*All areas within the same OSPF network must use the same shortcutting mode.*

Figure 570: OSPF Area Form

1. Shortcut List

6. Configure the following parameter(s) as required:

Parameter	Description
shortcut	<b>Synopsis:</b> { default, disable, enable } <b>Default:</b> default

Parameter	Description
	Sets the area's shortcutting mode. Options include: <itemizedlist><listitem>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.</listitem><listitem>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.</listitem> <listitem>Disable: The ABR does not use this area for shortcutting, or set the new bit (S-bit) in the router-LSA originated for it.</listitem></itemizedlist>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

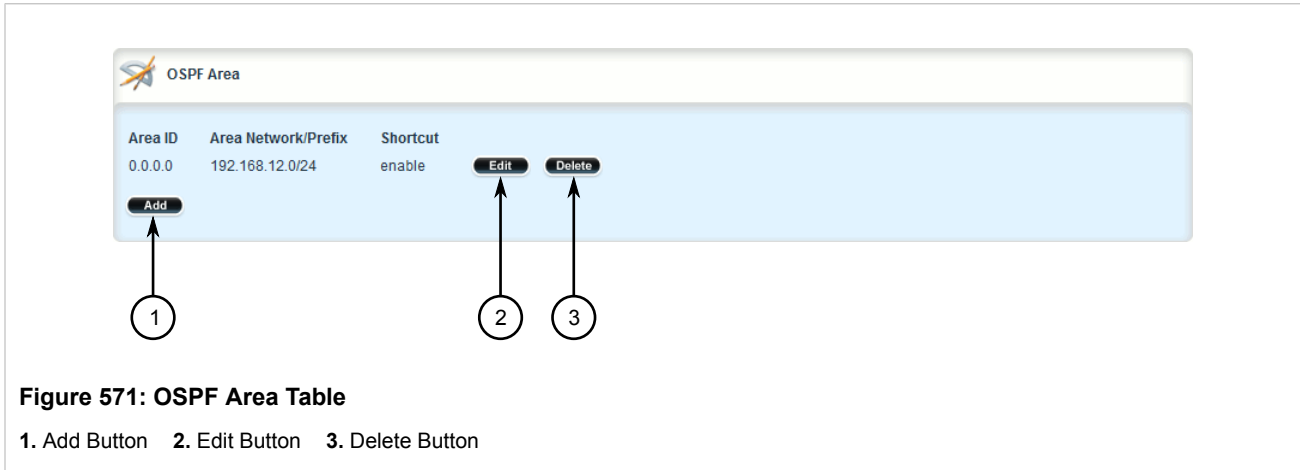
Section 5.20.5.3

## Deleting an Area

To delete an area for dynamic OSPF routes, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » area*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » area*, where:
    - {vrf} is the chosen VRF

The **OSPF Area** table appears.



- Click **Delete** next to the chosen area.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.20.6

## 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.

The following sections describe how to configure and manage route maps for OSPF:

- [Section 5.20.6.1, “Viewing a List of Route Map Filters”](#)
- [Section 5.20.6.2, “Viewing a List of Route Map Filter Entries”](#)
- [Section 5.20.6.3, “Adding a Route Map Filter”](#)
- [Section 5.20.6.4, “Adding a Route Map Filter Entry”](#)
- [Section 5.20.6.5, “Deleting a Route Map Filter”](#)
- [Section 5.20.6.6, “Deleting a Route Map Filter Entry”](#)
- [Section 5.20.6.7, “Configuring Match Rules”](#)

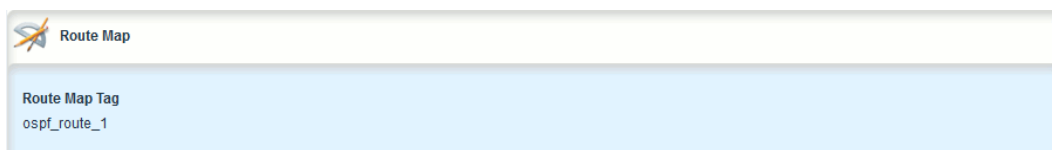
## Section 5.20.6.1

### Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic OSPF routes, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » route-map*
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » route-map*, where:
  - {vrf} is the chosen VRF

If filters have been configured, the **Route Map** table appears.



Route Map
Route Map Tag ospf_route_1

**Figure 572: Route Map Table**

If no filters have been configured, add filters as needed. For more information, refer to [Section 5.20.6.3, “Adding a Route Map Filter”](#).

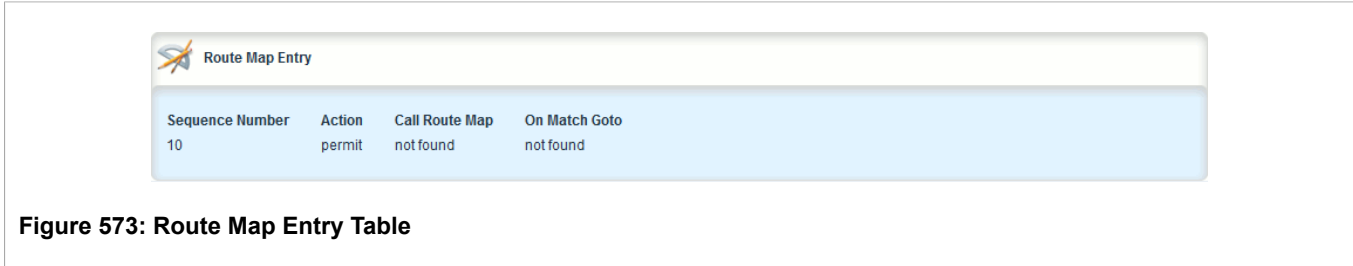
Section 5.20.6.2

## Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either OSPF, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » route-map » {tag} » entry*, where:
  - *{tag}* is the tag for the route map filter
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » route-map » {tag} » entry*, where:
  - *{vrf}* is the chosen VRF

If entries have been configured, the **Route Map Entry** table appears.



If no filters have been configured, add filters as needed. For more information, refer to [Section 5.20.6.4, “Adding a Route Map Filter Entry”](#).

Section 5.20.6.3

## Adding a Route Map Filter

To add a route map filter for dynamic OSPF routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » route-map*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » route-map*, where:
    - *{vrf}* is the chosen VRF
3. Click **<Add route-map>**. The **Key Settings** form appears.

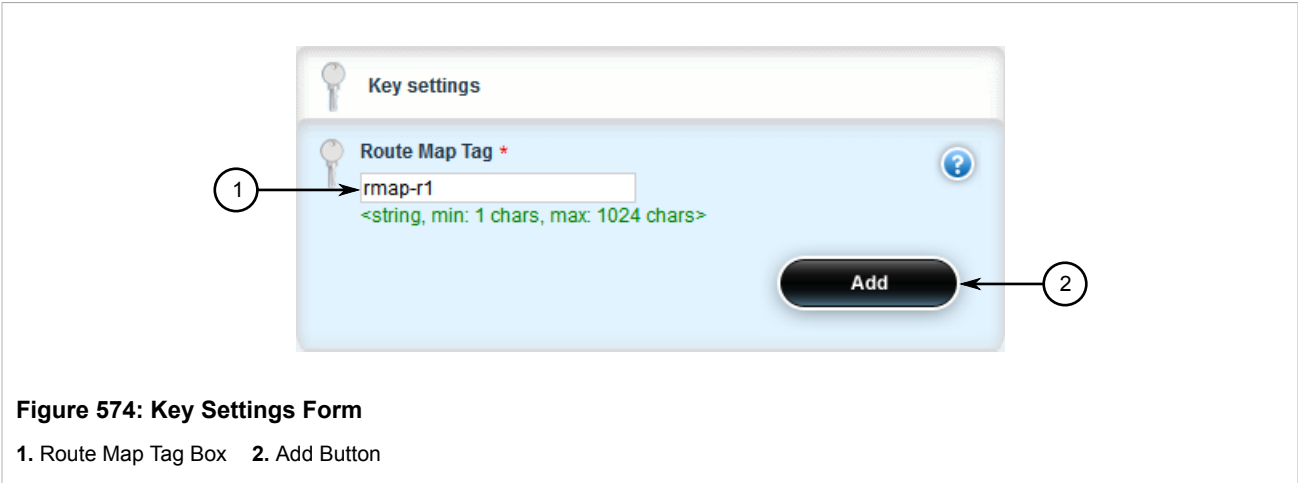


Figure 574: Key Settings Form

1. Route Map Tag Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Route Map Tag	<b>Synopsis:</b> A string 1 to 1024 characters long Route map tag.

- 5. Click **Add** to create the new filter.
- 6. Add one or more entries. For more information, refer to [Section 5.20.6.4, “Adding a Route Map Filter Entry”](#).
- 7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 8. Click **Exit Transaction** or continue making changes.

Section 5.20.6.4

Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » route-map » {tag} » entry*, where:
    - {tag} is the tag for the route map filter
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » route-map » {tag} » entry*, where:
    - {vrf} is the chosen VRF
- 3. Click **<Add entry>**. The **Key Settings** form appears.

**Figure 575: Key Settings Form**

1. Sequence Number Box 2. Add Button

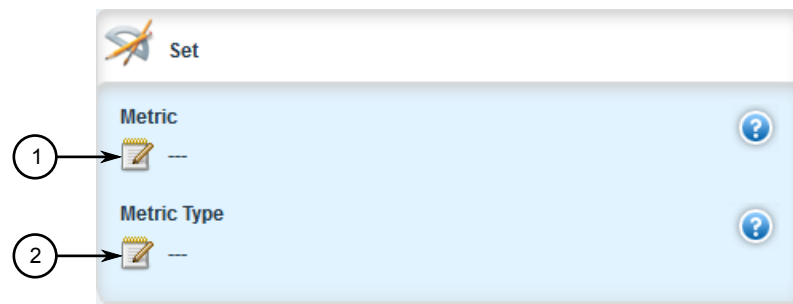
4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	<b>Synopsis:</b> An integer between 1 and 65535 The sequence number of the route-map entry.

5. Click **Add** to create the new entry. The **Route Map Entry** and **Set** forms appear.

**Figure 576: Route Map Entry Form**

1. Action List 2. Call Route Map List 3. On Match Goto List

**Figure 577: Set Form**

1. Metric Box    2. Metric Type Box

6. On the **Route Map Entry** form, configure the following parameter(s) as required:

Parameter	Description
Action	<b>Synopsis:</b> { deny, permit } <b>Default:</b> permit Action.
Call Route Map	Jump to another route-map after match+set.
On Match Goto	Go to this entry on match.

7. On the **Set** form, configure the following parameter(s) as required:

Parameter	Description
Metric	Metric value.
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 External route type.

8. Configure the match rules for the route map filter. For more information, refer to [Section 5.20.6.7, "Configuring Match Rules"](#).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
10. Click **Exit Transaction** or continue making changes.

#### Section 5.20.6.5

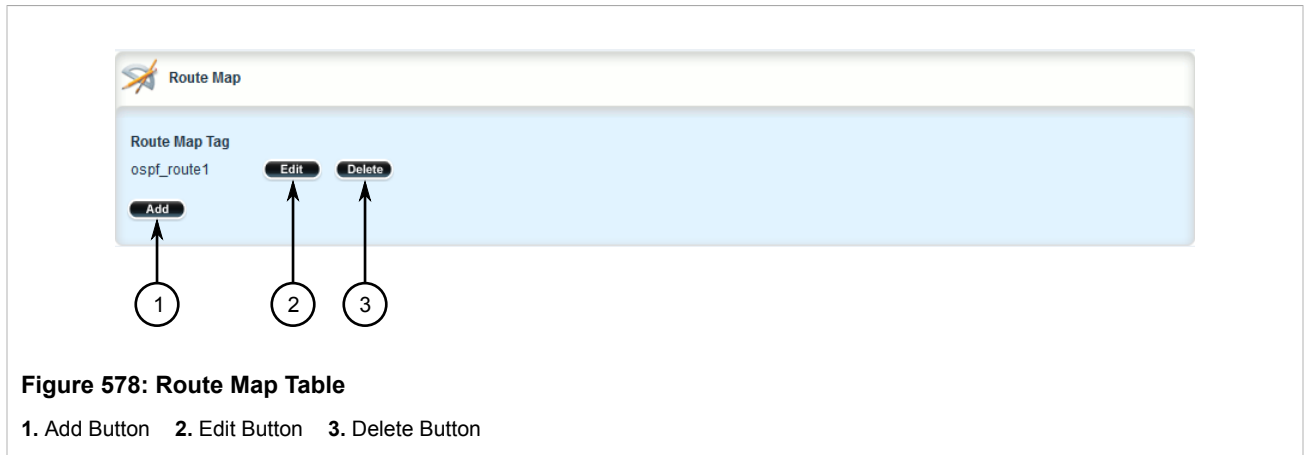
### Deleting a Route Map Filter

To delete a route map filter for dynamic OSPF routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » route-map*

- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » route-map*, where:
  - {vrf} is the chosen VRF

The **Route Map** table appears.



3. Click **Delete** next to the chosen filter.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.20.6.6

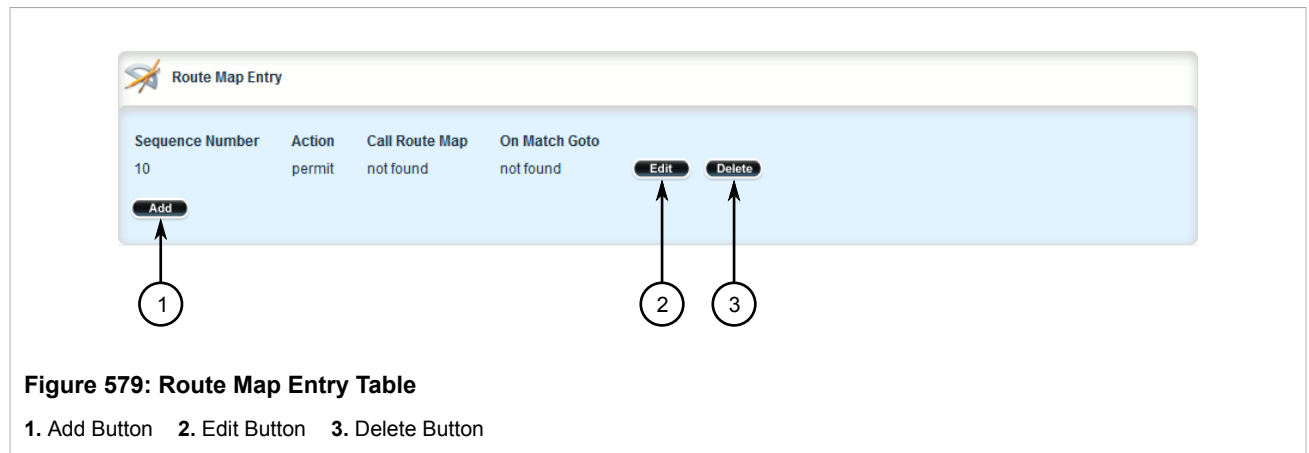
### Deleting a Route Map Filter Entry

To delete an entry for a route map filter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » filter » route-map » {tag} » entry*, where:
    - {tag} is the tag for the route map filter
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » filter » route-map » {tag} » entry*, where:
    - {vrf} is the chosen VRF

The **Route Map Entry** table appears.





- Click **Delete** next to the chosen entry.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

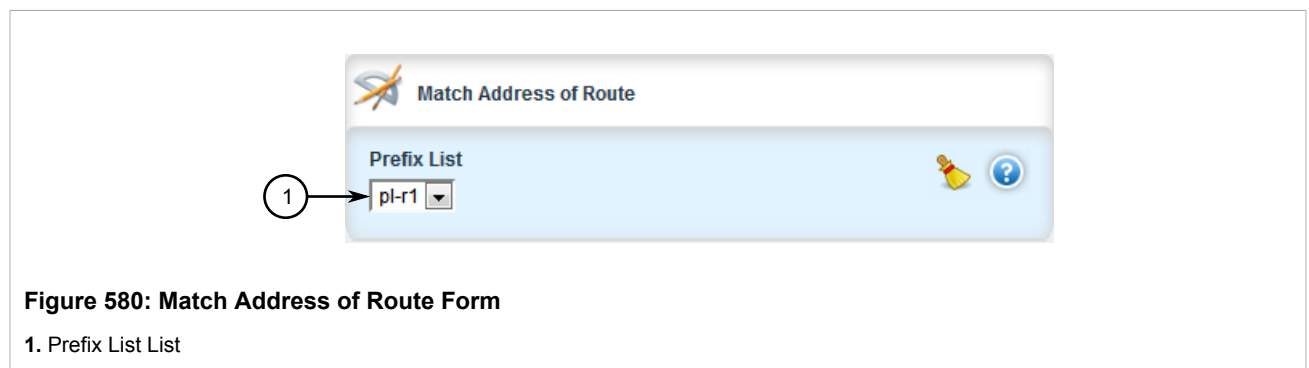
#### Section 5.20.6.7

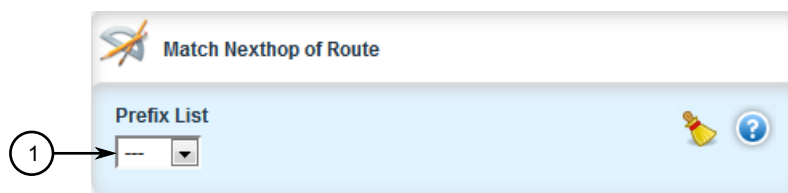
### Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to either:
  - For Standard OSPF Routes**  
*routing » dynamic » ospf » 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
  - 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 and {number} is the sequence number for the entry

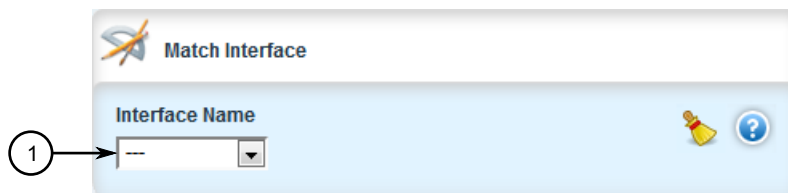
The **Match Address of Route**, **Match Nexthop of Route**, **Match Advertising Source Address** and **Match** forms appear.





**Figure 581: Match Nexthop of Route Form**

1. Prefix List List



**Figure 582: Match Interface Form**

1. Interface Name List

- On the **Match Address of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	The prefix list name.

- On the **Match Nexthop of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	The prefix list name.

- On the **Match** form, configure the following parameters as required:

Parameter	Description
Interface Name	The interface name.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.20.7

## 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 5.20.6, “Managing Route Maps”](#).

The following sections describe how to configure and manage incoming route filters:

- [Section 5.20.7.1, “Viewing List of Incoming Route Filters”](#)
- [Section 5.20.7.2, “Adding an Incoming Route Filter”](#)
- [Section 5.20.7.3, “Deleting an Incoming Route Filter”](#)

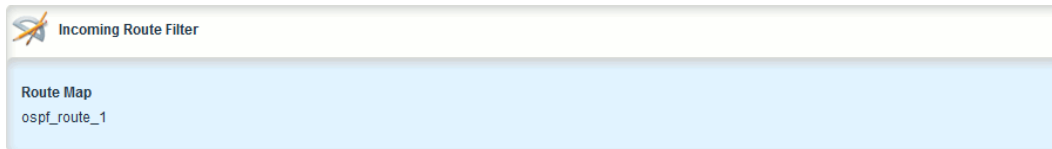
## Section 5.20.7.1

## Viewing List of Incoming Route Filters

To view a list of route filters configured for incoming advertised routes, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » incoming-route-filter*
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » incoming-route-filter*, where:
  - {vrf} is the chosen VRF

If route filters have been configured, the **Incoming Route Filter** table appears.



**Figure 583: Incoming Route Filter Table**

If no route filters have been configured, add filters as needed. For more information, refer to [Section 5.20.7.2, “Adding an Incoming Route Filter”](#).

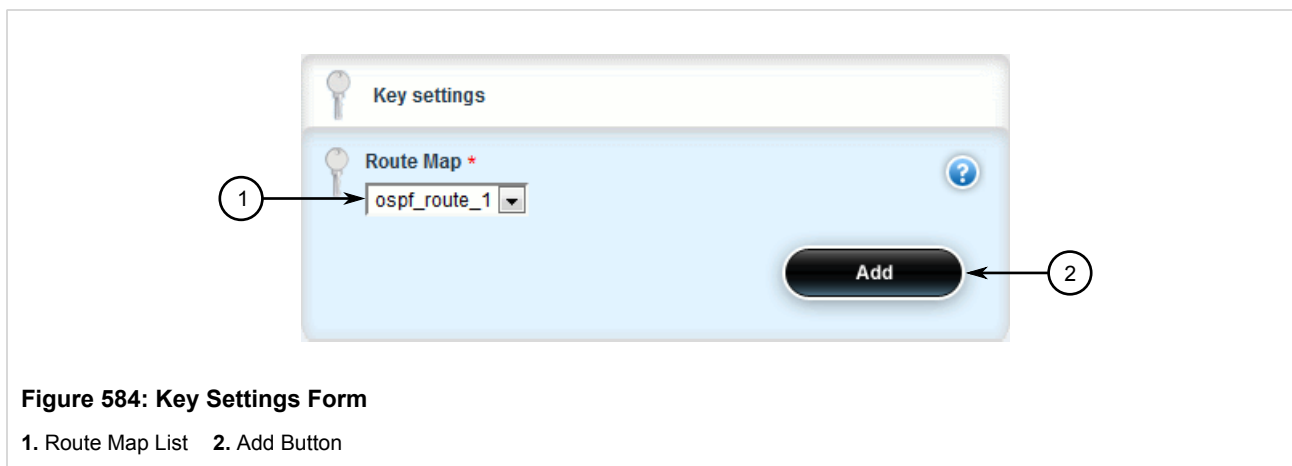
## Section 5.20.7.2

## Adding an Incoming Route Filter

To add a route filter for incoming advertised routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure a route map has been configured. For more information, refer to [Section 5.20.6, “Managing Route Maps”](#)
3. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » incoming-route-filter*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » incoming-route-filter*, where:
    - {vrf} is the chosen VRF

4. Click **<Add incoming-route-filter>**. The **Key Settings** form appears.



5. Click **Add** to create the new incoming route filter.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

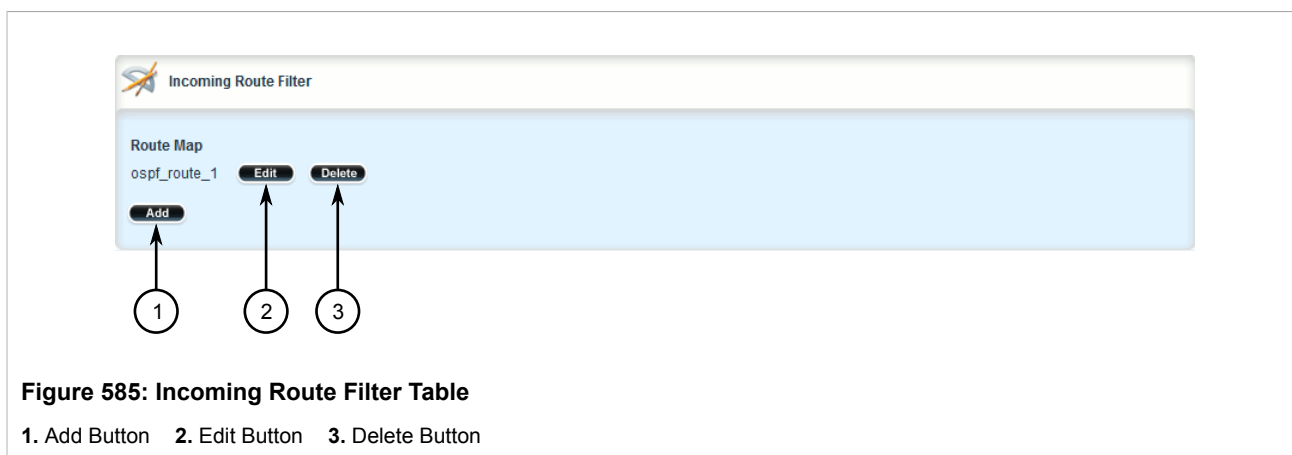
#### Section 5.20.7.3

### Deleting an Incoming Route Filter

To delete a route filter configured for incoming advertised routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » incoming-route-filter*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » incoming-route-filter*, where:
    - {vrf} is the chosen VRF

The **Incoming Route Filter** table appears.



- Click **Delete** next to the chosen incoming route filter.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.20.8

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.

The following sections describe how to configure and manage redistribution metrics:

- Section 5.20.8.1, “Viewing a List of Redistribution Metrics”
- Section 5.20.8.2, “Adding a Redistribution Metric”
- Section 5.20.8.3, “Deleting a Redistribution Metric”

Section 5.20.8.1

Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic OSPF routes, navigate to either:

- For Standard OSPF Routes**  
*routing » dynamic » ospf » redistribute*
- For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » redistribute*, where:
  - {vrf} is the chosen VRF

If metrics have been configured, the **Redistribute Route from Other Protocols** table appears.

Redistribute From Other Routing Protocols		
Redistribute Route From	Metric Type	Metric
bgp	2	not found

Figure 586: Redistribute Route from Other Protocols Table

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to [Section 5.20.8.2, “Adding a Redistribution Metric”](#).

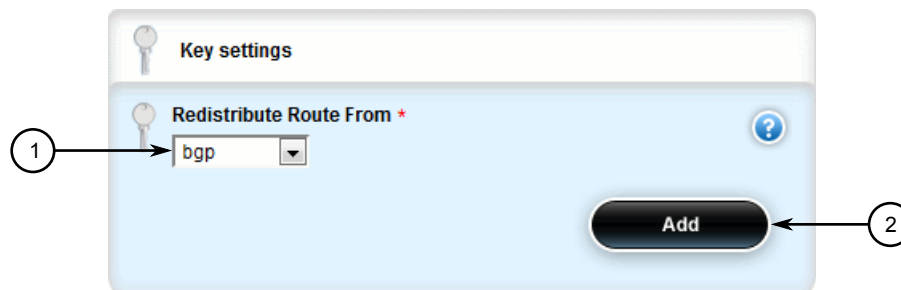
Section 5.20.8.2

Adding a Redistribution Metric

To add a redistribution metric for dynamic OSPF routes, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » redistribute*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » redistribute*, where:
    - {vrf} is the chosen VRF
3. Click **<Add redistribute>**. The **Key Settings** form appears.



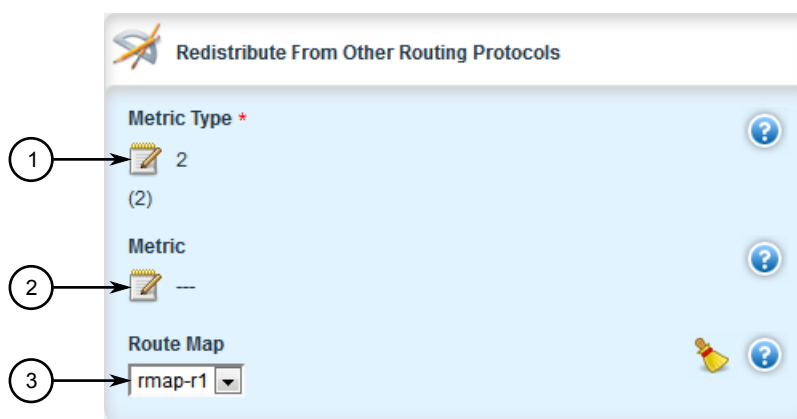
**Figure 587: Key Settings Form**

1. Redistribute Route From List    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Route From	<b>Synopsis:</b> { kernel, static, connected, rip, bgp } Redistributes the route type.

5. Click **Add** to add the metric. The **Redistribute From Other Routing Protocols** form appears.



**Figure 588: Redistribute From Other Routing Protocols Form**

1. Metric Type Box    2. Metric Box    3. Route Map List

6. Configure the following parameter(s) as required:

Parameter	Description
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 <b>Default:</b> 2 The OSPF exterior metric type for redistributed routes.
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric for redistributed routes.
Route Map	The route map name.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

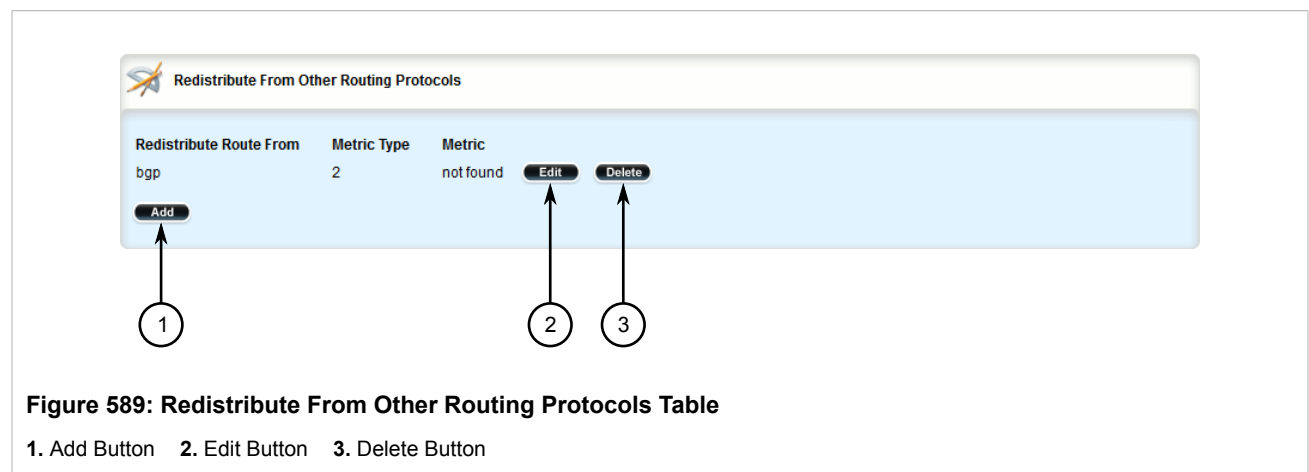
## Section 5.20.8.3

## Deleting a Redistribution Metric

To delete a redistribution metric for dynamic OSPF routes, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » redistribute*
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » redistribute*, where:
    - {vrf} is the chosen VRF

The **Redistribute From Other Routing Protocols** table appears.



**Figure 589: Redistribute From Other Routing Protocols Table**

1. Add Button    2. Edit Button    3. Delete Button

- Click **Delete** next to the chosen metric.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.20.9

## Managing Routing Interfaces

The following sections describe how to configure and manage routing interfaces for dynamic OSPF routes:

- [Section 5.20.9.1, “Viewing a List of Routing Interfaces”](#)
- [Section 5.20.9.2, “Configuring a Routing Interface”](#)


## Section 5.20.9.1

### Viewing a List of Routing Interfaces

To view a list of routing interfaces for an OSPF network, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » interface*
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » interface*, where:
  - {vrf} is the chosen VRF

If interfaces have been configured, the **Interface Parameters** table appears.



Interface Name	Authentication Type	Link Cost	Hello Interval	Priority	Passive Interface	Retransmit Interval	Transmit Delay
dummy0	not found	not found	10	1	true	5	1
fe-cm-1	not found	not found	10	1	true	5	1
switch.0001	not found	not found	10	1	true	5	1

**Figure 590: Interface Parameters Table**

## Section 5.20.9.2

### Configuring a Routing Interface

To configure a routing interface for an OSPF network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » interface » {name}*, where:
    - {name} is the name of the interface
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » interface » {name}*, where:
    - {vrf} is the chosen VRF

The **Dead Interval** and **Interface Parameters** forms appear.



**Dead Interval**

Dead Interval \* 40 (40)

Number of Hellos Per Second ---

**Figure 591: Dead Interval Form**

1. Dead Interval Box 2. Number of Hellos Per Second Box

**Interface Parameters**

Authentication Type ---

Link Cost ---

Hello Interval \* 10 (10)

Priority \* 1 (1)

Passive Interface \* ☒ Enabled (true)

Retransmit Interval \* 5 (5)

Transmit Delay \* 1 (1)

**Figure 592: Interface Parameters Form**

1. Authentication Type List 2. Link Cost Box 3. Hello Interval Box 4. Priority Box 5. Passive Interface Box 6. Retransmit Interval Box 7. Transmit Delay Box

- On the **Dead Interval** form, configure the following parameter(s) as required:



#### NOTE

For reliable operation, it is recommended that the **Dead Interval** value be at least four times the number of Hellos per second.



#### NOTE

Lower values of **Dead Interval** and **Number of Hellos Per Second** will help speed up the change in network routes when the topology of the network changes. It will also increase the load on the router and the links, due to higher traffic caused by the increase in messages.

Lower values will also put limits on the number of routes that can be distributed within an OSPF network area, as will running over slower links.



#### 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	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 40 The time before considering a router dead (in seconds).
Number of Hellos Per Second	<b>Synopsis:</b> An integer between 1 and 10 The number of times a hello message can be sent within one second.

- On the **Interface Parameters** form, configure the following parameter(s) as required:



#### NOTE

Link detection is enabled automatically for active network interfaces. It makes sure the appropriate routing daemon is notified when an interface goes down and stops advertising subnets associated with that interface. The routing daemon resumes advertising the subnet when the link is restored. This allows routing daemons to detect link failures more rapidly, as the router does not have to wait for the **dead interval** to time out. Link detection also causes **redistributed** routes to start and stop being advertised based on the status of their interface links.



#### NOTE

The link cost determines which route to use when multiple links can reach a given destination. By default, OSPF assigns the same cost to all links unless it is provided with extra information about the links. Each interface is assumed to be 10 Mbit, unless otherwise specified by the **Auto-Cost Bandwidth** parameter set for the interface. For more information about the **Auto-Cost Bandwidth**, refer to [Section 5.39.1, "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
Authentication Type	<b>Synopsis:</b> { message-digest, null } The authentication type on this interface.

Parameter	Description
Link Cost	<b>Synopsis:</b> An integer between 1 and 65535 The link cost. If not set, the cost is based on calculation of reference bandwidth divide by interface bandwidth.
Hello Interval	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 10 The time (in seconds) between sending hello packets.
priority	<b>Synopsis:</b> An integer between 0 and 255 <b>Default:</b> 1 Priority of interface.
Passive Interface	<b>Synopsis:</b> true or false <b>Default:</b> true Whether an interface is active or passive. Passive interfaces do not send LSAs to other routers and are not part of an OSPF area.
Retransmit Interval	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 5 Time (in seconds) between retransmitting lost link state advertisements.
Transmit Delay	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1 The link state transmit delay (in seconds).

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.20.10

## 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.*

The following sections describe how to configure and manage message digest keys:

- [Section 5.20.10.1, “Viewing a List of Message Digest Keys”](#)

- [Section 5.20.10.2, “Adding a Message Digest Key”](#)
- [Section 5.20.10.3, “Deleting a Message Digest Key”](#)


## Section 5.20.10.1

## Viewing a List of Message Digest Keys

To view a list of message digest keys for an OSPF routing interface, navigate to either:

- **For Standard OSPF Routes**  
*routing » dynamic » ospf » interface » {name} » message-digest-key*, where:
  - {name} is the name of the routing interface
- **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » interface » {name} » message-digest-key*, where:
  - {vrf} is the chosen VRF

If keys have been configured, the **RMessage Digest** table appears.



Key ID	Password (key)
1	RUGGEDCOM

Figure 593: Message Digest Table

If no message digest keys have been configured, add keys as needed. For more information, refer to [Section 5.20.10.2, “Adding a Message Digest Key”](#).

## Section 5.20.10.2

## Adding a Message Digest Key

To add a message digest key to an OSPF routing interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
*routing » dynamic » ospf » interface » {name} » message-digest-key*, where:
    - {name} is the name of the routing interface
  - **For VRF Routes via OSPF**  
*routing » dynamic » ospf » vrf » {vrf} » interface » {name} » message-digest-key*, where:
    - {vrf} is the chosen VRF
3. Click **<Add message-digest-key>**. The **Key Settings** form appears.

**Figure 594: Key Settings Form**

1. Key ID Box 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Key ID	<b>Synopsis:</b> A number with a value of 255 or less The key ID.

5. Click **Add** to add the key. The **Message Digest** form appears.

**Figure 595: Message Digest Form**

1. Password (Key) Box

6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.20.10.3

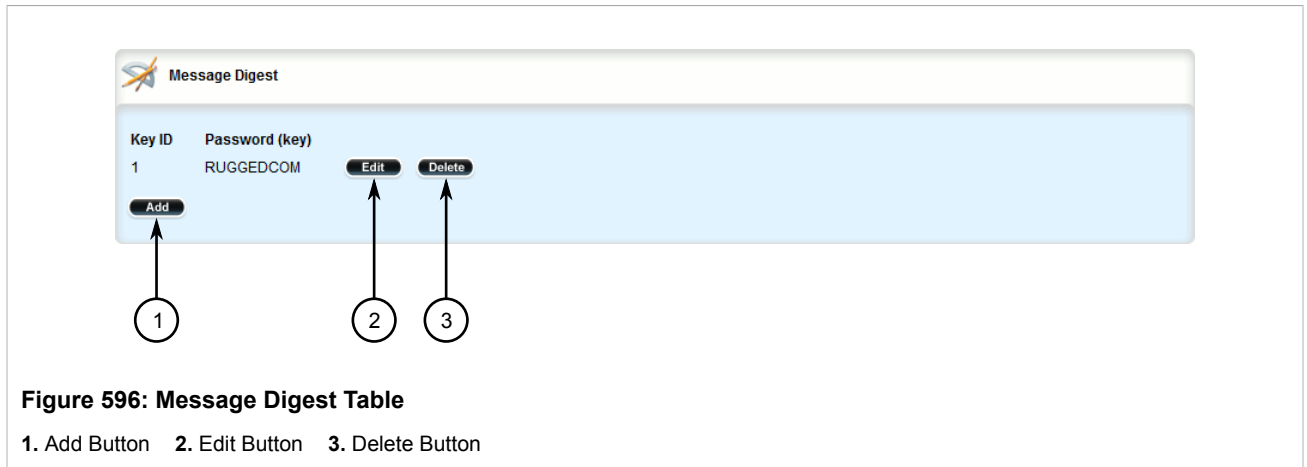
## Deleting a Message Digest Key

To delete a message digest key from an OSPF routing interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Standard OSPF Routes**  
**routing » dynamic » ospf » interface » {name} » message-digest-key**, where:
    - {name} is the name of the routing interface

- For VRF Routes via OSPF  
**routing » dynamic » ospf » vrf » {vrf} » interface » {name} » message-digest-key**, where:
  - {vrf} is the chosen VRF

The **Message Digest** table appears.



3. Click **Delete** next to the chosen key.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.21

# Managing Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) allows multiple routing tables 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 assigned to a specific IP address or interface. Any traffic sent by the CE is labeled to identify the VRF routing table to which it belongs. The Provider Edge (PE) router then routes the traffic through a VPN tunnel based on the designated VRF routing table.

An MPLS label can be applied as well to traffic traversing the tunnel to improve security. This is considered full VRF, as compared to VRF-Lite (first introduced by Cisco).

RUGGEDCOM RX5000/MX5000/MX5000RE devices can be configured to act as a CE, PE or P (provider core) router.

The following sections describe how to configure and manage VRF:

- [Section 5.21.1, “VRF Concepts”](#)
- [Section 5.21.2, “Viewing VRF Interface Statistics”](#)
- [Section 5.21.3, “Configuring VRF”](#)
- [Section 5.21.4, “Configuring a VRF Interface”](#)
- [Section 5.21.5, “Managing VRF Definitions”](#)
- [Section 5.21.6, “Managing Route Targets”](#)

- [Section 5.21.7, “Managing VRF Instances and OSPF”](#)
- [Section 5.21.8, “Managing IP/VPN Tunnels”](#)
- [Section 5.21.9, “Managing VPNv4 Neighbors”](#)
- [Section 5.21.10, “Managing IPv4 Address Families”](#)
- [Section 5.21.11, “Managing Redistribution for IPv4 Address Families”](#)
- [Section 5.21.12, “Managing Neighbors for IPv4 Address Families”](#)
- [Section 5.21.13, “Managing Static VRF Routes”](#)
- [Section 5.21.14, “Managing Gateways for Static VRF Routes”](#)
- [Section 5.21.15, “Managing Interfaces for Static VRF Routes”](#)

## Section 5.21.1

## VRF Concepts

The following sections describe some of the concepts important to the implementation of Virtual Routing and Forwarding (VRP) in RUGGEDCOM ROX II:

- [Section 5.21.1.1, “VRF and VRF-Lite”](#)
- [Section 5.21.1.2, “Advantages and Disadvantages of Using VRF”](#)

## Section 5.21.1.1

### 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 5.21.1.2

### 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

**Disadvantages**

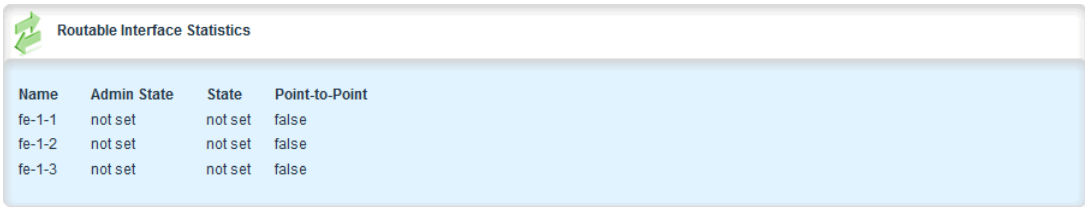
- Greater memory consumption. Each VRF configured results in BGP route replication and requires new FIBs and IP routing tables
- Extra processing (overhead) and memory consumption due to namespace management

- 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

## Section 5.21.2

## Viewing VRF Interface Statistics

To view statistics for interfaces associated with a VRF instance, navigate to **interfaces » vrf » {vrf} » ip**, where {vrf} is the chosen VRF list. The **Routable Interface Statistics** form appears.



Name	Admin State	State	Point-to-Point
fe-1-1	not set	not set	false
fe-1-2	not set	not set	false
fe-1-3	not set	not set	false

**Figure 597: Routable Interface Statistics Form**

This table provides the following information:

Parameter	Description
name	<b>Synopsis:</b> A string 1 to 15 characters long The name of the interface.
Admin State	<b>Synopsis:</b> { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status.
state	<b>Synopsis:</b> { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down.
Point-to-Point	<b>Synopsis:</b> true or false The point-to-point link.
bytes	The number of bytes received.
packets	The number of packets received.
errors	The number of error packets received.
dropped	The number of packets dropped by the receiving device.
bytes	The number of bytes transmitted.
packets	The number of packets transmitted.
errors	The number of error packets transmitted.
dropped	The number of packets dropped by the transmitting device.
collisions	The number of collisions detected on the port.



Section 5.21.3

## 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 5.18.1, “Configuring BGP”](#).
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to [Section 5.21.5.2, “Adding a VRF Definition”](#).
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to [Section 5.21.4, “Configuring a VRF Interface”](#).
4. Enable OSPF. For more information, refer to [Section 5.20.2, “Configuring OSPF”](#).
5. Configure one or more VRF instances for OSPF. For more information, refer to [Section 5.20.2, “Configuring OSPF”](#).
6. Add one or more BGP neighbors. For more information, refer to [Section 5.18.7.2, “Adding a Neighbor”](#).
7. Configure one or more IP/VPN tunnel for each interface. For more information, refer to [Section 5.21.8.2, “Adding an IP/VPN Tunnel”](#).
8. Add one or more BGP neighbors to the VPNv4 address family. For more information, refer to [Section 5.21.9.2, “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 5.18.1, “Configuring BGP”](#).
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to [Section 5.21.5.2, “Adding a VRF Definition”](#).
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to [Section 5.21.4, “Configuring a VRF Interface”](#).
4. Enable OSPF. For more information, refer to [Section 5.20.2, “Configuring OSPF”](#).
5. Configure one or more VRF instances for OSPF. For more information, refer to [Section 5.20.2, “Configuring OSPF”](#).
6. Configure an IPv4 address family for each VRF instance. For more information, refer to [Section 5.21.10.2, “Adding an IPv4 Address Family”](#).
7. Configure one or more static VRF routes. For more information, refer to [Section 5.21.13.2, “Adding a Static VRF Route”](#).
8. Verify the network configuration.

Section 5.21.4

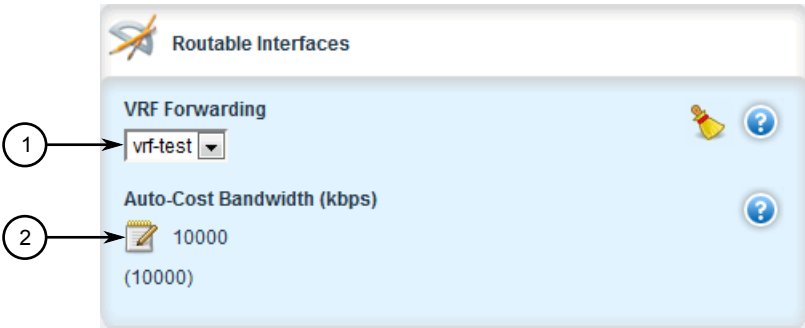
# Configuring a VRF Interface

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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface}**, where {interface} is the name of the routable interface. The **Routable Interfaces** form appears.

**NOTE**  
*The VRF Forwarding list is not available for the dummy interface.*



**Figure 598: Routable Interfaces Form**

1. VRF Forwarding List    2. Auto-Cost Bandwidth Box

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Forwarding	The VRF to which this interface is to be forwarded. When forwarded, this interface will be made available when that VRF is configured in the IS-IS and OSPF routing protocols. When forwarding is changed/removed for this interface, a validation error will be emitted if the interface is configured for use with that VRF in any of those protocols.

4. Configure an IPv4 or IPv6 address for the interface. For more information, refer to [Section 5.39.3.2, “Adding an IPv4 Address”](#) or [Section 5.39.6.2, “Adding an IPv6 Address”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

Section 5.21.5

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.

The following sections describe further how to define and manage VRF definitions:

- [Section 5.21.5.1, “Viewing a List of VRF Definitions”](#)
- [Section 5.21.5.2, “Adding a VRF Definition”](#)
- [Section 5.21.5.3, “Deleting a VRF Definition”](#)

Section 5.21.5.1

Viewing a List of VRF Definitions

To view a list of VRF definitions, navigate to **global » vrf**. If definitions have been configured, the **VRF Definition List Configuration** table appears.

VRF Definition List Configuration		
VRF Name	VRF Description	Route Distinguisher
vrf1	Site A	100:1
vrf2	Site B	100:2

Figure 599: VRF Definition List Configuration Table

If no VRF definitions have been configured, add definitions as needed. For more information, refer to [Section 5.21.5.2, “Adding a VRF Definition”](#).

Section 5.21.5.2

Adding a VRF Definition

To add a VRF definition, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **global » vrf** and click **<Add definition>**. The **Key Settings** form appears.

**Figure 600: Key Settings Form**

1. VRF Name Box    2. Add Button



**NOTE**

*Whenever possible, use meaningful names for each VRF definition, such as **Fin** for financial or **User** for user data.*

*Consider including numbers as well to further isolate separate streams of data (i.e. **PLCvrf1**, **PLCvrf2**, etc.).*

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	<b>Synopsis:</b> A string 1 to 32 characters long The name of the VRF, consisting of 1 to 32 alphanumeric characters. Spaces are not allowed. The 1st character must not be a special character, and following that the only permitted special characters are: -(hyphen), _(underscore), :(colon), and . (period). When created, this VRF name will be added to the list of VRF's available for BGP, IS-IS and OSPF routing protocols. If deleted, a validation error will be emitted if the VRF is configured for use in any of those protocols.

4. Click **Add**. The **VRF Definition Configuration** form appears.

**Figure 601: VRF Definition Configuration Form**

1. VRF Description Box    2. Route Distinguisher Box

5. Configure the following parameter(s) as required:

Parameter	Description
VRF Description	<b>Synopsis:</b> A string 0 to 256 characters long A string that can be used to describe the vrf. Maximum length 256 characters, including blanks.
Route Distinguisher	<b>Synopsis:</b> 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.

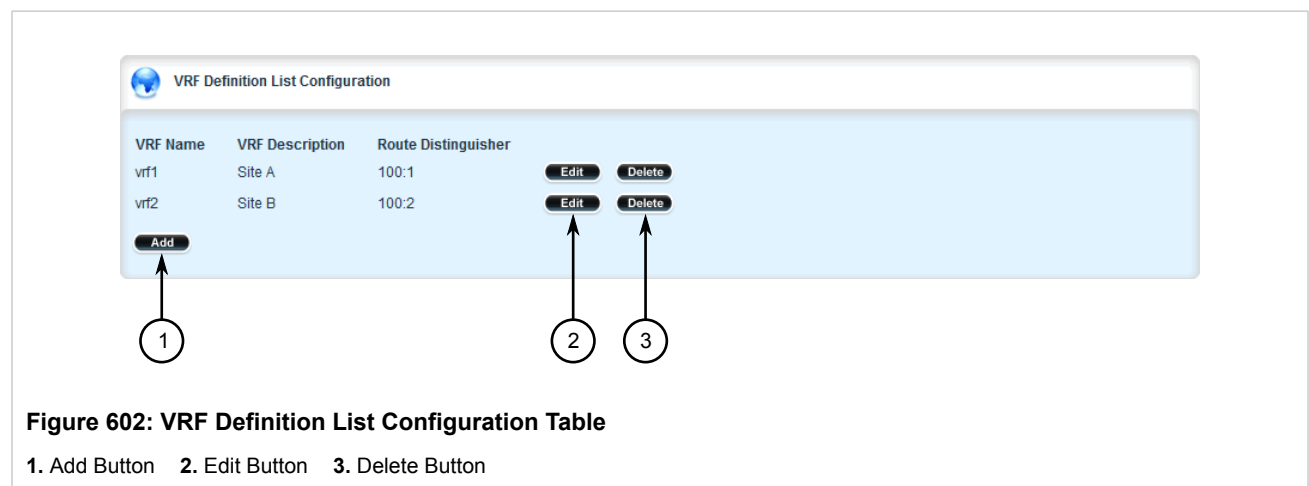
6. Add one or more route targets. For more information, refer to [Section 5.21.6.2, “Adding a Route Target”](#).
7. Configure a routable interface for the VRF instance. For more information, refer to [Section 5.21.4, “Configuring a VRF Interface”](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

## Section 5.21.5.3

## Deleting a VRF Definition

To delete a VRF definition, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
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 5.21.7.3, “Deleting a VRF Instance”](#).
4. Delete the associated IPv4 address family under BGP. For more information, refer to [Section 5.21.10.3, “Deleting an IPv4 Address Family”](#).
5. Navigate to **global » vrf**. The **VRF Definition List Configuration** table appears.



6. Click **Delete** next to the chosen definition.
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

8. Click **Exit Transaction** or continue making changes.

## Section 5.21.6

## 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.

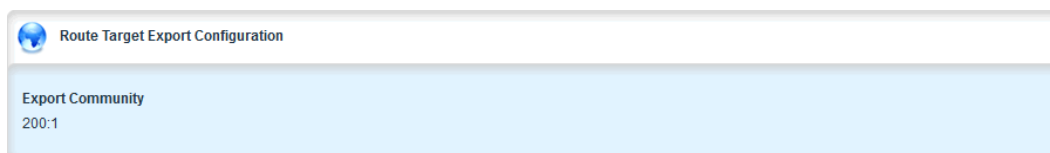
The following sections describe further how to define and manage route targets for VRF:

- [Section 5.21.6.1, “Viewing a List of Route Targets”](#)
- [Section 5.21.6.2, “Adding a Route Target”](#)
- [Section 5.21.6.3, “Deleting a Route Target”](#)

## Section 5.21.6.1

### Viewing a List of Route Targets

To view a list of route targets for a VRF definition, navigate to **global » vrf » {definition} » route-target » {export|import|both}**, where *{definition}* is the name of the VRF definition. If definitions have been configured, the **Route Target Export Configuration**, **Route Target Import Configuration** or **Route Target Both Configuration** table appears, which is applicable.



**Figure 603: Route Target Export Configuration Table (Example)**

If no VRF definitions have been configured, add definitions as needed. For more information, refer to [Section 5.21.5.2, “Adding a VRF Definition”](#).

## Section 5.21.6.2

### Adding a Route Target

To add a route target, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **global » vrf » {definition} » route-target » {export|import|both}**, where *{definition}* is the name of the VRF definition.
3. Click **<Add export>**, **<Add import>** or **<Add both>**, whichever is applicable. The **Key Settings** form appears.

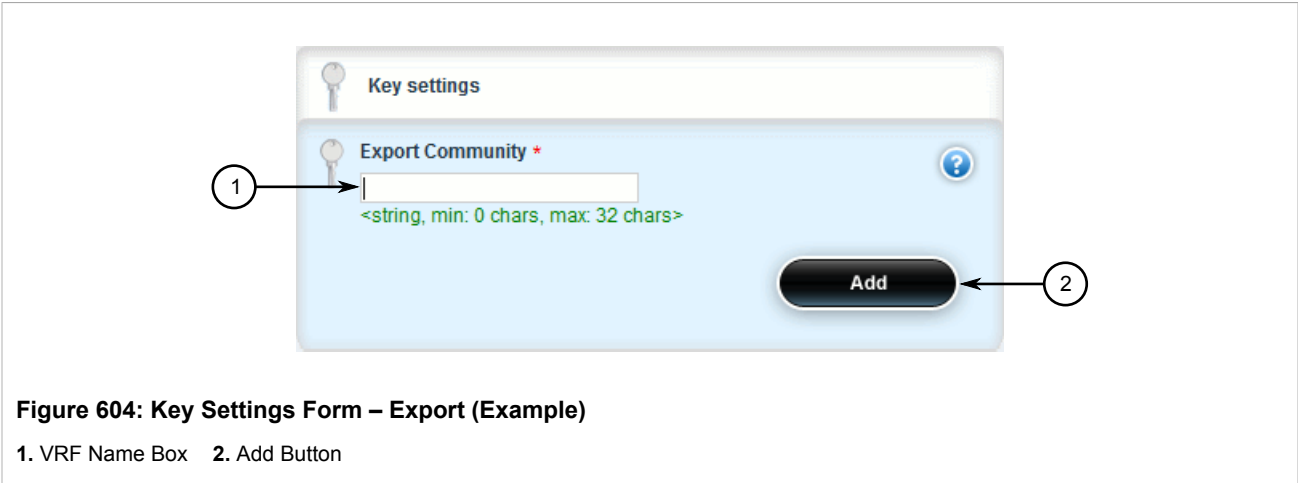


Figure 604: Key Settings Form – Export (Example)

1. VRF Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Export Community	<b>Synopsis:</b> A string 0 to 32 characters long Target VPN extended community to which routing information is exported.

- 5. Click **Add**.
- 6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 7. Click **Exit Transaction** or continue making changes.

Section 5.21.6.3

Deleting a Route Target

- To delete a route target, do the following:
- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
  - 2. Navigate to **global » vrf » {definition} » route-target » {export|import|both}**, where *{definition}* is the name of the VRF definition. The **Route Target Export Configuration**, **Route Target Import Configuration** or **Route Target Both Configuration** table appears, which is applicable.



3. Click **Delete** next to the chosen route target.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.21.7

## Managing VRF Instances and OSPF

OSPF can be configured for one or more VRF definitions. This is done 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).

The following sections detail how to manage VRF instances and configure OSPF:

- [Section 5.21.7.1, “Viewing a List of VRF Instances”](#)
- [Section 5.21.7.2, “Adding a VRF Instance and Configuring OSPF”](#)
- [Section 5.21.7.3, “Deleting a VRF Instance”](#)

#### Section 5.21.7.1

### Viewing a List of VRF Instances

To view a list of VRF instances defined for OSPF, navigate to **routing » dynamic » ospf » vrf**. If definitions have been configured, the **VRF Configuration for OSPF** table appears.



VRF Configuration for OSPF							
VRF Name	Enable OSPF	ABR Type	Auto Cost Reference Bandwidth	Compatible with RFC1583	Default Information Originate	Default Metric	Distance
vrf1	enabled	cisco	100	disabled	disabled	not found	not found
vrf2	enabled	cisco	100	disabled	disabled	not found	not found

**Figure 606: VRF Configuration for OSPF Table**

If no VRF definitions have been configured, add definitions as needed. For more information, refer to [Section 5.21.5.2, “Adding a VRF Definition”](#).

#### Section 5.21.7.2

### Adding a VRF Instance and Configuring OSPF

To add a VRF instance and configure OSPF, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » ospf » vrf** and click **<Add vrf>**. The **Key Settings** form appears.

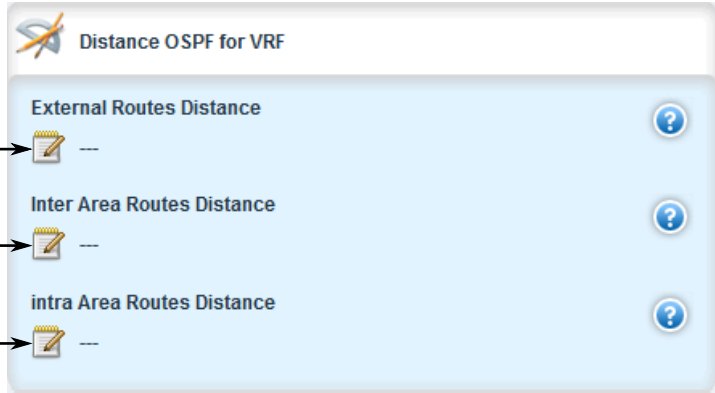
**Figure 607: Key Settings Form**

1. VRF Name List   2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	The VRF name.

4. Click **Add**. The **Distance OSPF for VRF** and **OSPF Configuration for VRF** forms appear.



The image shows a web interface form titled "Distance OSPF for VRF". The form has a light blue background and contains three rows of configuration options. Each row has a label, a text input field, and a help icon (a blue circle with a white question mark). The rows are: "External Routes Distance", "Inter Area Routes Distance", and "intra Area Routes Distance". To the left of the form, there are three numbered circles (1, 2, and 3) with arrows pointing to the text input fields of the three rows respectively.

Label	Value	Help Icon
External Routes Distance	---	?
Inter Area Routes Distance	---	?
intra Area Routes Distance	---	?

**Figure 608: Distance OSPF for VRF Form**

1. External Routes Distance Box    2. Inter Area Routes Distance Box    3. Intra Area Routes Distance Box

The screenshot shows the 'OSPF Configuration for VRF' web form. It contains the following fields and controls, each with a numbered callout:

- 1:** 'Enable OSPF' checkbox, which is checked and labeled 'Enabled'.
- 2:** 'ABR Type' dropdown menu, currently set to 'cisco'.
- 3:** 'Auto Cost Reference Bandwidth' field with a value of '100'.
- 4:** 'Compatible with RFC1583' checkbox, which is unchecked.
- 5:** 'Default Information Originate' checkbox, which is unchecked.
- 6:** 'Default Metric' field, currently empty.
- 7:** 'Distance' field, currently empty.
- 8:** 'Enable Opaque-LSA capability' checkbox, which is unchecked.
- 9:** 'Passive Default' checkbox, which is checked and labeled 'Enabled (true)'.
- 10:** 'Refresh Timer' field with a value of '10'.
- 11:** 'Router-id' field, currently empty.

Each field has a corresponding help icon (a blue circle with a question mark) to its right.

Figure 609: OSPF Configuration for VRF Form

1. Enable OSPF Check Box   2. ABR Type List   3. Auto Cost Reference Bandwidth Box   4. Compatible with RFC1583 Check Box   5. Default Information Originate Check Box   6. Default Metric Box   7. Distance Box   8. Enable Opaque LSA Capability Box   9. Passive Default Check Box   10. Refresh Timer Box   11. Router ID Box

5. In the **Distance OSPF** form, configure the following parameters:

Parameter	Description
External Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for external routes.

Parameter	Description
Inter Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for inter-area routes.
intra Area Routes Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance for intra-area routes.

6. In the **OSPF Configuration** form, configure the following parameters:

Parameter	Description
Enable OSPF	<b>Synopsis:</b> typeless Enables the OSPF dynamic routing protocol.
ABR Type	<b>Synopsis:</b> { cisco, ibm, shortcut, standard } <b>Default:</b> cisco The OSPF ABR type.
Auto Cost Reference Bandwidth	<b>Synopsis:</b> An integer between 1 and 4294967 <b>Default:</b> 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
Compatible with RFC1583	<b>Synopsis:</b> typeless Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
Default Information Originate	<b>Synopsis:</b> typeless Advertises the default route.
Default Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The default metric of redistribute routes.
Distance	<b>Synopsis:</b> An integer between 1 and 255 The administrative distance.
Enable Opaque-LSA capability	<b>Synopsis:</b> typeless Enables the Opaque-LSA capability (RFC2370).
Passive Default	<b>Synopsis:</b> true or false <b>Default:</b> true Default passive value for new interface.
Refresh Timer	<b>Synopsis:</b> An integer between 10 and 1800 <b>Default:</b> 10 The refresh timer.
router-id	<b>Synopsis:</b> A string 7 to 15 characters long The Router ID for OSPF.

7. If **Default Information Originate** is selected on the **OSPF Configuration** form, the **Default Information Originate for VRF** form appears.

**Figure 610: Default Information Originate for VRF Form**

1. Always Advertise Default Route Enable Check Box    2. Metric Box    3. Metric Type Box    4. Route Map List

8. In the **Default Information Originate** form, configure the following parameters:

Parameter	Description
Always Advertise Default Route	<b>Synopsis:</b> true or false <b>Default:</b> false Always advertise default route even when there is no default route present in routing table.
Metric	<b>Synopsis:</b> An integer between 0 and 16777214 The metric value for default route.
Metric Type	<b>Synopsis:</b> An integer between 1 and 2 <b>Default:</b> 2 The metric type for default route.
Route Map	The route map name.

9. Configure prefix list filters for the VRF instance. For more information, refer to [Section 5.20.4.3, “Adding a Prefix List”](#).
10. Configure areas for the VRF instance. For more information, refer to [Section 5.20.5.2, “Adding an Area”](#).
11. Configure route map filters for the VRF instance. For more information, refer to [Section 5.20.6.3, “Adding a Route Map Filter”](#).
12. Configure redistribution metrics for the VRF instance. For more information, refer to [Section 5.20.8.2, “Adding a Redistribution Metric”](#).
13. Configure interfaces for the VRF instance. For more information, refer to [Section 5.20.9.2, “Configuring a Routing Interface”](#).
14. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
15. Click **Exit Transaction** or continue making changes.

## Section 5.21.7.3

## Deleting a VRF Instance

To delete a VRF instance under OSPF, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » ospf » vrf**. The **VRF Configuration for OSPF** table appears.

**VRF Configuration for OSPF**

VRF Name	Enable OSPF	ABR Type	Auto Cost Reference Bandwidth	Compatible with RFC1583	Default Information Originate	Default Metric	Distance	
vrf1	enabled	cisco	100	disabled	disabled	not found	not found	Edit Delete
vrf2	enabled	cisco	100	disabled	disabled	not found	not found	Edit Delete

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen VRF instance.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.21.8

## 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.*

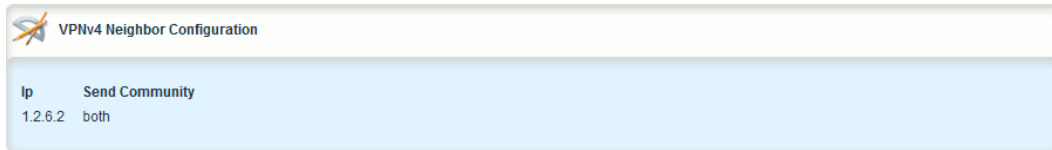
The following sections describe how to configure and manage IP/VPN tunnels:

- [Section 5.21.8.1, “Viewing a List of IP/VPN Tunnels”](#)
- [Section 5.21.8.2, “Adding an IP/VPN Tunnel”](#)
- [Section 5.21.8.3, “Deleting an IP/VPN Tunnels”](#)

### Section 5.21.8.1

## Viewing a List of IP/VPN Tunnels

To view a list of IP/VPN tunnels configured for VRF, navigate to **routing » dynamic » bgp » address-family » vpnv4**. The **VPNv4 Neighbor Configuration** table appears.



VPNv4 Neighbor Configuration	
Ip	Send Community
1.2.6.2	both

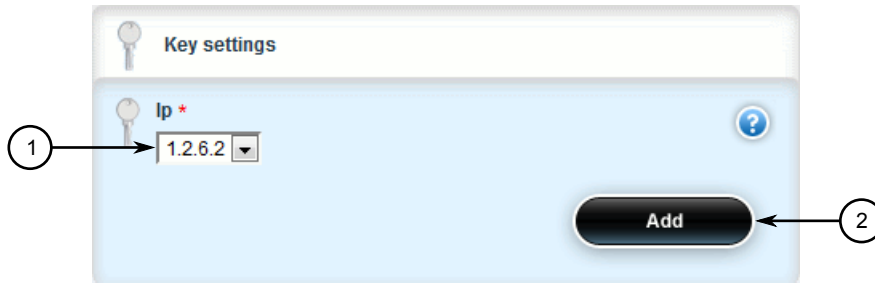
**Figure 612: VPNv4 Neighbor Configuration Table (Example)**

### Section 5.21.8.2

## Adding an IP/VPN Tunnel

To add a new IP/VPN tunnel for VRF, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » vpnv4** and click **<Add neighbor>**. The **Key Settings** form appears.



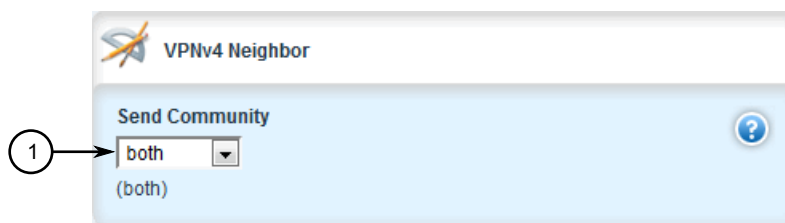
**Figure 613: Key Settings Form**

1. IP Box    2. Add Button

3. Configure the following parameter as required:

Parameter	Description
ip	The neighbor IP address.

4. Click **Add** to add the address. The **VPNv4 Neighbor** form appears.



**Figure 614: VPNv4 Neighbor Form**

1. Select Community List

- Configure the following parameter as required:

Parameter	Description
Send Community	<b>Synopsis:</b> { standard, extended, both, none } <b>Default:</b> both Identifies the send Community. Default is both.

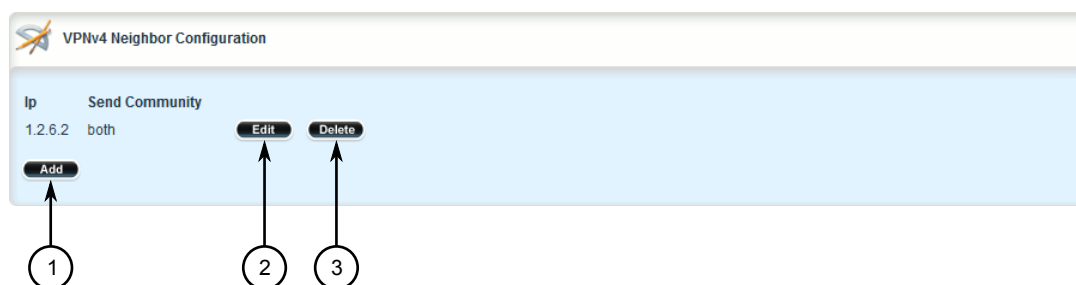
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.21.8.3

## Deleting an IP/VPN Tunnels

To delete an IP/VPN tunnel, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » dynamic » bgp » address-family » vpnv4**. The **VPNv4 Neighbor Configuration** table appears.



**Figure 615: VPNv4 Neighbor Configuration Table (Example)**

1. Add Button 2. Edit Button 3. Delete Button

- Click **Delete** next to the chosen tunnel.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.



5. Click **Exit Transaction** or continue making changes.

## Section 5.21.9

## 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.

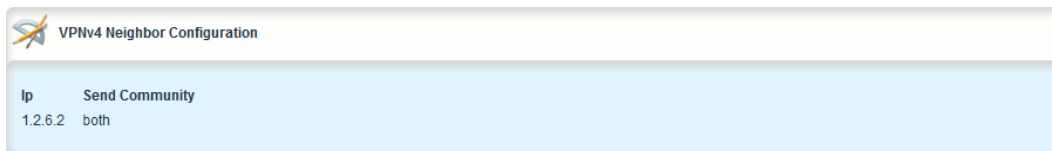
The following sections describe how to configure and manage VPNv4 neighbors for VRF-Lite:

- [Section 5.21.9.1, “Viewing a List of Neighbors”](#)
- [Section 5.21.9.2, “Adding a Neighbor”](#)
- [Section 5.21.9.3, “Deleting a Neighbor”](#)

## Section 5.21.9.1

### Viewing a List of Neighbors

To view a list of configured VPNv4 neighbors, navigate to **routing » dynamic » bgp » address-family » vpnv4**. If neighbors have been configured, the **VPNv4 Neighbor Configuration** table appears.



Ip	Send Community
1.2.6.2	both

**Figure 616: VPNv4 Neighbor Configuration Table**

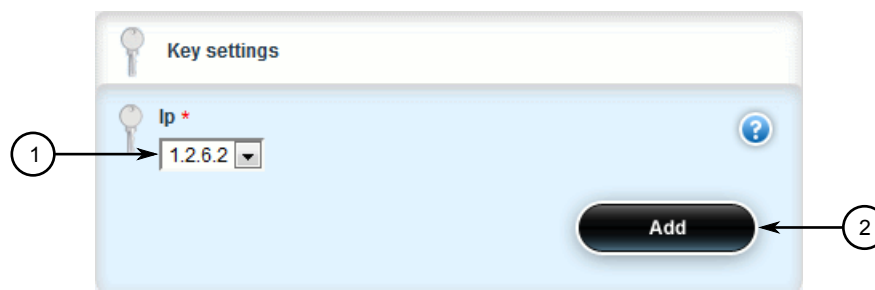
If no neighbors have been configured, add neighbors as needed. For more information, refer to [Section 5.21.12.2, “Adding a Neighbor”](#).

## Section 5.21.9.2

### Adding a Neighbor

To add a new VPNv4 neighbor, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure the desired neighbor is configured for the BGP network. For more information, refer to [Section 5.18.7.2, “Adding a Neighbor”](#).
3. Navigate to **routing » dynamic » bgp » address-family » vpnv4** and click **<Add neighbor>**. The **Key Settings** form appears.



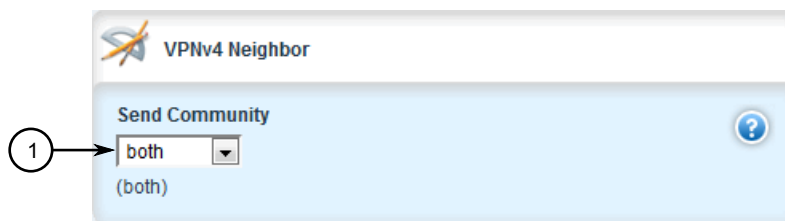
**Figure 617: Key Settings Form**

1. IP Box 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
ip	The neighbor IP address.

5. Click **Add** to add the address. The **VPNv4 Neighbor** form appears.



**Figure 618: VPNv4 Neighbor Form**

1. Send Community List

6. Configure the following parameter(s) as required:

Parameter	Description
Send Community	<b>Synopsis:</b> { standard, extended, both, none } <b>Default:</b> both Identifies the send Community. Default is both.

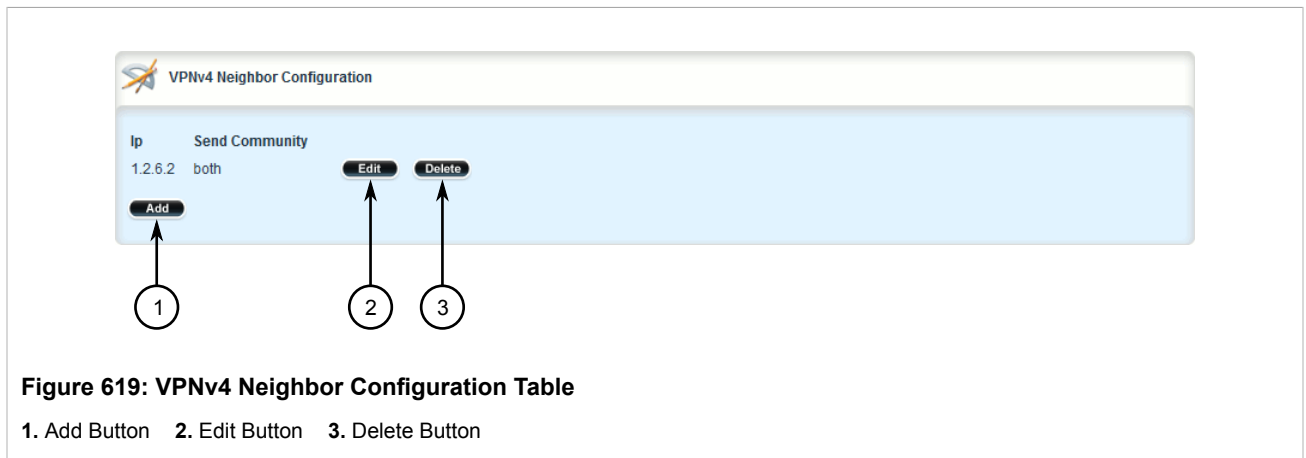
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.21.9.3

## Deleting a Neighbor

To delete a VPNv4 neighbor, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » vpnv4**. The **VPNv4 Neighbor Configuration** table appears.



3. Click **Delete** next to the chosen neighbor.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.21.10

## 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.

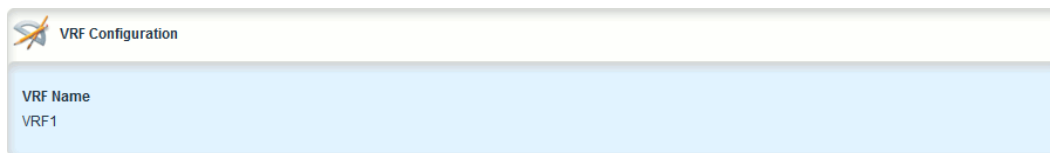
The following sections describe how to configure and manage IPv4 address families:

- [Section 5.21.10.1, “Viewing a List of IPv4 Address Families”](#)
- [Section 5.21.10.2, “Adding an IPv4 Address Family”](#)
- [Section 5.21.10.3, “Deleting an IPv4 Address Family”](#)

#### Section 5.21.10.1

### Viewing a List of IPv4 Address Families

To view a list of IPv4 address families configured for VRF, navigate to **routing » dynamic » bgp » address-family » ipv4**. The **VRF Configuration** form appears.



The image shows a web interface titled "VRF Configuration". It contains a single text input field labeled "VRF Name" with the value "VRF1" entered.

**Figure 620: VRF Configuration Form**

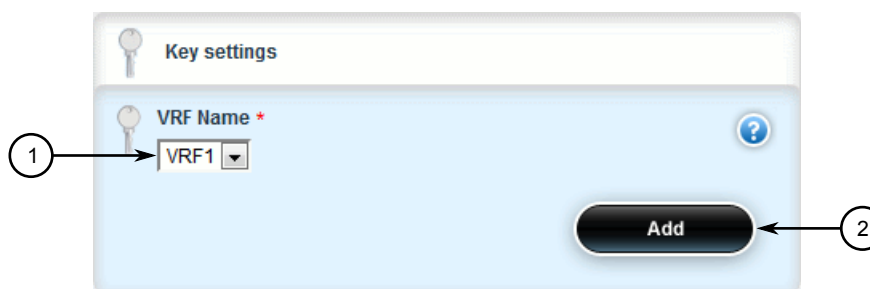
If no IPv4 address families have been configured, add them as needed. For more information, refer to [Section 5.21.10.2, “Adding an IPv4 Address Family”](#).

#### Section 5.21.10.2

### Adding an IPv4 Address Family

To add an IPv4 address family, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » ipv4** and click **<Add vrf>**. The **Key Settings** form appears.



The image shows a web interface titled "Key settings". It contains a dropdown menu labeled "VRF Name \*" with the value "VRF1" selected. A circled number "1" points to the dropdown menu. A circled number "2" points to an "Add" button located at the bottom right of the form.

**Figure 621: Key Settings Form**

1. VRF Name List 2. Add Button

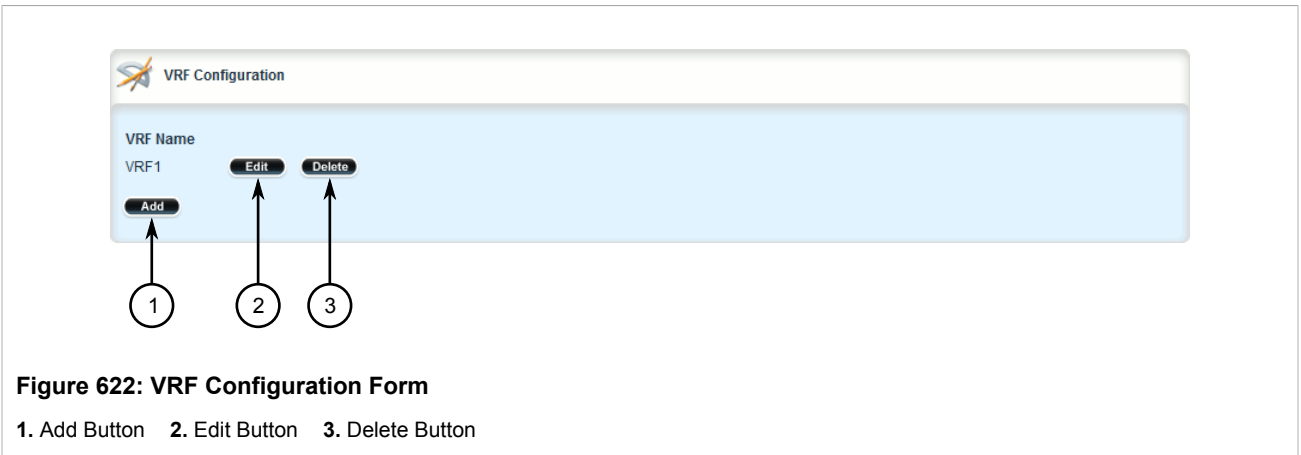
3. Select the desired VRF and then click **Add**. The **Route Map** and **Neighbor** forms appear.
4. Add one or more neighbors. For more information, refer to [Section 5.21.12.2, “Adding a Neighbor”](#).
5. Add one or more redistributions. For more information, refer to [Section 5.21.11.2, “Adding a Redistribution”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.21.10.3

### Deleting an IPv4 Address Family

To delete an IPv4 address family, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » ipv4**. The **VRF Configuration** form appears.



**Figure 622: VRF Configuration Form**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen IPv4 address family.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.21.11

## 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.

The following sections describe how to configure and manage redistribution for IPv4 address families:

- [Section 5.21.11.1, “Viewing a List of Redistributions”](#)
- [Section 5.21.11.2, “Adding a Redistribution”](#)
- [Section 5.21.11.3, “Deleting a Redistribution”](#)

#### Section 5.21.11.1

### Viewing a List of Redistributions

To view a list of redistributions defined for an IPv4 address family, navigate to **routing » dynamic » bgp » address-family » ipv4 » {vrf} » redistribute**, where {vrf} is the chosen VRF instance. If redistributions have been configured, the **Redistribute Route from Other Protocols** table appears.



Source	Metric	Route Map
connected	not found	not found
ospf	not found	not found
static	not found	not found

Figure 623: Redistribute Route from Other Protocols Table

If no redistributions have been configured, add them as needed. For more information, refer to [Section 5.21.11.2, “Adding a Redistribution”](#).

Section 5.21.11.2  
**Adding a Redistribution**

To add a redistribution for an IPv4 address family, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *routing » dynamic » bgp » address-family » ipv4 » {vrf} » redistribute*, where {vrf} is the chosen VRF instance.
3. Click **<Add redistribute>**. The **Key Settings** form appears.

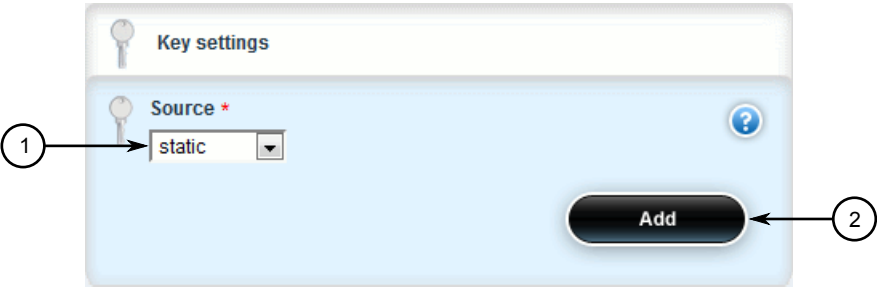
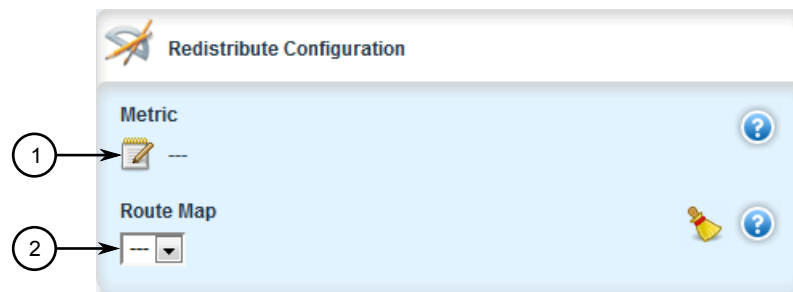


Figure 624: Key Settings Form  
1. Redistribute Route From List    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
source	<b>Synopsis:</b> { connected, ospf, static } Protocol that is source of VRF information. Mandatory field.

5. Click **Add** to add the redistribution. The **Redistribute Configuration** form appears.



**Figure 625: Redistribute Configuration Form**

1. Metric Box

6. Configure the following parameter(s) as required:

Parameter	Description
metric	<b>Synopsis:</b> An integer between 0 and 4294967295 The metric for redistributed routes.
Route Map	The route map name.

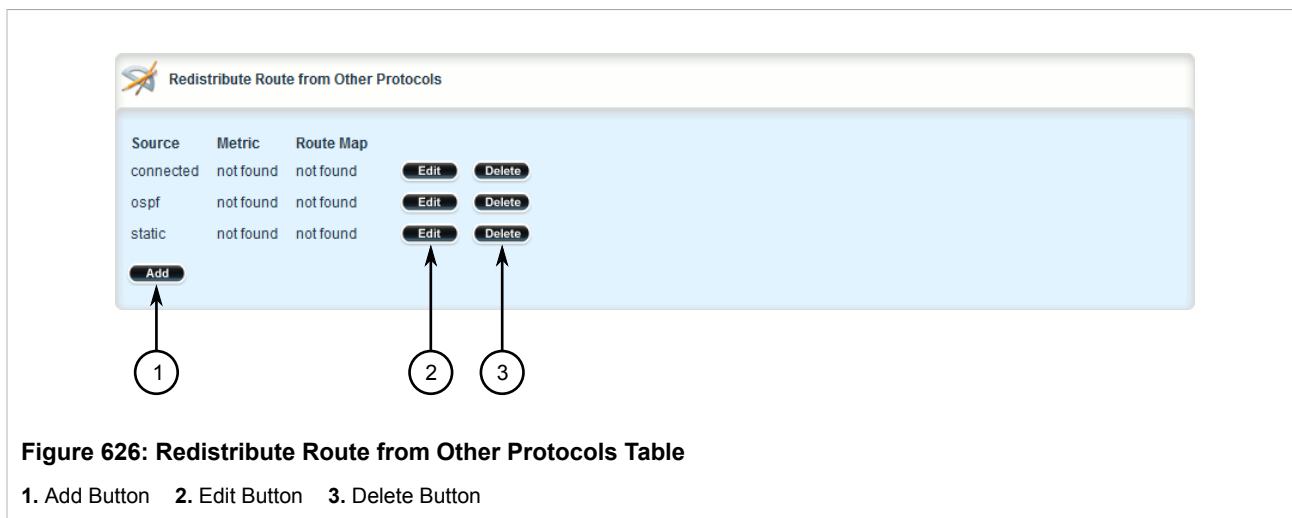
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.21.11.3

## Deleting a Redistribution

To delete a redistribution defined for an IPv4 address family, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » ipv4 » {vrf} » redistribute**, where {vrf} is the chosen VRF instance. The **Redistribute Route from Other Protocols** table appears.



3. Click **Delete** next to the chosen redistribution.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.21.12

## 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.

The following sections describe how to configure and manage neighbors for VRF:

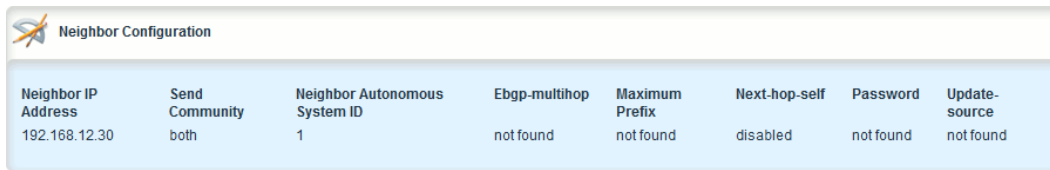
- [Section 5.21.12.1, “Viewing a List of Neighbors”](#)
- [Section 5.21.12.2, “Adding a Neighbor”](#)
- [Section 5.21.12.3, “Configuring the Distribution of Prefix Lists”](#)
- [Section 5.21.12.4, “Tracking Commands”](#)
- [Section 5.21.12.5, “Deleting a Neighbor”](#)

#### Section 5.21.12.1

### Viewing a List of Neighbors

To view a list of neighbors configured for an IPv4 address family, navigate to **routing » dynamic » bgp » address-family » ipv4 » {vrf} » neighbor**, where {vrf} is the chosen VRF instance. If neighbors have been configured, the **Neighbor Configuration** table appears.





Neighbor IP Address	Send Community	Neighbor Autonomous System ID	Ebgp-multi-hop	Maximum Prefix	Next-hop-self	Password	Update-source
192.168.12.30	both	1	not found	not found	disabled	not found	not found

**Figure 627: Neighbor Configuration Table**

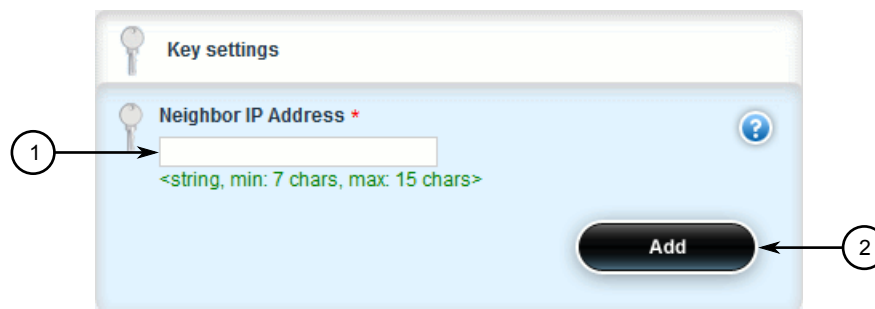
If no neighbors have been configured, add neighbors as needed. For more information, refer to [Section 5.21.12.2, “Adding a Neighbor”](#).

### Section 5.21.12.2

## Adding a Neighbor

To add a new neighbor to an IPv4 address family, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » ipv4 » {vrf} » neighbor**, where {vrf} is the chosen VRF instance.
3. Click **<Add neighbor>**. The **Key Settings** form appears.



The image shows a web form titled "Key settings" with a key icon. Below the title is a section for "Neighbor IP Address \*". It contains a text input box with a blue question mark icon to its right. Below the input box is the text "<string, min: 7 chars, max: 15 chars>". To the right of the input box is a dark blue button labeled "Add". Numbered callouts point to the input box (1) and the "Add" button (2).

**Figure 628: Key Settings Form**

1. Neighbor IP Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	<b>Synopsis:</b> A string 7 to 15 characters long The BGP VRF neighbor IP address.

5. Click **Add** to add the address. The **Neighbor Configuration** and **Route Map** forms appear.

The image shows a 'Neighbor Configuration' form with the following fields and callouts:

- 1** points to the 'Send Community' dropdown menu, which is currently set to 'both'.
- 2** points to the 'Neighbor Autonomous System ID' text input box.
- 3** points to the 'Ebgp-multihop' field, which has a configuration icon and a value of '---'.
- 4** points to the 'Maximum Prefix' field, which has a configuration icon and a value of '---'.
- 5** points to the 'Next-hop-self' checkbox, which is currently checked and labeled 'Enabled'.
- 6** points to the 'Password' field, which has a configuration icon and a value of '---'.
- 7** points to the 'Update-source' field, which has a configuration icon and a value of '---'.
- 8** points to the 'Disable-connected-check' checkbox, which is currently checked and labeled 'Enabled'.
- 9** points to the 'Soft-reconfiguration' checkbox, which is currently checked and labeled 'Enabled'.
- 10** points to the 'Weight' field, which has a configuration icon and a value of '---'.

**Figure 629: Neighbor Configuration Form**

1. Send Community List   2. Neighbor Autonomous System ID Box   3. Ebgp-multihop Box   4. Maximum Prefix Box   5. Next-hop-self Box   6. Password Box   7. Update-source Box   8. Disable-connected-check Check Box   9. Soft-reconfiguration Check Box   10. Weight Box

The screenshot shows the 'Neighbor Configuration' form with the following fields and callouts:

- 1. Send Community: A dropdown menu with 'both' selected.
- 2. Neighbor Autonomous System ID: A text input field with a red asterisk and a range constraint '<unsignedInt, 1 .. 65535>'.
- 3. Ebgp-multihop: A text input field with a red asterisk and a range constraint '<unsignedInt, 1 .. 255>'.
- 4. Maximum Prefix: A text input field with a red asterisk and a range constraint '<unsignedInt, 1 .. 65535>'.
- 5. Next-hop-self: A checkbox labeled 'Enabled'.
- 6. Password: A text input field with a red asterisk and a range constraint '<string, 1 .. 65535>'.
- 7. Update-source: A text input field with a red asterisk and a range constraint '<string, 1 .. 65535>'.
- 8. Disable-connected-check: A checkbox labeled 'Enabled'.
- 9. Soft-reconfiguration: A checkbox labeled 'Enabled'.
- 10. Weight: A text input field with a red asterisk and a range constraint '<unsignedInt, 1 .. 65535>'.

**Figure 630: Route Maps Form**  
1. In List   2. Out List

6. On the **Neighbor Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Send Community	<b>Synopsis:</b> { standard, extended, both, none } <b>Default:</b> both Identifies the send Community. Default is both.
Neighbor Autonomous System ID	<b>Synopsis:</b> An integer between 1 and 65535 A BGP neighbor.
ebgp-multihop	<b>Synopsis:</b> An integer between 1 and 255 The maximum hop count. This allows EBGp neighbors not on directly connected networks.

Parameter	Description
Maximum Prefix	<b>Synopsis:</b> An integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
next-hop-self	<b>Synopsis:</b> typeless Disables the next hop calculation for this neighbor.
password	<b>Synopsis:</b> A string 1 to 1024 characters long Password.
update-source	<b>Synopsis:</b> A string 7 to 15 characters long Source IP address of routing updates.
disable-connected-check	<b>Synopsis:</b> typeless Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
soft-reconfiguration	<b>Synopsis:</b> typeless Per neighbor soft reconfiguration.
weight	The default weight for routes from this neighbor.

- On the **Route Maps** form, configure the following parameter(s) as required:

Parameter	Description
in	Apply route map to incoming routes.
out	Apply route map to outbound routes.

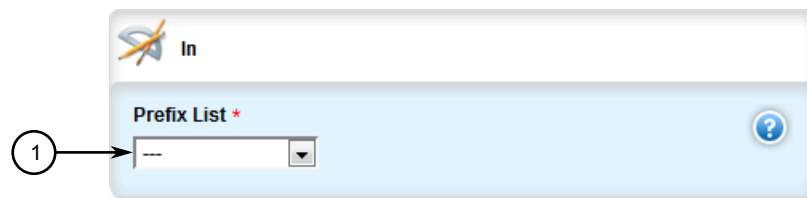
- Configure the prefix list distribution. For more information, refer to [Section 5.21.12.3, “Configuring the Distribution of Prefix Lists”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.21.12.3

## Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in an IPv4 address family, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Make sure the desired prefix list is configured for the BGP network. For more information, refer to [Section 5.18.5.3, “Adding a Prefix List”](#).
- Navigate to **routing » dynamic » bgp » address-family » ipv4 » {vrf} » neighbor » {address} » distribute-prefix-list**, where {vrf} is the chosen VRF instance and {address} is the IP address of the neighbor.
- Click the **+** symbol in the menu next to either **in** or **out**, depending on the direction of the route (incoming or outbound). The **In** or **Out** form appears.



**Figure 631: In Form (Example)**

1. Prefix List

5. Select the desired prefix list.
6. If necessary, configure an event tracker to track network commands. For more information, refer to [Section 5.21.12.4, “Tracking Commands”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.21.12.4

### Tracking Commands

Network commands can be tracked using event trackers configured under **global » tracking**. For more information about event trackers, refer to [Section 3.17, “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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure a prefix list distribution path has been configured. For more information, refer to [Section 5.19.8, “Managing the Prefix List Distribution”](#).
3. 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.
4. Click the **+** symbol in the menu next to **track**. The **Track** form appears

**Figure 632: Track Form**

1. Event List   2. Apply When List

5. Configure the following parameter(s) as required:

Parameter	Description
event	Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state.
apply-when	<b>Synopsis:</b> { up, down } <b>Default:</b> up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

6. Click **Add** to create the tracker.
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.21.12.5

### Deleting a Neighbor

To delete a VPNv4 neighbor, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » dynamic » bgp » address-family » ipv4 » {vrf} » neighbor**, where {vrf} is the chosen VRF instance. The **Neighbor Configuration** table appears.

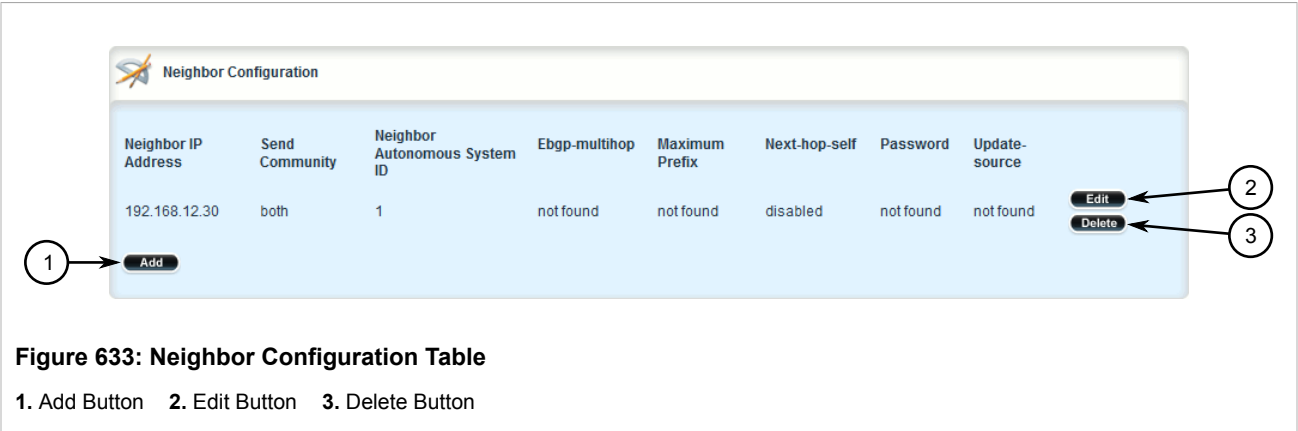


Figure 633: Neighbor Configuration Table

1. Add Button    2. Edit Button    3. Delete Button

- 3. Click **Delete** next to the chosen neighbor.
- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

Section 5.21.13

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.

The following sections describe how to configure and manage static routes for VRF-Lite:

- [Section 5.21.13.1, “Viewing a List of Static VRF Routes”](#)
- [Section 5.21.13.2, “Adding a Static VRF Route”](#)
- [Section 5.21.13.3, “Configuring a Black Hole Connection for a Static VRF Route”](#)
- [Section 5.21.13.4, “Deleting a Static VRF Route”](#)

Section 5.21.13.1

Viewing a List of Static VRF Routes

To view a list of static IPv4 routes configured for a VRF instance, navigate to **routing » static » vrf » {vrf} » ipv4**, where *vrf* is the chosen VRF instance. If routes have been configured, the **VRF Static Route** table appears.

Subnet (network/prefix)	HW Accelerate
192.168.10.0/24	disabled

Figure 634: VRF Static Route Table

If no static routes have been configured, add routes as needed. For more information, refer to [Section 5.21.13.2, “Adding a Static VRF Route”](#).

### Section 5.21.13.2

## Adding a Static VRF Route

To add an IPv4 static route for a VRF instance, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » vrf** and click **<Add vrf>**. The **Key Settings** form appears.

**Figure 635: Key Settings Form**

1. VRF Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	The VRF name.

4. In the menu, click **ipv4** and then click **<Add route>**. The **Key Settings** form appears.

**Figure 636: Key Settings Form**

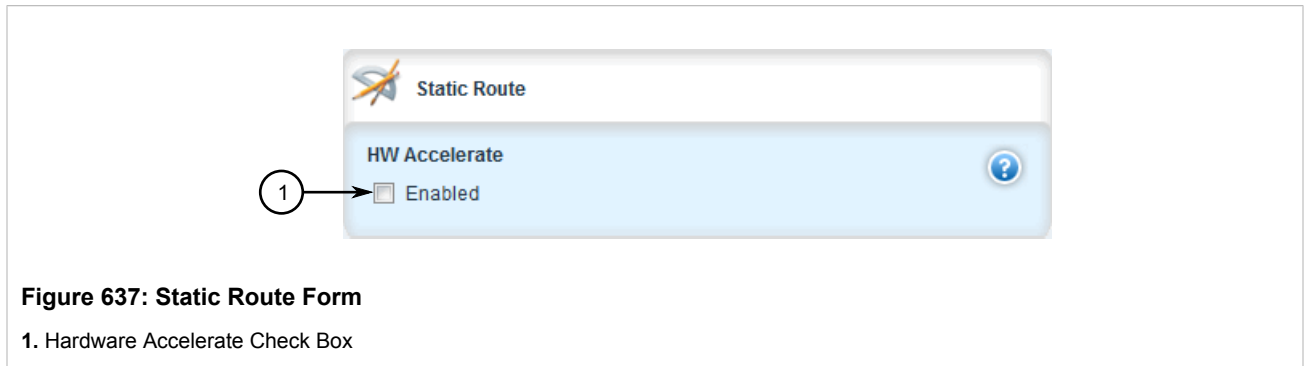
1. Subnet (Network/Prefix) Box    2. Add Button

5. Configure the following parameter(s) as required:



Parameter	Description
Subnet (network/prefix)	<b>Synopsis:</b> A string 9 to 18 characters long The subnet (network/mask) of the static route.

6. Click **Add** to add the route. If the device has a Layer 3 switch installed, the **Static Route** form appears.



7. 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	<b>Synopsis:</b> typeless 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.

8. If necessary, configure a black hole connection for the static route. For more information, refer to [Section 5.21.13.3, “Configuring a Black Hole Connection for a Static VRF Route”](#).
9. If necessary, add gateways for the static route. For more information, refer to [Section 5.21.14.2, “Adding a Gateway for a Static VRF Route”](#).
10. If necessary, add interfaces for the static route. For more information, refer to [Section 5.21.15.2, “Adding a Gateway for a Static VRF Route”](#).
11. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
12. Click **Exit Transaction** or continue making changes.

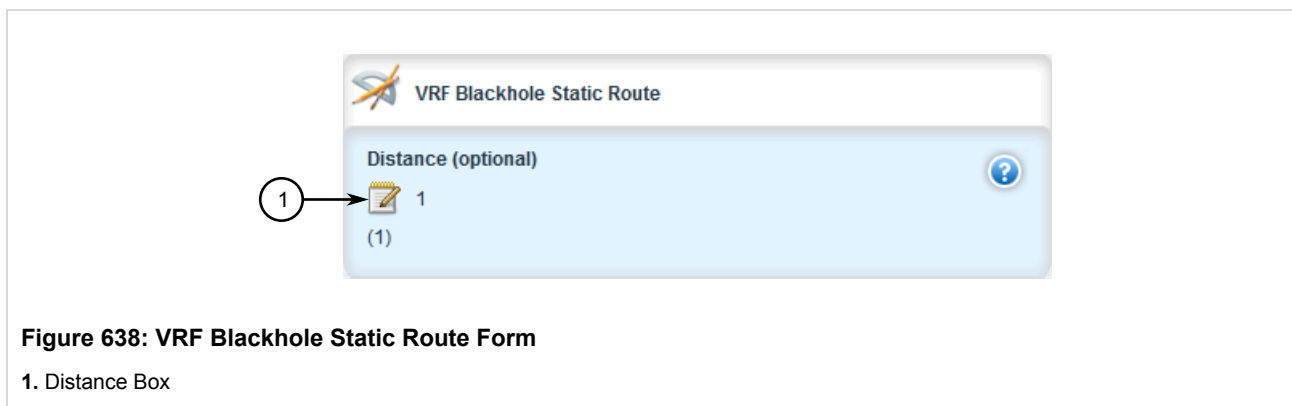
## Section 5.21.13.3

**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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet}**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route.

- Click the **+** symbol in the menu next to *blackhole*. The **VRF Blackhole Static Route** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1 The distance for this static route's blackhole. Default is 1.

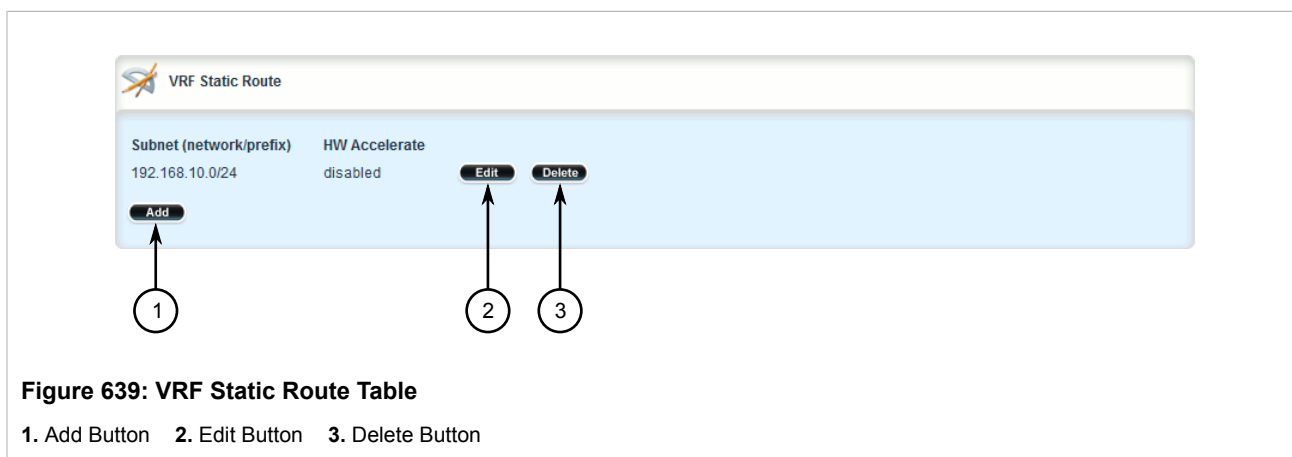
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.21.13.4

### Deleting a Static VRF Route

To delete an IPv4 static route configured for a VRF instance, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » static » vrf » {vrf} » ipv4**, where *vrf* is the chosen VRF instance. The **VRF Static Route** table appears.



- Click **Delete** next to the chosen route.

- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

Section 5.21.14

# Managing Gateways for Static VRF Routes


The following sections describe how to configure and manage gateways for static VRF routes:

- [Section 5.21.14.1, “Viewing a List of Gateways for Static VRF Routes”](#)
- [Section 5.21.14.2, “Adding a Gateway for a Static VRF Route”](#)
- [Section 5.21.14.3, “Deleting a Gateway for a Static VRF Route”](#)

Section 5.21.14.1

## Viewing a List of Gateways for Static VRF Routes

To view a list of gateway addresses assigned to a static VRF route, navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet} » via**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route. The **VRF Static Route Using Gateway** table appears.



VRF Static Route Using Gateway	
Gateway Address	Distance (optional)
1.9.5.1	not found

Figure 640: VRF Static Route Using Gateway Table

If no gateway addresses have been configured, add addresses as needed. For more information, refer to [Section 5.21.14.2, “Adding a Gateway for a Static VRF Route”](#).

Section 5.21.14.2

## Adding a Gateway for a Static VRF Route

To add a gateway address for a static VRF route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet} » via**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route.
3. Click **<Add via>**. The **Key Settings** form appears.

**Figure 641: Key Settings Form**

1. Gateway Address Box 2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	<b>Synopsis:</b> A string 7 to 15 characters long The gateway for the static route.

5. Click **Add** to add the gateway address. The **Static VRF Route Using Gateway** form appears.

**Figure 642: Static VRF Route Using Gateway Form**

1. Distance Box

6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

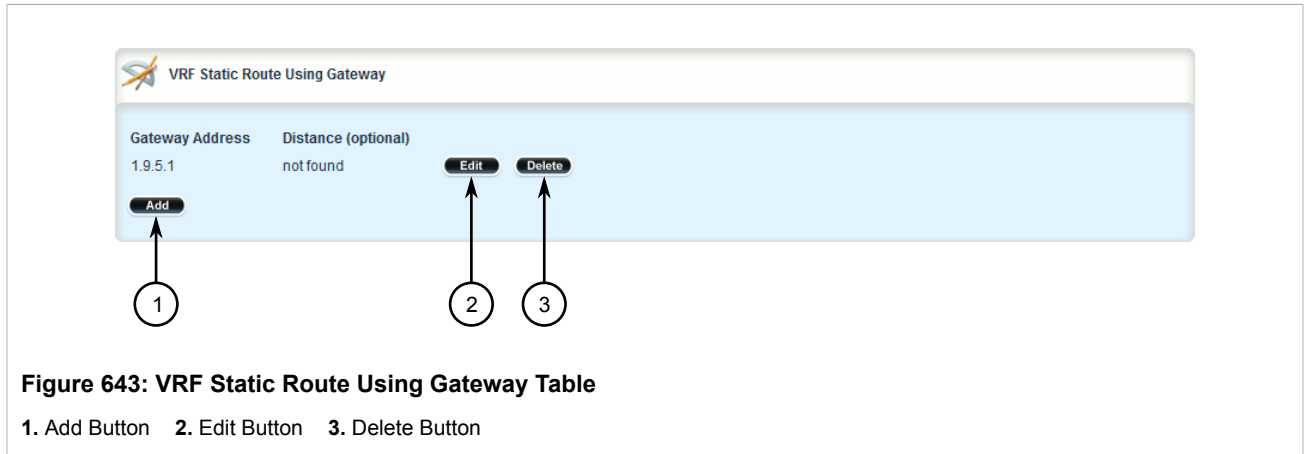
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.21.14.3

### Deleting a Gateway for a Static VRF Route

To delete a gateway address assigned to a static VRF route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet} » via**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route. The **VRF Static Route Using Gateway** table appears.



3. Click **Delete** next to the chosen gateway address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.21.15

## Managing Interfaces for Static VRF Routes

The following sections describe how to configure and manage interfaces for static VRF routes:

- [Section 5.21.15.1, “Viewing a List of Gateways for Static VRF Routes”](#)
- [Section 5.21.15.2, “Adding a Gateway for a Static VRF Route”](#)
- [Section 5.21.15.3, “Deleting a Gateway for a Static VRF Route”](#)

## Section 5.21.15.1

### Viewing a List of Gateways for Static VRF Routes

To view a list of interfaces assigned to a static VRF route, navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet} » dev**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route. The **VRF Static Route Using Interface** table appears.

**VRF Static Route Using Interface**

Interface Name	Distance (optional)
fe-cm-1	not found

**Figure 644: VRF Static Route Using Interface Table**

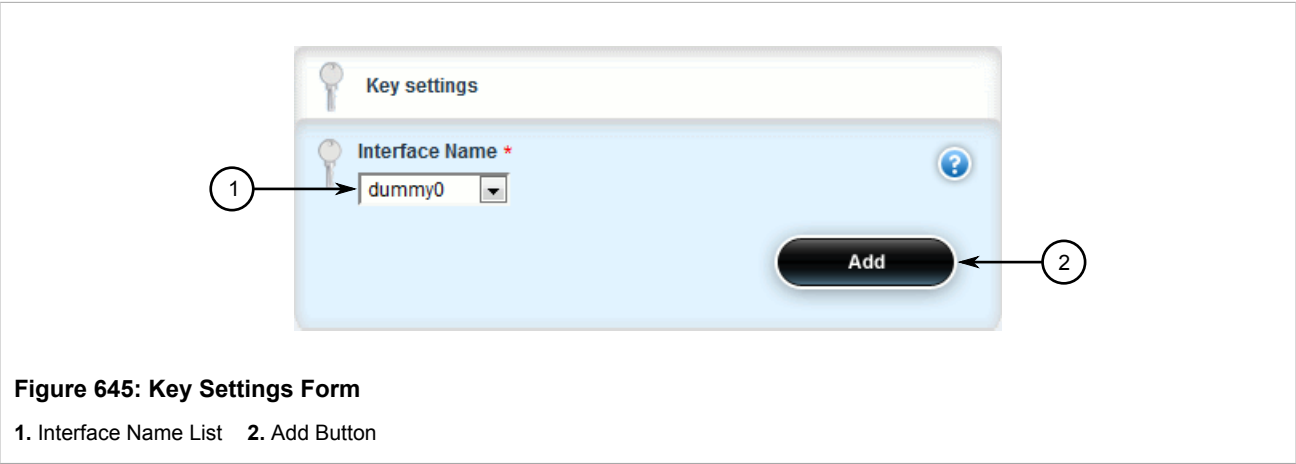
If no gateway addresses have been configured, add addresses as needed. For more information, refer to [Section 5.21.15.2, “Adding a Gateway for a Static VRF Route”](#).

Section 5.21.15.2

**Adding a Gateway for a Static VRF Route**

To add an interface for an static VRF route, do the following:

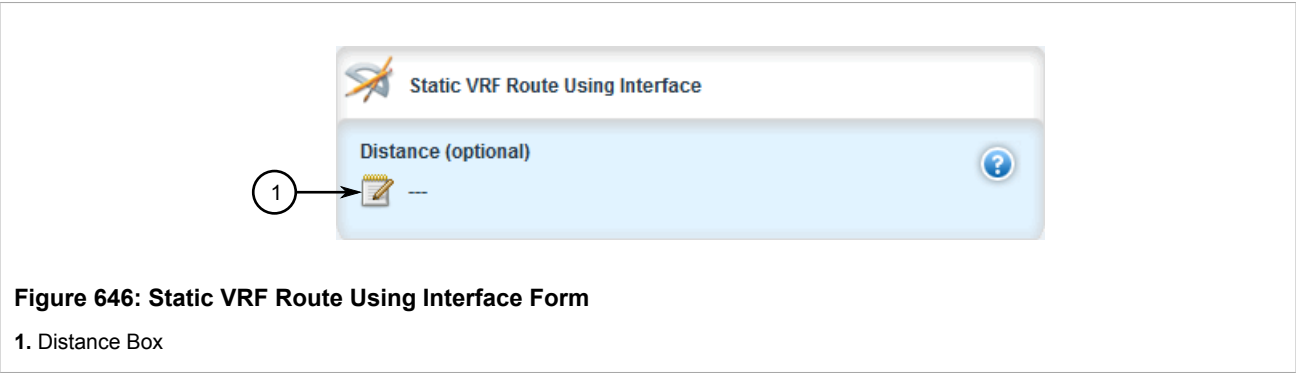
1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet} » dev**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route.
3. Click **<Add dev>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	The interface for the static route.

5. Click **Add** to add the interface. The **Static VRF Route Using Interface** form appears.



6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255

Parameter	Description
	The distance for the static route.

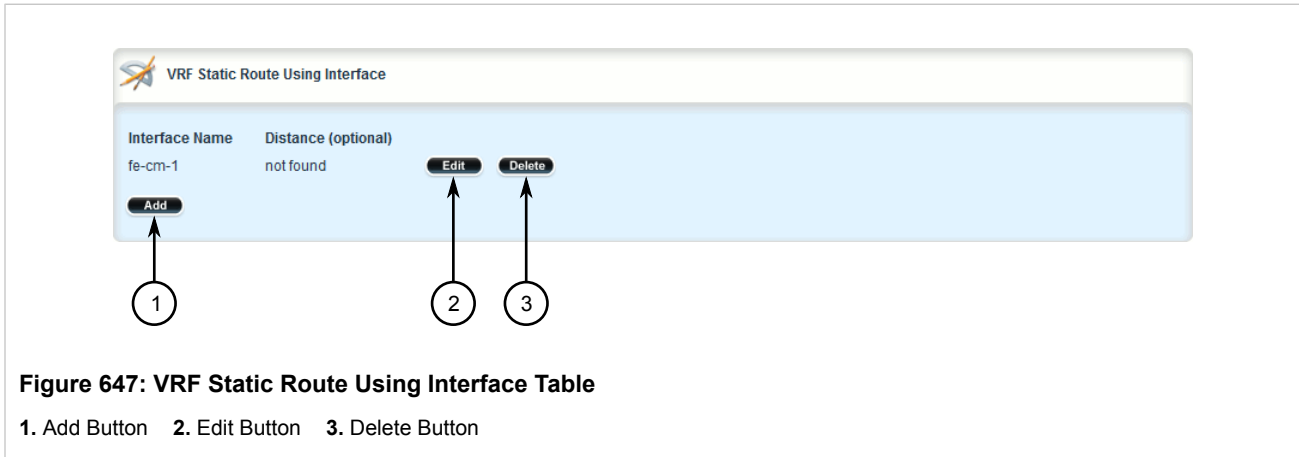
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.21.15.3

Deleting a Gateway for a Static VRF Route

To delete an interface assigned to a static VRF route, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » static » vrf » {vrf} » ipv4 » {subnet} » dev**, where *vrf* is the chosen VRF instance and *{subnet}* is the subnet (network/prefix) of the static route. The **VRF Static Route Using Interface** table appears.



- Click **Delete** next to the chosen interface.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.22

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.

The following sections describe how to configure and manage static routes:

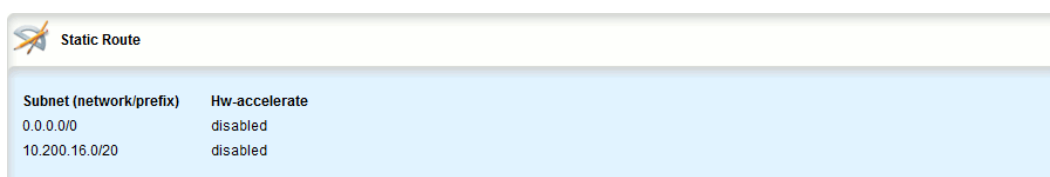
- Section 5.22.1, "Viewing a List of Static Routes"
- Section 5.22.2, "Adding an IPv4 Static Route"
- Section 5.22.3, "Adding an IPv6 Static Route"

- [Section 5.22.4, “Deleting a Static Route”](#)
- [Section 5.22.5, “Configuring a Black Hole Connection for an IPv4 Static Route”](#)
- [Section 5.22.6, “Managing Gateways for Static Routes”](#)
- [Section 5.22.7, “Managing Interfaces for Static Routes”](#)

### Section 5.22.1

## Viewing a List of Static Routes

To view a list of static routes configured on the device, navigate to **routing » static » {protocol}**, where *{protocol}* is either *IPv4* or *IPv6*. If routes have been configured, the **Static Route** table appears.



Subnet (network/prefix)	Hw-accelerate
0.0.0.0/0	disabled
10.200.16.0/20	disabled

**Figure 648: Static Route Table**

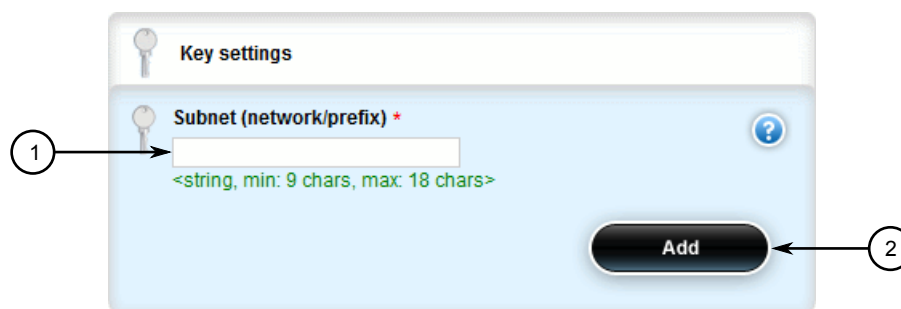
If no static routes have been configured, add routes as needed. For more information, refer to [Section 5.22.2, “Adding an IPv4 Static Route”](#) or [Section 5.22.3, “Adding an IPv6 Static Route”](#).

### Section 5.22.2

## Adding an IPv4 Static Route

To add an IPv4 static route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » ipv4** and click **<Add route>**. The **Key Settings** form appears.



The screenshot shows the 'Key settings' form for adding a static route. A circled '1' with an arrow points to the 'Subnet (network/prefix) \*' input field, which has a placeholder text '<string, min: 9 chars, max: 18 chars>'. A circled '2' with an arrow points to the 'Add' button at the bottom right of the form.

**Figure 649: Key Settings Form**

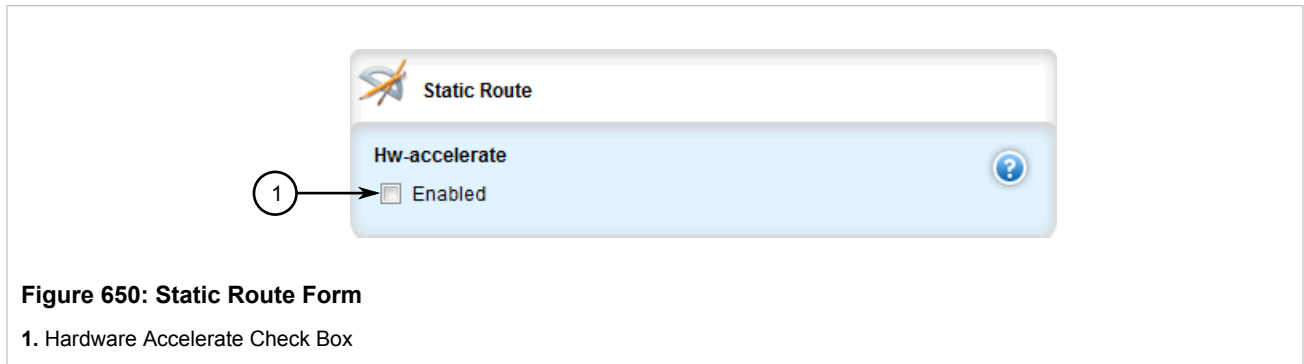
1. Subnet (Network/Prefix) Box    2. Add Button

3. Configure the following parameter(s) as required:



Parameter	Description
Subnet (network/prefix)	<b>Synopsis:</b> A string 9 to 18 characters long The subnet (network/mask) of the static route.

- Click **Add** to add the route. If the device has a Layer 3 switch installed, the **Static Route** form appears.



- 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	<b>Synopsis:</b> typeless 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.

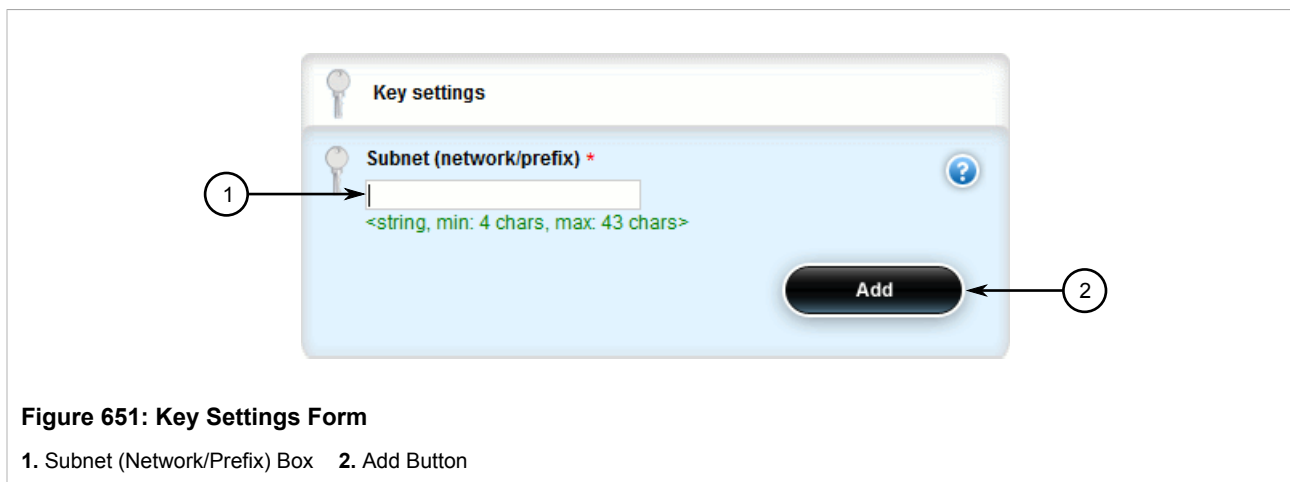
- If necessary, configure a black hole connection for the static route. For more information, refer to [Section 5.22.5, “Configuring a Black Hole Connection for an IPv4 Static Route”](#).
- If necessary, add gateways for the static route. For more information, refer to [Section 5.22.6.3, “Adding a Gateway for an IPv4 Static Route”](#).
- If necessary, add interfaces for the static route. For more information, refer to [Section 5.22.7.3, “Adding an Interface for an IPv4 Static Route”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.22.3

## Adding an IPv6 Static Route

To add an IPv6 static route, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » static » ipv6** and click **<Add route>**. The **Key Settings** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Subnet (network/prefix)	<b>Synopsis:</b> A string 4 to 43 characters long The subnet (network/mask) of the static route.

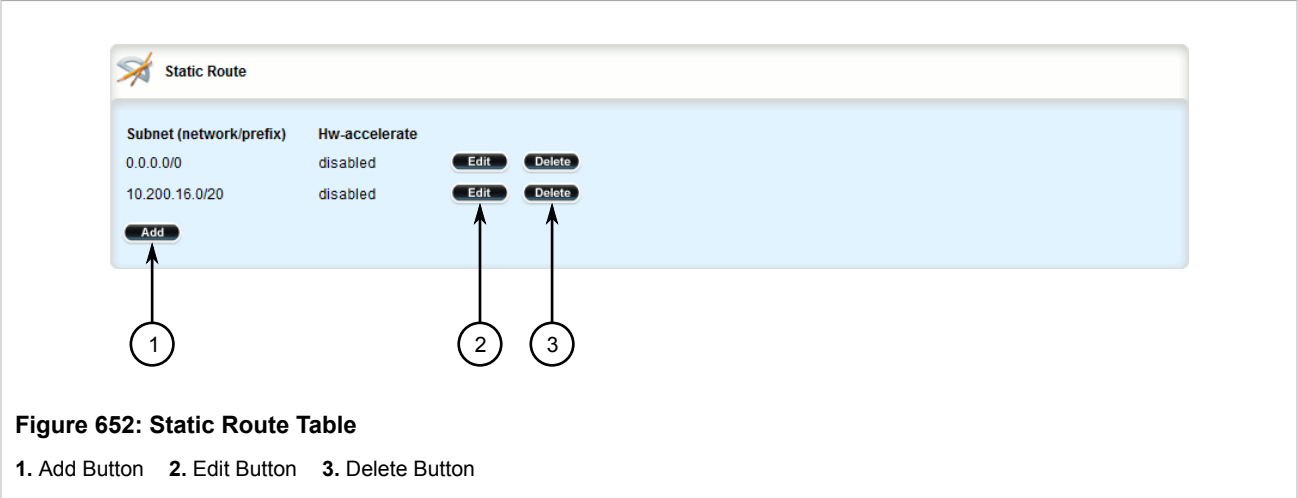
- Click **Add** to add the route.
- If necessary, configure either a gateway or an interface for the static route. Only one can be configured per static route. For more informatoin, refer to [Section 5.22.6.1, “Configuring Gateways for IPv6 Static Routes”](#) or [Section 5.22.7.1, “Configuring Interfaces for IPv6 Static Routes”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.22.4

## Deleting a Static Route

To delete a static route, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » static » {protocol}**, where *{protocol}* is either *IPv4* or *IPv6*. The **Static Route** table appears.



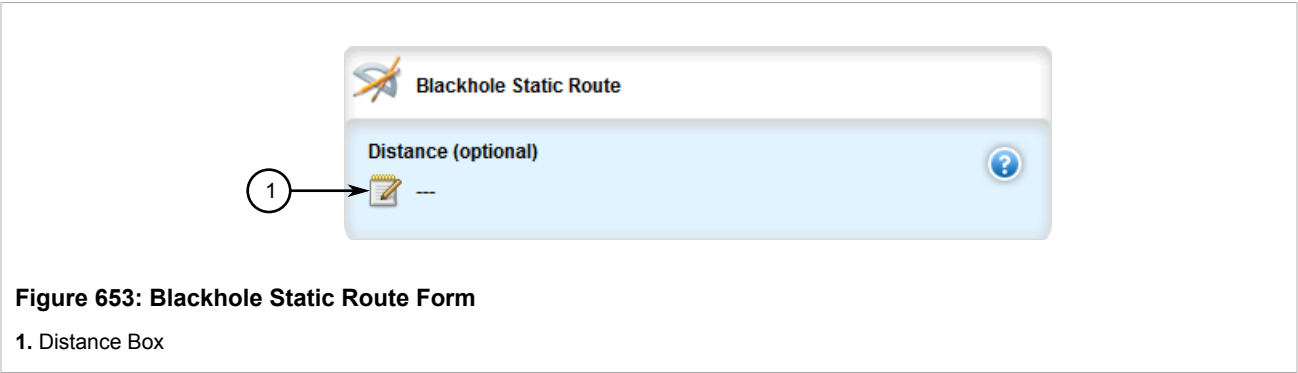
- 3. Click **Delete** next to the chosen route.
- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

Section 5.22.5

# 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. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to **routing » static » ipv4 » {subnet}**, where *subnet* is the subnet (network/prefix) of the static route.
- 3. Click the **+** symbol in the menu next to *blackhole*. The **Blackhole Static Route** form appears.



- 4. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1

Parameter	Description
	The distance for this static route's blackhole. Default is 1.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.22.6

## Managing Gateways for Static Routes

The following sections describe how to configure and manage gateways for static routes:

- [Section 5.22.6.1, “Configuring Gateways for IPv6 Static Routes”](#)
- [Section 5.22.6.2, “Viewing a List of Gateways for IPv4 Static Routes”](#)
- [Section 5.22.6.3, “Adding a Gateway for an IPv4 Static Route”](#)
- [Section 5.22.6.4, “Deleting a Gateway for an IPv4 Static Route”](#)

## Section 5.22.6.1

### Configuring Gateways for IPv6 Static Routes

To configure a gateway address for an IPv6 static route, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » static » ipv6 » {subnet}**, where *subnet* is the subnet (network/prefix) of the static route.
- Click the **+** symbol in the menu next to *via*. The **Static Route Using Gateway** form appears

**Figure 654: Static Route Using Gateway Form**

1. Gateway Address Box    2. Distance Box

- Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	<b>Synopsis:</b> A string 6 to 40 characters long

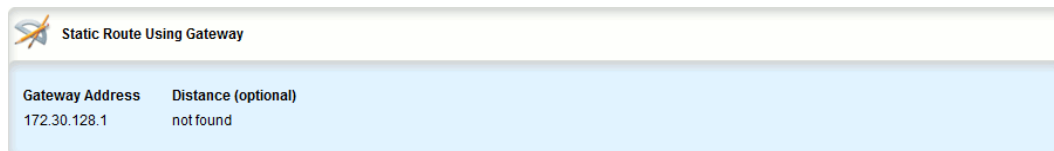
Parameter	Description
	The gateway for the static route.
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.22.6.2

## Viewing a List of Gateways for IPv4 Static Routes

To view a list of gateway addresses assigned to an IPv4 static route, navigate to **routing » static » ipv4 » {subnet} » via**, where *subnet* is the subnet (network/prefix) of the static route. If addresses have been configured, the **Static Route Using Gateway** table appears.



Static Route Using Gateway	
Gateway Address	Distance (optional)
172.30.128.1	not found

**Figure 655: Static Route Using Gateway Table**

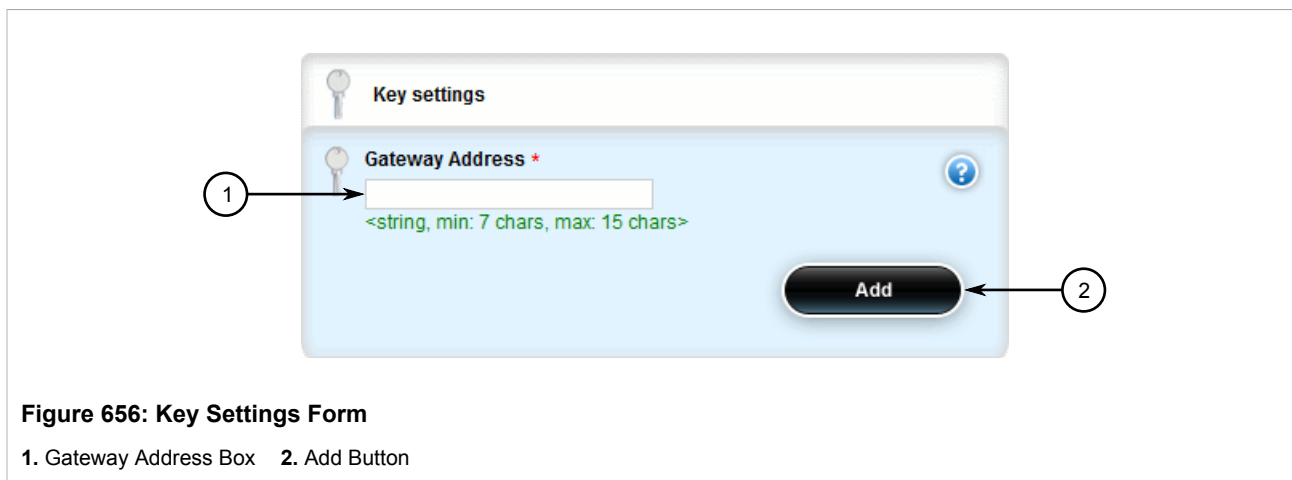
If no gateway addresses have been configured, add addresses as needed. For more information, refer to [Section 5.22.6.3, “Adding a Gateway for an IPv4 Static Route”](#).

## Section 5.22.6.3

## Adding a Gateway for an IPv4 Static Route

To add a gateway address for an IPv4 static route, do the following:

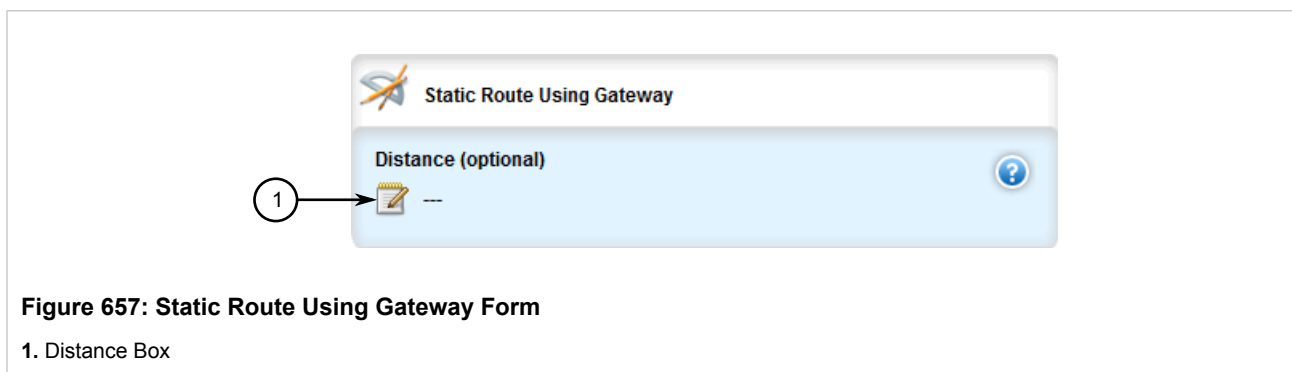
- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **routing » static » ipv4 » {subnet} » via**, where *subnet* is the subnet (network/prefix) of the static route.
- Click **<Add via>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	<b>Synopsis:</b> A string 7 to 15 characters long The gateway for the static route.

5. Click **Add** to add the gateway address. The **Static Route Using Gateway** form appears.



6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

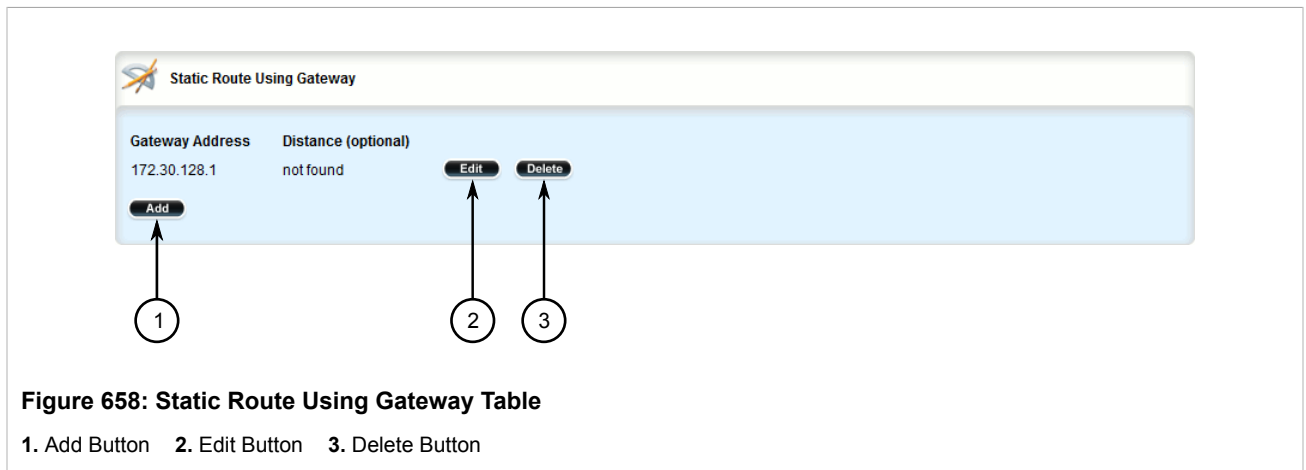
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

#### Section 5.22.6.4

### Deleting a Gateway for an IPv4 Static Route

To delete a gateway for an IPv4 static route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » ipv4 » {subnet} » via**, where *subnet* is the subnet (network/prefix) of the static route. The **Static Route Using Gateway** table appears.



**Figure 658: Static Route Using Gateway Table**

1. Add Button   2. Edit Button   3. Delete Button

3. Click **Delete** next to the chosen gateway address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.22.7

## Managing Interfaces for Static Routes

The following sections describe how to configure and manage interfaces for static routes:

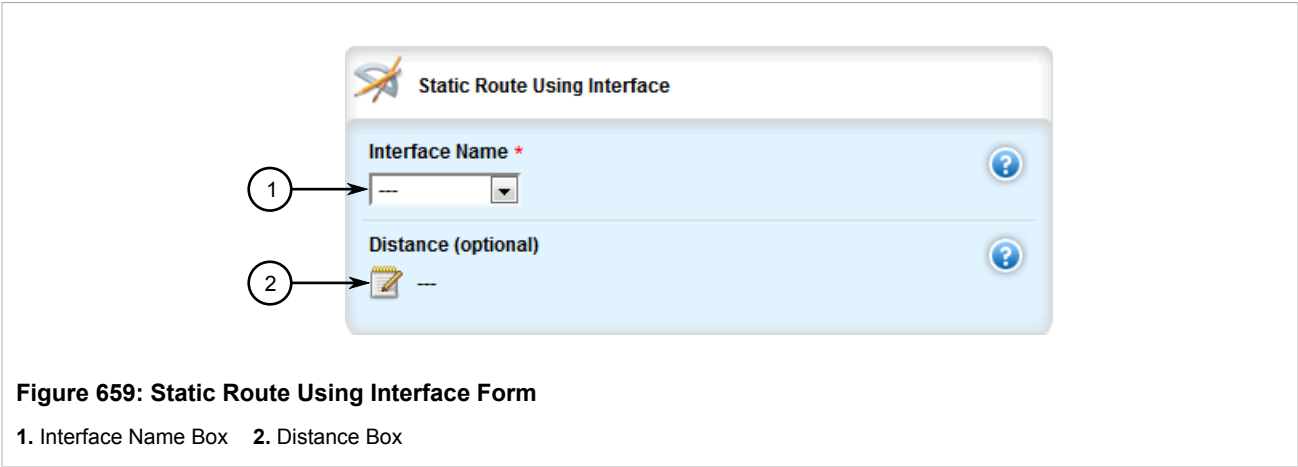
- [Section 5.22.7.1, “Configuring Interfaces for IPv6 Static Routes”](#)
- [Section 5.22.7.2, “Viewing a List of Interfaces for IPv4 Static Routes”](#)
- [Section 5.22.7.3, “Adding an Interface for an IPv4 Static Route”](#)
- [Section 5.22.7.4, “Deleting an Interface for an IPv4 Static Route”](#)

#### Section 5.22.7.1

### Configuring Interfaces for IPv6 Static Routes

To configure an interface for an IPv6 static route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » ipv6 » {subnet}**, where *subnet* is the subnet (network/prefix) of the static route.
3. Click the **+** symbol in the menu next to *dev*. The **Static Route Using Interface** form appears



4. Configure the following parameter(s) as required:

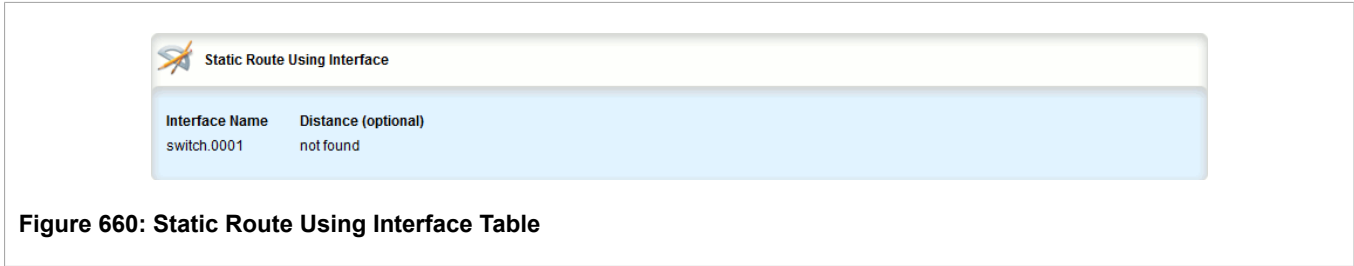
Parameter	Description
Interface Name	The interface for the static route.
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

Section 5.22.7.2

## Viewing a List of Interfaces for IPv4 Static Routes

To view a list of interfaces assigned to an IPv4 static route, navigate to **routing » static » ipv4 » {subnet} » dev**, where *subnet* is the subnet (network/prefix) of the static route. If interfaces have been configured, the **Static Route Using Interface** table appears.



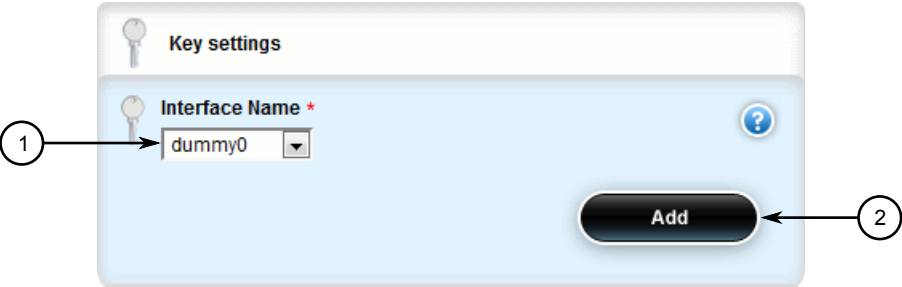
If no interfaces have been configured, add interfaces as needed. For more information, refer to [Section 5.22.7.3, “Adding an Interface for an IPv4 Static Route”](#).



Section 5.22.7.3

Adding an Interface for an IPv4 Static Route

- To add an interface for an IPv4 static route, do the following:
1. Change the mode to **Edit Private** or **Edit Exclusive**.
  2. Navigate to *routing » static » ipv4 » {subnet} » dev*, where *subnet* is the subnet (network/prefix) of the static route.
  3. Click **<Add dev>**. The **Key Settings** form appears.



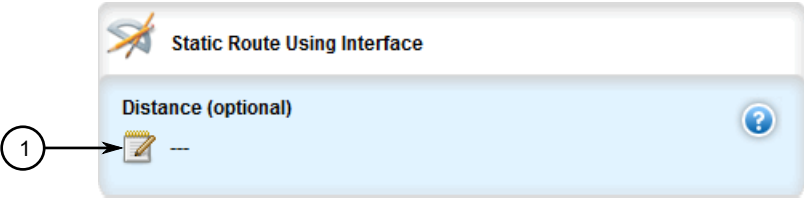
**Figure 661: Key Settings Form**

1. Interface Name Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	The interface for the static route.

5. Click **Add** to add the interface. The **Static Route Using Interface** form appears.



**Figure 662: Static Route Using Interface Form**

1. Distance Box

6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	<b>Synopsis:</b> An integer between 1 and 255 The distance for the static route.

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

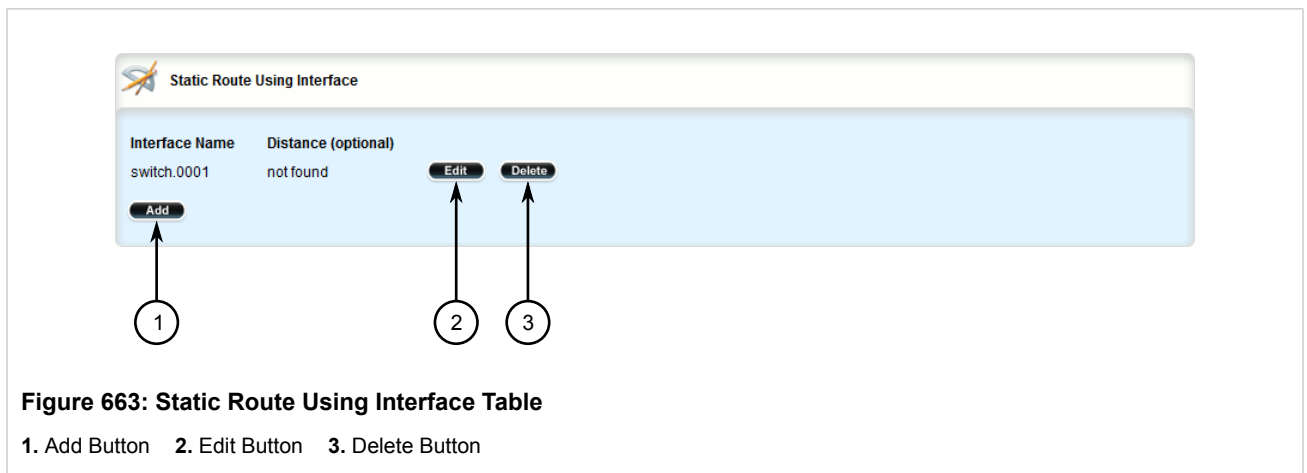
8. Click **Exit Transaction** or continue making changes.

#### Section 5.22.7.4

### Deleting an Interface for an IPv4 Static Route

To delete an interface for an IPv4 static route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » static » ipv4 » {subnet} » dev**, where *subnet* is the subnet (network/prefix) of the static route. The **Static Route Using Interface** table appears.



3. Click **Delete** next to the chosen interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.23

## Managing Static Multicast Routing

The following sections describe how to configure and manage static multicast routing:

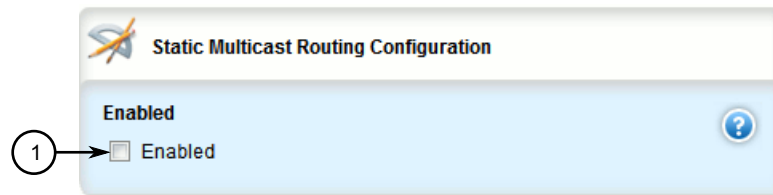
- [Section 5.23.1, “Enabling/Disabling Static Multicast Routing”](#)
- [Section 5.23.2, “Managing Static Multicast Groups”](#)
- [Section 5.23.3, “Managing Out-Interfaces”](#)

#### Section 5.23.1

### Enabling/Disabling Static Multicast Routing

To enable or disable static multicast routing, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » static**. The **Static Multicast Routing Configuration** form appears.



**Figure 664: Static Multicast Routing Configuration Form**

1. Enabled Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
enabled	<b>Synopsis:</b> typeless Enables static multicast routing service <b>Prerequisite:</b> Dynamic and static multicast routing can not be enabled together.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.23.2

## Managing Static Multicast Groups

The following sections describe how to configure and manage static multicast groups:

- [Section 5.23.2.1, “Viewing a List of Static Multicast Groups”](#)
- [Section 5.23.2.2, “Adding a Static Multicast Group”](#)
- [Section 5.23.2.3, “Deleting a Static Multicast Group”](#)

#### Section 5.23.2.1

### Viewing a List of Static Multicast Groups

To view a list of static multicast groups, navigate to **routing » multicast » static » mcast-groups**. If static multicast groups have been configured, the **Multicast Groups Configuration** table appears.

Description	Source-ip	Multicast-ip	In-interface	Hw-accelerate
test.001	169.150.24.12	238.1.12.12	switch.0001	disabled

**Figure 665: Multicast Groups Configuration Table**

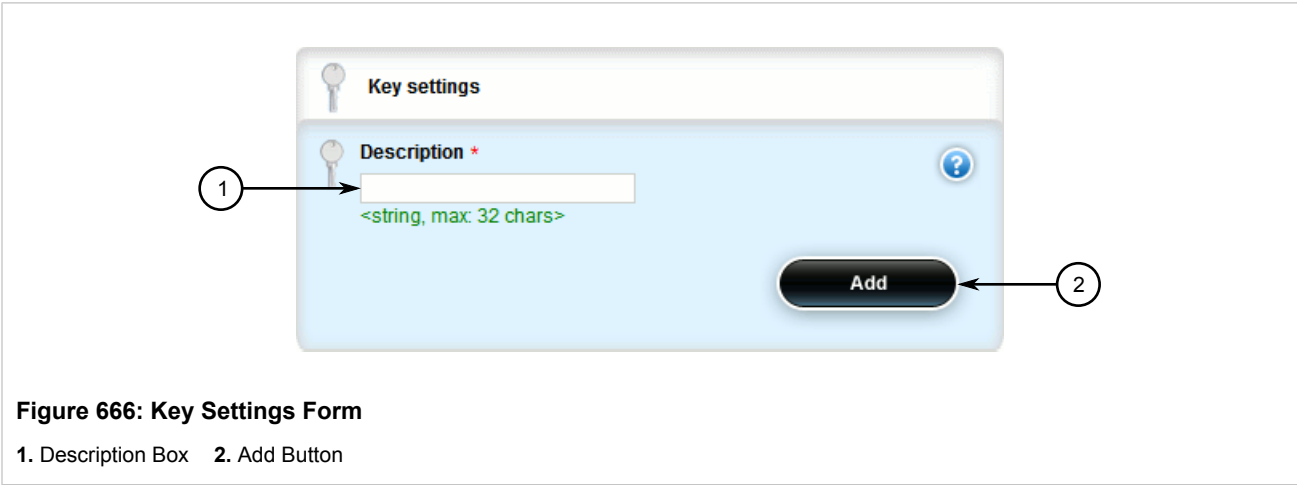
If no static multicast groups have been configured, add groups as needed. For more information about adding static multicast groups, refer to [Section 5.23.2.2, “Adding a Static Multicast Group”](#).

Section 5.23.2.2

Adding a Static Multicast Group

To add a static multicast group, do the following:

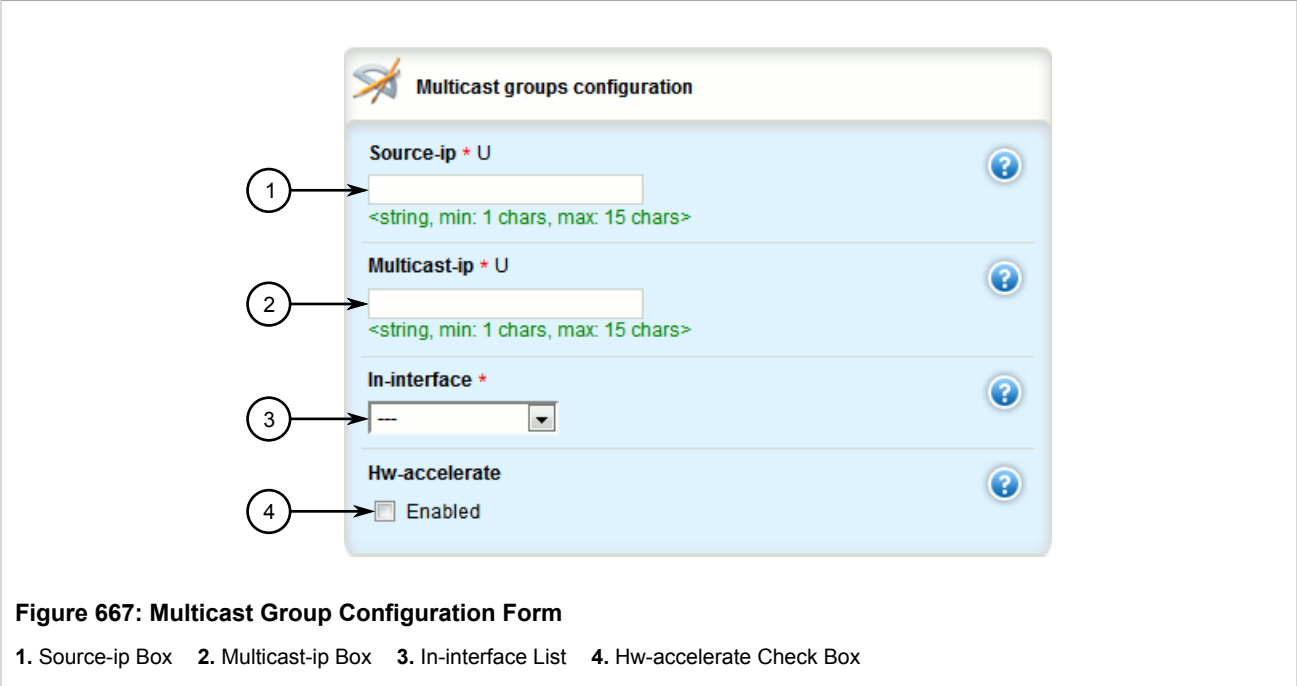
- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *routing » multicast » static » mcast-groups* and click **<Add mcast-groups>**. The **Key settings** form appears.



- 3. Configure the following parameter(s) as required:

Parameter	Description
description	<b>Synopsis:</b> A string 1 to 32 characters long Describes the multicast group, spaces are not allowed.

- 4. Click the **Add** button. The **Multicast Group Configuration** form appears.



5. Configure the following parameter(s) as required:



**NOTE**  
*Only TCP and UDP traffic flows will be accelerated by the IP/Layer 3 switch fabric. Non-IP packet types, such as ICMP and IGMP, will not be accelerated.*

Parameter	Description
source-ip	<b>Synopsis:</b> A string 7 to 15 characters long The expected source IP address of the multicast packet, in the format xxx.xxx.xxx.xxx. This address is uniquely paired with the multicast address. You cannot use this IP address to create another multicast routing entry with a different Multicast-IP address.
multicast-ip	<b>Synopsis:</b> A string 7 to 15 characters long The multicast IP address to be forwarded, in the format xxx.xxx.xxx.xxx. The address must be in the range of 224.0.0.0 to 239.255.255.255. This address is uniquely paired with the source IP address. You cannot use this IP address to create another multicast routing entry with a different Source-IP address.
in-interface	The interface upon which the multicast packet arrives.
hw-accelerate	<b>Synopsis:</b> typeless If the multicast route can be hardware accelerated, the option will be available. For a multicast route to be accelerated, the ingress and egress interfaces must be switched.

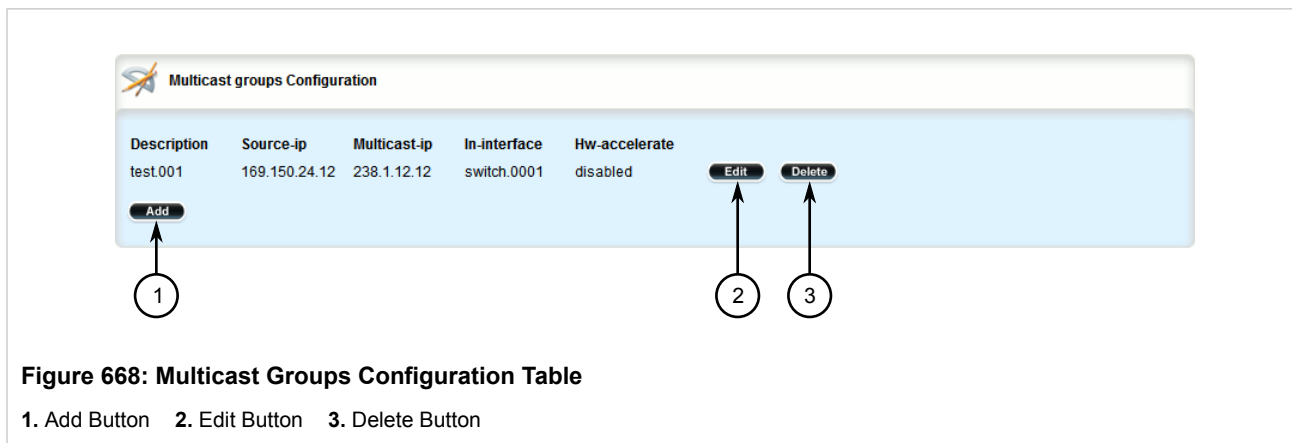
6. Configure out-interfaces. Refer to [Section 5.23.3.2, “Adding an Out-Interface”](#)
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.23.2.3

## Deleting a Static Multicast Group

To delete a static multicast group, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » static » mcast-groups**. The **Multicast Groups Configuration** table appears.



3. Click **Delete** next to the chosen multicast group.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.23.3

## Managing Out-Interfaces

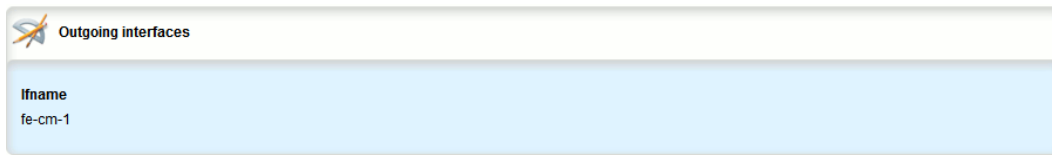
The following sections describe how to configure and manage out-interfaces:

- [Section 5.23.3.1, “Viewing a List of Out-Interfaces”](#)
- [Section 5.23.3.2, “Adding an Out-Interface”](#)
- [Section 5.23.3.3, “Deleting an Out-Interface”](#)

### Section 5.23.3.1

## Viewing a List of Out-Interfaces

To view a list of out-interfaces, navigate to **routing » multicast » static » mcast-groups » {group} » out-interface**, where *{group}* is the name of the multicast group. If out-interfaces have been configured, the **Outgoing Interfaces** table appears.



Outgoing interfaces	
Ifname	fe-cm-1

**Figure 669: Outgoing Interfaces Table**

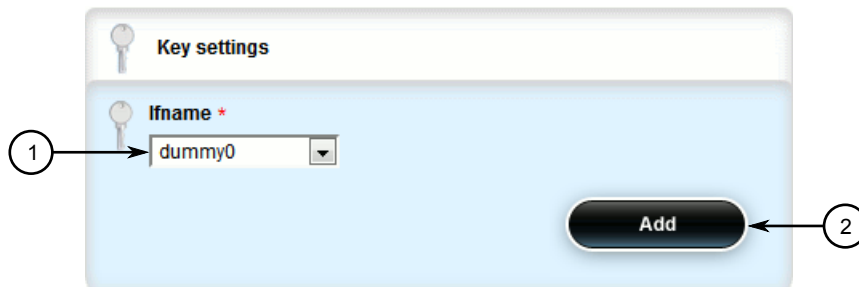
If no out-interfaces have been configured, add groups as needed. For more information about adding out-interfaces, refer to [Section 5.23.3.2, “Adding an Out-Interface”](#).

### Section 5.23.3.2

## Adding an Out-Interface

To add an out-interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » static » mcast-groups » {group} » out-interface**, where {group} is the name of the multicast group
3. Click **<Add out-interface>** in the menu. The **Key settings** form appears.



**Figure 670: Key Settings Form**

1. Ifname List    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
ifname	

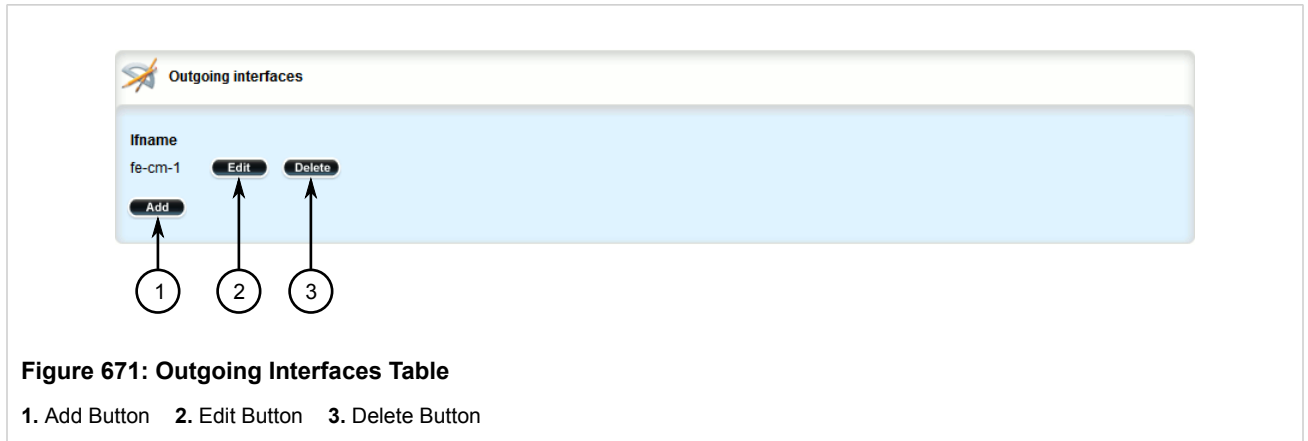
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.23.3.3

## Deleting an Out-Interface

To delete an out-interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » static » mcast-groups » {group} » out-interface**. The **Outgoing Interfaces** table appears.



3. Click **Delete** next to the chosen out-interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.24

## 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.

The following sections describe how to configure and manage PIM-SM:

- [Section 5.24.1, “PIM-SM Concepts”](#)
- [Section 5.24.2, “Configuring PIM-SM”](#)
- [Section 5.24.3, “Viewing a List of PIM-SM Interfaces”](#)
- [Section 5.24.4, “Enabling/Disabling a PIM-SM Interface”](#)
- [Section 5.24.5, “Configuring a Static RP Address”](#)
- [Section 5.24.6, “Managing a Boot Strap Router”](#)
- [Section 5.24.7, “Viewing the Status of PIM-SM”](#)
- [Section 5.24.8, “Viewing the Status of Dynamic Multicast Routing”](#)

#### Section 5.24.1

## 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 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 5.24.2

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » dynamic » PIM-SM**. The **PIM-SM Configuration** form appears.

**Figure 672: PIM-SM Configuration Form**

1. Enable PIM-SM Check Box    2. Default Preference Box    3. Default Metric Box    4. Broken Cisco Checksum Check Box

3. Configure the following parameters as required:

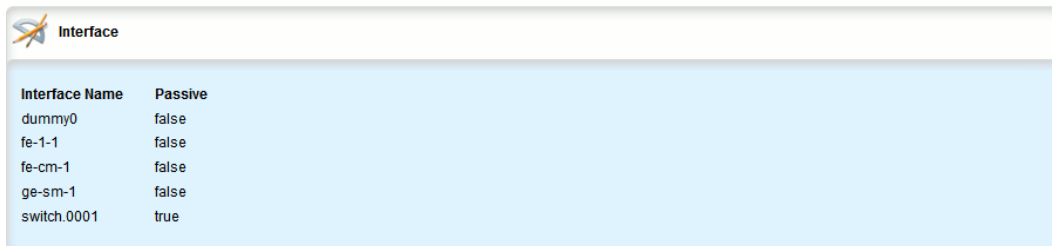
Parameter	Description
Enable PIM-SM	<b>Synopsis:</b> typeless Enable PIM-SM service.
Default Preference	<b>Synopsis:</b> An integer <b>Default:</b> 1024 Default preference value. Preferences are used by assert elections to determine upstream routers.
Default Metric	<b>Synopsis:</b> An integer <b>Default:</b> 1024 Default metric value. Metric is the cost of sending data through interface.
Broken Cisco Checksum	<b>Synopsis:</b> typeless If your RP is a cisco and shows many PIM_REGISTER checksum errors from this router, setting this option will help.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.24.3

## Viewing a List of PIM-SM Interfaces

To view a list of PIM-SM interfaces, navigate to *routing » multicast » dynamic » pim-sm » interface*. If PIM-SM interfaces have been configured, the **Interface** table appears.



Interface Name	Passive
dummy0	false
fe-1-1	false
fe-cm-1	false
ge-sm-1	false
switch.0001	true

**Figure 673: Interface Table**

If no PIM-SM interfaces have been configured, enable interfaces as needed. For more information about enabling PIM-SM interfaces, refer to [Section 5.24.4, “Enabling/Disabling a PIM-SM Interface”](#).

## Section 5.24.4

## 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.

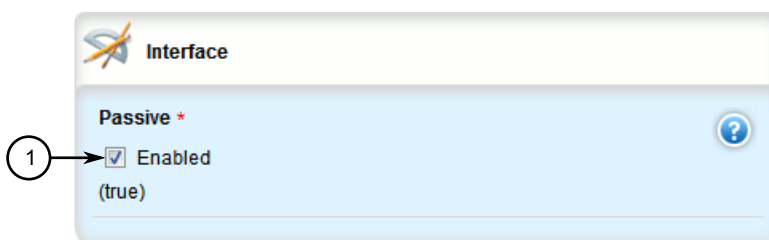
1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » dynamic » PIM-SM » interface » interface-name**, where *interface-name* is the name of the interface to be enabled for PIM-SM.



#### NOTE

A maximum of 30 non-passive interfaces can be active for PIM-SM.

3. The **Interface** form appears.



**Figure 674: Interface Form**

1. Enabled Check Box

4. Configure the following parameter(s) as required:

Parameter	Description
Passive	<b>Synopsis:</b> true or false <b>Default:</b> true Whether an interface is active or passive.



#### NOTE

Clear the **Passive Enabled** check box to activate PIM-SM on the interface, or check the **Passive Enabled** check box to disable PIM-SM on the interface.

5. For VLAN interfaces only, if IGMP snooping is enabled on the interface, make sure the IGMP query interval is set to 125 seconds. For more information, refer to [Section 5.25.3.1, “Configuring IGMP Snooping”](#).  
The same is required for any Layer 2 switches on the network.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.24.5

## Configuring a Static RP Address

To configure a Static RP address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » dynamic » pim-sm » rp-address** and click **<Add dest-address>**. The **Key Settings** form appears.

**Figure 675: RP Address Form**

1. Address Box   2. Group Box   3. Add Button

3. Configure the following parameters as required:

Parameter	Description
Address	<b>Synopsis:</b> A string 7 to 15 characters long Static RP (Rendezvous Point) address.
Group	<b>Synopsis:</b> A string 9 to 18 characters long The multicast group the RP handles.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.24.6

## Managing a Boot Strap Router

The following sections describe how to configure and manage a Boot Strap Router:

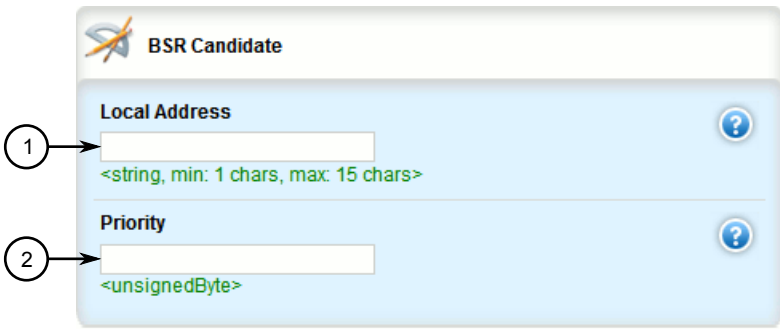
- [Section 5.24.6.1, “Configuring a BSR Candidate”](#)
- [Section 5.24.6.2, “Configuring a Group Prefix”](#)
- [Section 5.24.6.3, “Configuring an RP Candidate”](#)

#### Section 5.24.6.1

### Configuring a BSR Candidate

To configure a BSR candidate, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » dynamic » pim-sm** and click the **+** symbol in the menu next to **bsr-candidate**. The **BSR Candidate** form appears.



**Figure 676: BSR Candidate Form**

1. Local Address Box    2. Priority Box

3. Configure the following parameters as required:

Parameter	Description
Local Address	<b>Synopsis:</b> A string 7 to 15 characters long 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	<b>Synopsis:</b> An integer between 1 and 255 Bigger value means higher priority

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.24.6.2

### Configuring a Group Prefix

To configure a group-prefix, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » dynamic » pim-sm » group-prefix** and click **<Add group-prefix>**. The **Key settings** form appears.

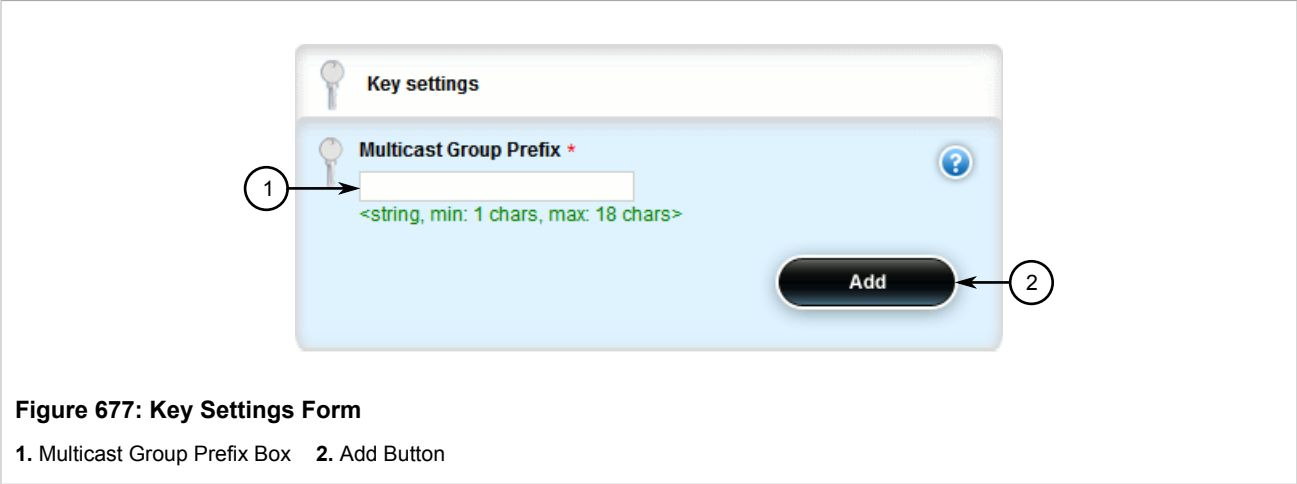


Figure 677: Key Settings Form

1. Multicast Group Prefix Box    2. Add Button



**NOTE**  
*A maximum of 20 group prefixes can be defined for PIM-SM.*

3. Configure the following parameters as required:

Parameter	Description
Multicast Group Prefix	<b>Synopsis:</b> A string 9 to 18 characters long Multicast group prefix (for example, 225.1.2.0/24).

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.24.6.3

Configuring an RP Candidate

To configure an RP candidate, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **routing » multicast » dynamic » pim-sm » rp-candidate**. The **RP Candidate** form appears.
3. Press the **+** symbol in the menu next to **rp-candidate** to open the form fields.

**Figure 678: RP Candidate Form**

1. Local Address Box   2. Timer Box   3. Priority Box

4. Configure the following parameters as required:

Parameter	Description
Local Address	<b>Synopsis:</b> A string 7 to 15 characters long Local address to be used in the Cand-RP messages. If not specified, the largest local IP address will be used (excluding passive interfaces).
Timer	<b>Synopsis:</b> An integer between 10 and 65535 <b>Default:</b> 60 The number of seconds to wait between advertising Cand-RP message.
Priority	<b>Synopsis:</b> An integer between 1 and 255 Priority of this CRP, smaller value means higher priority.

5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 5.24.7

## Viewing the Status of PIM-SM

To view the status of PIM-SM, do the following:

1. Navigate to **routing » status » pim-sm**. The **PIM-SM Status** form appears displaying the address of the BSR.



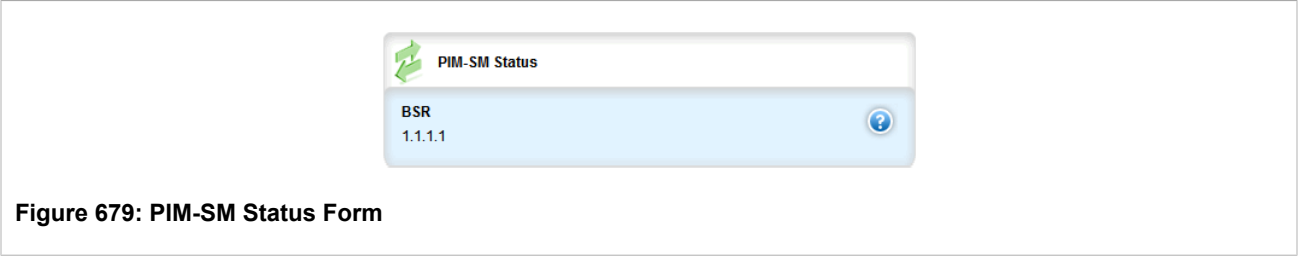


Figure 679: PIM-SM Status Form

2. Navigate to **routing » status » pim-sm » vinterface**. The **Virtual Interface** table appears displaying the status of the configured devices.

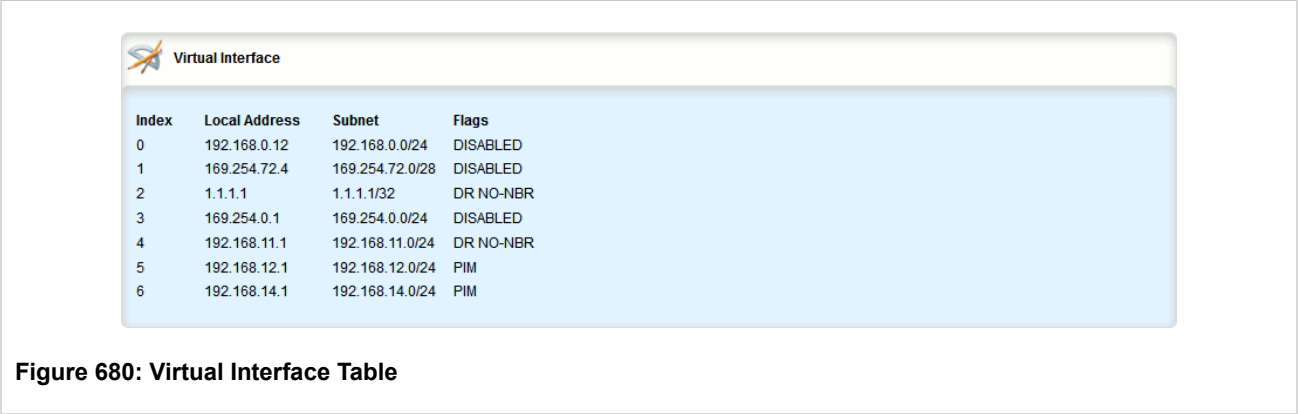


Figure 680: Virtual Interface Table

Parameter	Description
Index	Virtual interface index.
Local Address	<b>Synopsis:</b> A string 1 to 16 characters long Local address.
Subnet	<b>Synopsis:</b> A string 1 to 20 characters long Subnet.
Flags	<b>Synopsis:</b> A string 1 to 128 characters long Flags indicates virtual interface information. <ul style="list-style-type: none"><li>DISABLED: The virtual interface is administratively disabled for PIM-SM.</li><li>DOWN: This virtual interface is down.</li><li>DR: Designated router.</li><li>NO-NBR: No neighbor on this virtual interface.</li><li>PIM: PIM neighbor.</li><li>DVMRP: DVMRP neighbor.</li></ul>

3. Navigate to **routing » status » pim-sm » rp**. The **Rendezvous Point** table appears displaying the RP server addresses.

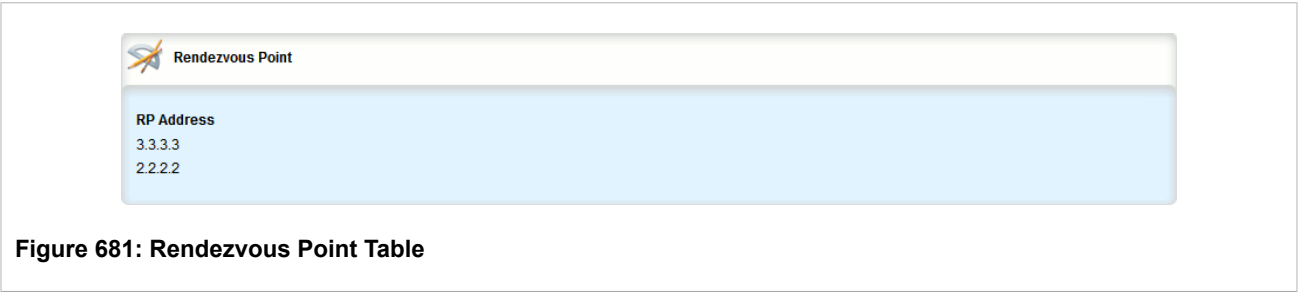
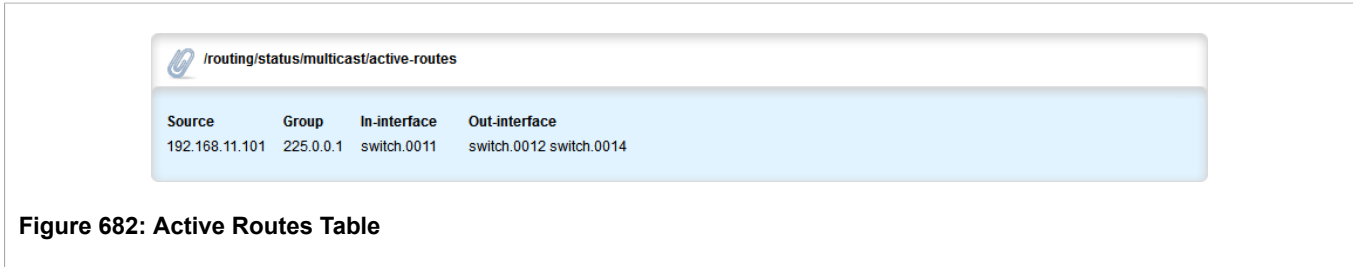


Figure 681: Rendezvous Point Table

Section 5.24.8

# Viewing the Status of Dynamic Multicast Routing

To view the status of dynamic multicast routing, navigate to **routing » status » multicast**. If multicast routes have been configured, the **Active Routes** table appears.



Section 5.25

# 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).

The following sections describe how to configure and manage multicast filtering:

- [Section 5.25.1, “Multicast Filtering Concepts”](#)
- [Section 5.25.2, “Enabling and Configuring GMRP”](#)
- [Section 5.25.3, “Managing IGMP Snooping”](#)
- [Section 5.25.4, “Managing the Static Multicast Group Table”](#)
- [Section 5.25.5, “Managing Egress Ports for Multicast Groups”](#)
- [Section 5.25.6, “Viewing a Summary of Multicast Groups”](#)
- [Section 5.25.7, “Viewing a List of IP Multicast Groups”](#)

Section 5.25.1

# Multicast Filtering Concepts

The following sections describe some of the concepts important to the implementation of multicast filtering in RUGGEDCOM ROX II:

- [Section 5.25.1.1, “IGMP”](#)
- [Section 5.25.1.2, “GMRP \(GARP Multicast Registration Protocol\)”](#)

Section 5.25.1.1

## IGMP

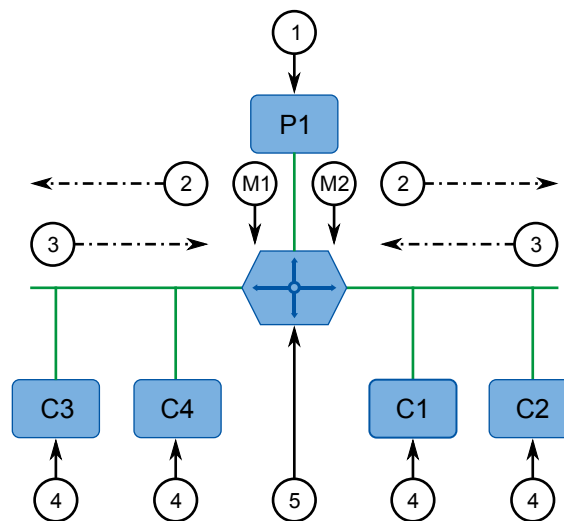
IGMP is used by IP hosts to report their host group memberships with multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host.

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 683: Example – IGMP In Operation**

1. Producer 2. Membership Queries 3. Membership Reports 4. Host 5. Multicast 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.

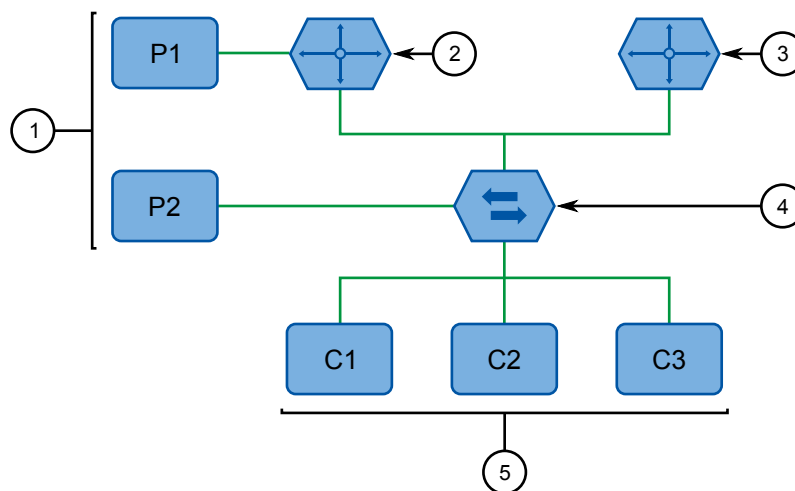
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- 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 684: 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 5.25.1.2

### GMRP (GARP Multicast Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.

**NOTE**

*GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.*

#### » Joining a Multicast Group

In order to join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

## » Leaving a Multicast Group

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

## » Notes About GMRP

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

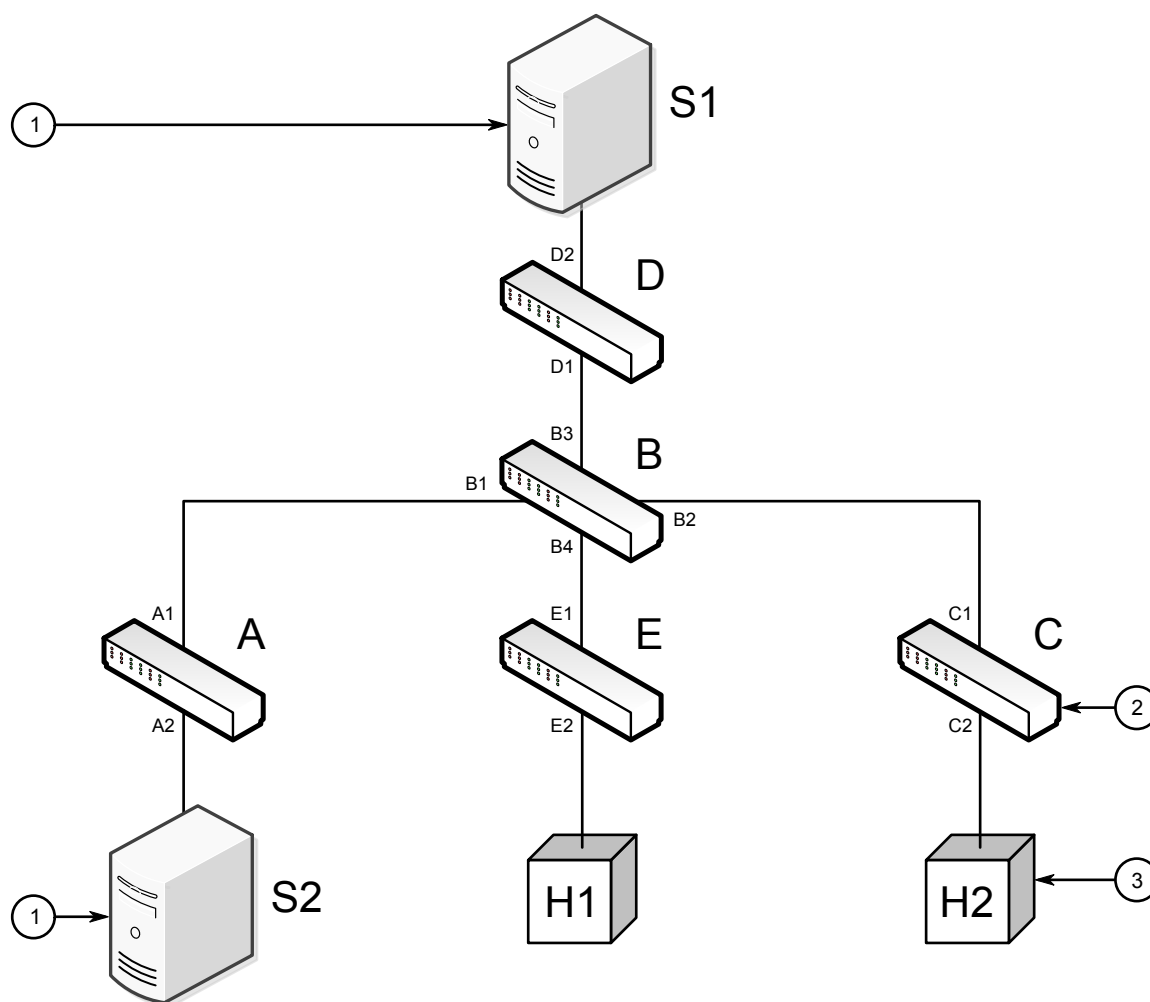
- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled on the RUGGEDCOM RX5000, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the RUGGEDCOM RX5000, and not forwarded.

## » Example: Establishing Membership with GMRP

The following example illustrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

In this scenario, there are two multicast sources, S1 and S2, multicasting to Multicast Groups 1 and 2, respectively. A network of five switches, including one core switch (B), connects the sources to two hosts, H1 and H2, which receive the multicast streams from S1 and S2, respectively.



**Figure 685: 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 5.25.2

## Enabling and Configuring GMRP

To enable and configure GMRP (GARP Multicast Registration Protocol), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering**. The **GMRP** form appears.

**Figure 686: GMRP Form**

1. Enabled Check Box    2. RSTP Flooding Check Box    3. Leave Timer Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false GMRP Enable
RSTP Flooding	<b>Synopsis:</b> typeless Determines whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge

Parameter	Description
	ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.
Leave Timer (ms)	<p><b>Synopsis:</b> An integer between 600 and 300000  <b>Default:</b> 4000</p> <p>The time in milliseconds to wait after issuing Leave or LeaveAll before removing registered multicast groups. If Join messages for specific addresses are received before this timer expires, the addresses will be kept registered.</p>

4. Enable GMRP on one or more switched Ethernet ports. For more information, refer to [Section 3.18.2, “Configuring a Switched Ethernet Port”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.25.3

## Managing IGMP Snooping

The following sections describe how to configure and manage IGMP snooping:

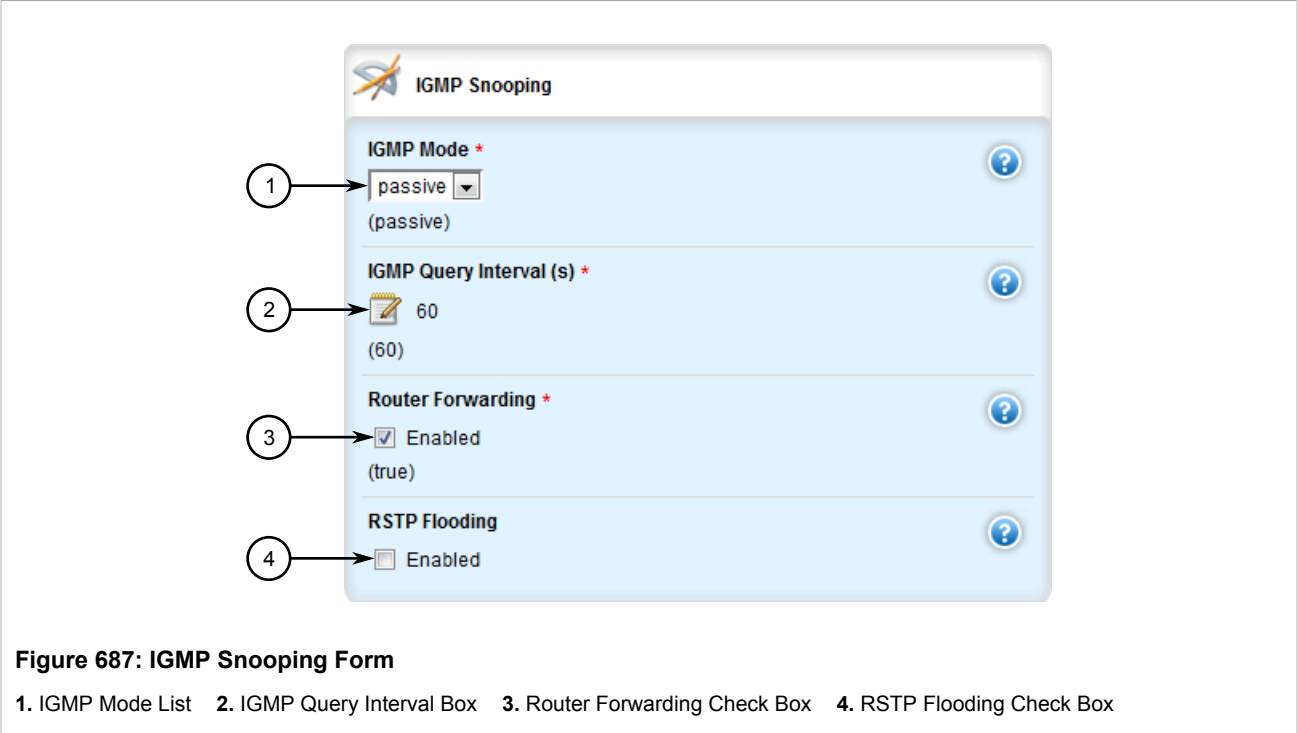
- [Section 5.25.3.1, “Configuring IGMP Snooping”](#)
- [Section 5.25.3.2, “Viewing a List of Router Ports”](#)
- [Section 5.25.3.3, “Adding a Router Port”](#)
- [Section 5.25.3.4, “Deleting a Router Port”](#)

### Section 5.25.3.1

## Configuring IGMP Snooping

To configure IGMP snooping, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering » igmp-snooping**. The **IGMP Snooping** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
IGMP Mode	<b>Synopsis:</b> { active, passive } <b>Default:</b> passive  Specifies the IGMP mode: <itemizedlist><listitem>PASSIVE : The switch passively snoops IGMP traffic and never sends IGMP queries.</listitem> <listitem>ACTIVE : The switch generates IGMP queries, if no queries from a better candidate for the querier are detected for a while.</listitem></itemizedlist>
IGMP Query Interval (s)	<b>Synopsis:</b> An integer between 10 and 3600 <b>Default:</b> 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	<b>Synopsis:</b> true or false <b>Default:</b> true  Whether or not multicast streams will always be forwarded to multicast routers.
RSTP Flooding	<b>Synopsis:</b> typeless  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.

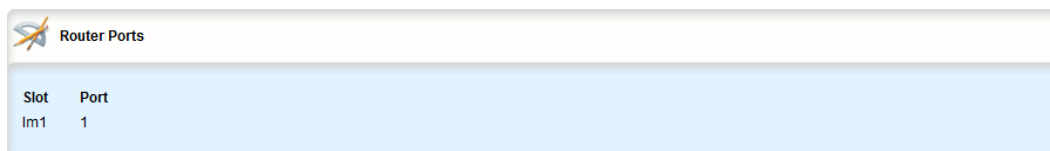
4. Assign one or more ports for IGMP to use when sending Membership Reports. For more information, refer to [Section 5.25.3.3, “Adding a Router Port”](#).

5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.25.3.2

## Viewing a List of Router Ports

To view a list of router ports used for IGMP snooping, navigate to **switch » mcast-filtering » igmp-snooping » router-ports**. If router ports have been configured, the **Router Ports** table appears.



Slot	Port
Im1	1

**Figure 688: Router Ports Table**

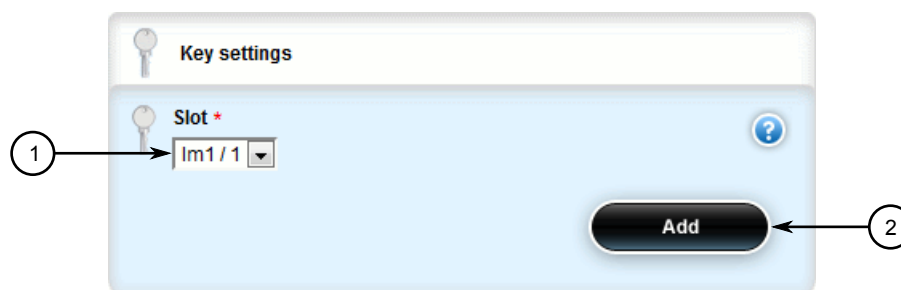
If no router ports have been configured, add ports as needed. For more information, refer to [Section 5.25.3.3, “Adding a Router Port”](#).

### Section 5.25.3.3

## Adding a Router Port

To add a router port for IGMP snooping, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering » igmp-snooping » router-ports** and click **<Add router-ports>**. The **Key Settings** form appears.



**Figure 689: Key Settings Form**

1. Slot Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Slot	The name of the module location provided on the silkscreen across the top of the device.
Port	The selected ports on the module installed in the indicated slot.

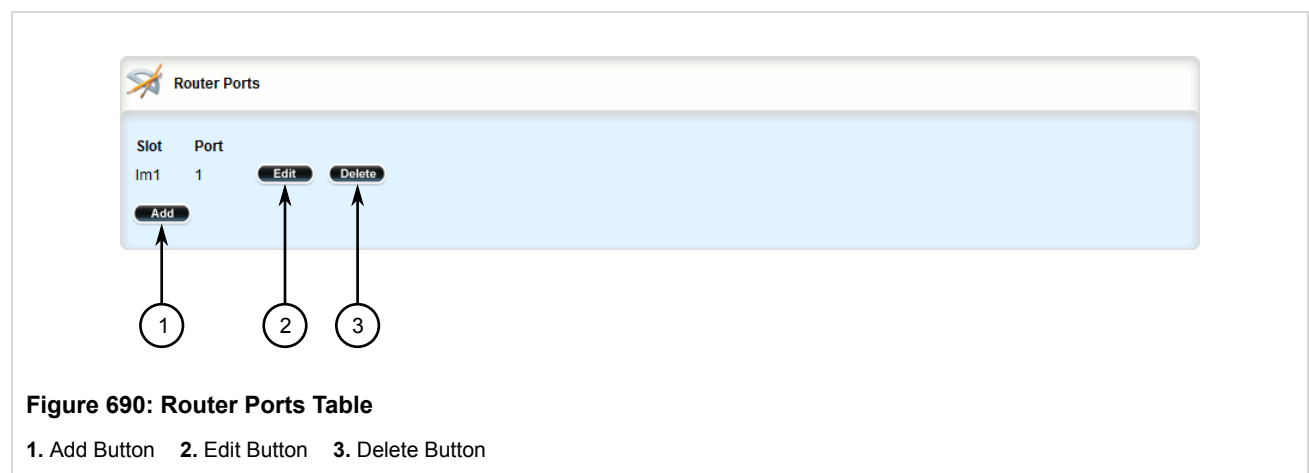
- Click **Add** to add the router port.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.25.3.4

## Deleting a Router Port

To delete a router port for IGMP snooping, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » mcast-filtering » igmp-snooping » router-ports**. The **Router Ports** table appears.



- Click **Delete** next to the chosen router port.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.25.4

## Managing the Static Multicast Group Table

The following sections describe how to configure and manage a list of known static multicast groups on other devices:

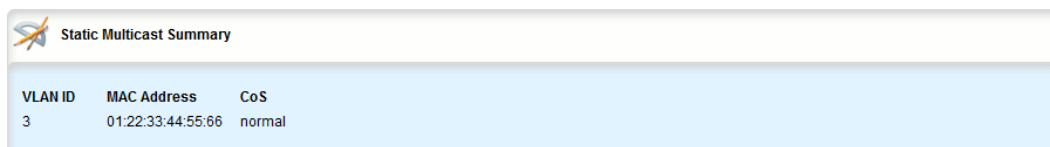
- [Section 5.25.4.1, “Viewing a List of Static Multicast Group Entries”](#)
- [Section 5.25.4.2, “Adding a Static Multicast Group Entry”](#)

- [Section 5.25.4.3, “Deleting a Static Multicast Group Entry”](#)

#### Section 5.25.4.1

### Viewing a List of Static Multicast Group Entries

To view a list of entries for known static multicast groups on other devices, navigate to **switch » mcast-filtering » static-mcast-table**. If entries have been configured, the **Static Multicast Summary** table appears.



VLAN ID	MAC Address	CoS
3	01:22:33:44:55:66	normal

**Figure 691: Static Multicast Summary Table**

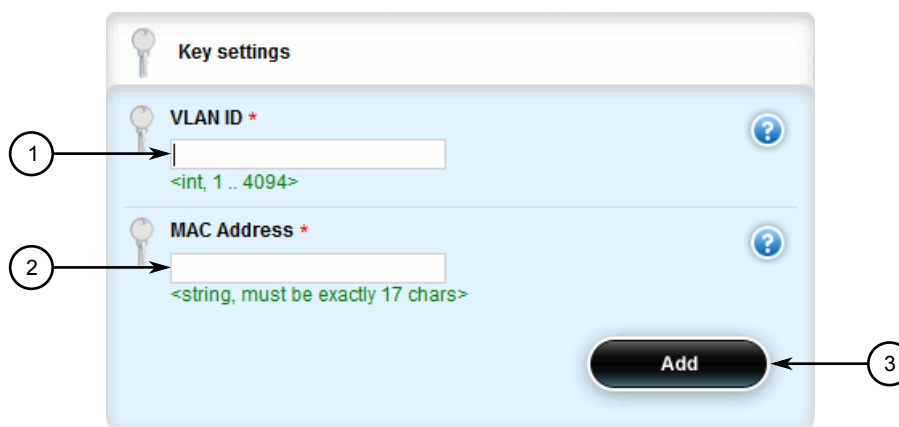
If no entries have been configured, add entries as needed. For more information, refer to [Section 5.25.4.2, “Adding a Static Multicast Group Entry”](#).

#### Section 5.25.4.2

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering » static-mcast-table** and click **<Add static-mcast-table>**. The **Key Settings** form appears.



**Key settings**

1. **VLAN ID \***  <int, 1 .. 4094>

2. **MAC Address \***  <string, must be exactly 17 chars>

3. **Add**

**Figure 692: Key Settings Form**

1. VLAN ID Box    2. MAC Address Box    3. Add Button

3. Configure the following parameter(s) as required:

**NOTE**

Letters in MAC addresses must be lowercase.

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 The VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	<b>Synopsis:</b> A string The multicast group MAC address in the form 01:xx:xx:xx:xx:xx.

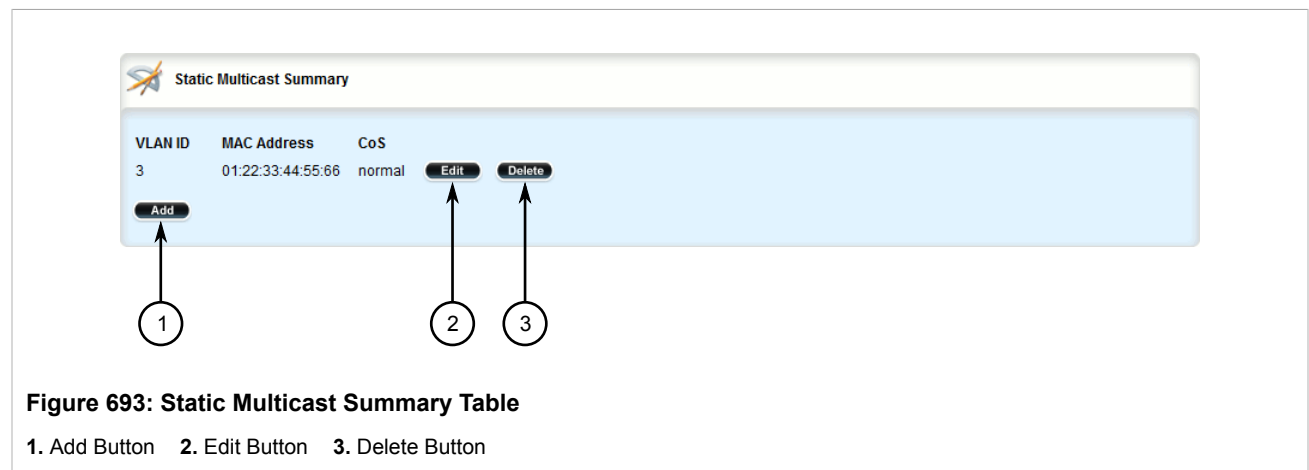
4. Add one or more egress ports. For more information, refer to [Section 5.25.5.2, “Adding an Egress Port”](#).
5. Click **Add** to create the table entry.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 5.25.4.3

## Deleting a Static Multicast Group Entry

To delete a static multicast group from the Static Multicast Summary table, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering » static-mcast-table**. The **Static Multicast Summary** table appears.



3. Click **Delete** next to the chosen table entry.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.25.5

## Managing Egress Ports for Multicast Groups

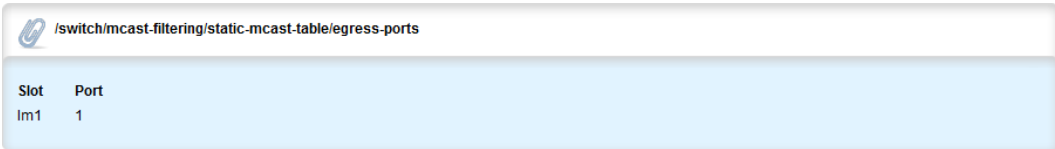
The following sections describe how to configure and manage egress ports for multicast groups:

- [Section 5.25.5.1, “Viewing a List of Egress Ports”](#)
- [Section 5.25.5.2, “Adding an Egress Port”](#)
- [Section 5.25.5.3, “Deleting an Egress Port”](#)

## Section 5.25.5.1

### Viewing a List of Egress Ports

To view a list of egress ports for a static multicast group defined in the Static Multicast Group Summary table, navigate to **switch » mcast-filtering » static-mcast-table » {id/address} » egress-ports**, where *{id/address}* is the VLAN ID for the static multicast group and the MAC address for the host device. If egress ports have been configured, the **Egress Ports** table appears.



/switch/mcast-filtering/static-mcast-table/egress-ports	
Slot	Port
Im1	1

**Figure 694: Egress Ports Table**

If no egress ports have been configured, add egress ports as needed. For more information, refer to [Section 5.25.5.2, “Adding an Egress Port”](#).

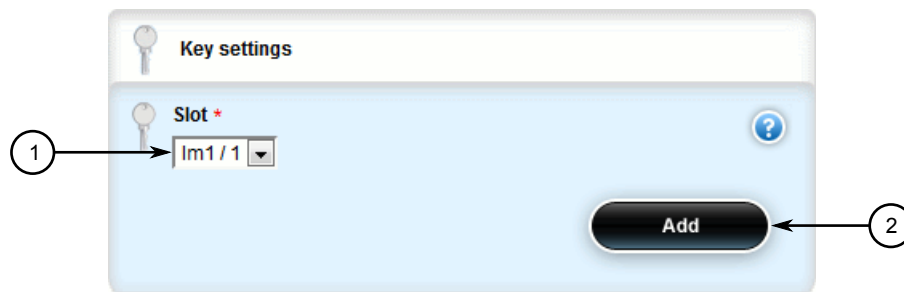
## Section 5.25.5.2

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering » static-mcast-table » {id/address} » egress-ports**, where *{id/address}* is the VLAN ID for the static multicast group and the MAC address for the host device.
3. Click **<Add egress-ports>**. The **Key Settings** form appears.





**Figure 695: Key Settings Form**

1. Slot List    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Slot	The name of the module location provided on the silkscreen across the top of the device.
Port	The selected ports on the module installed in the indicated slot.

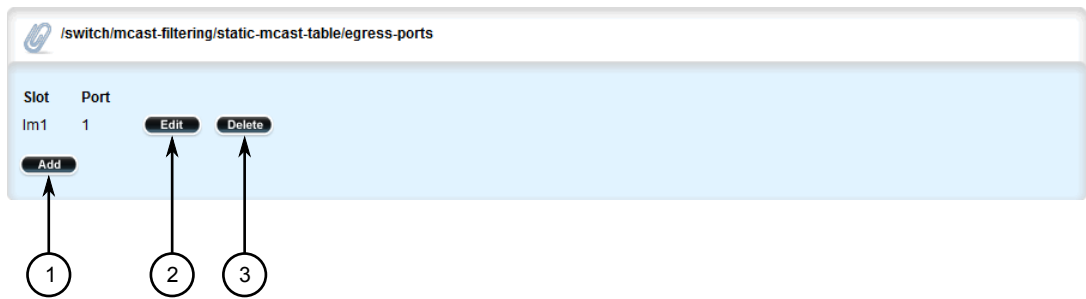
5. Click **Add** to create the egress port.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.25.5.3

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mcast-filtering » static-mcast-table » {id/address} » egress-ports**, where *{id/address}* is the VLAN ID for the static multicast group and the MAC address for the host device. The **Egress Ports** table appears.



**Figure 696: Egress Ports Table**

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen egress port.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.25.6

# Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, navigate to **switch » mcast-filtering » mcast-group-summary**. If multicast groups have been configured, the **Multicast Group Summary** table appears.

**Figure 697: Multicast Group Summary Table**

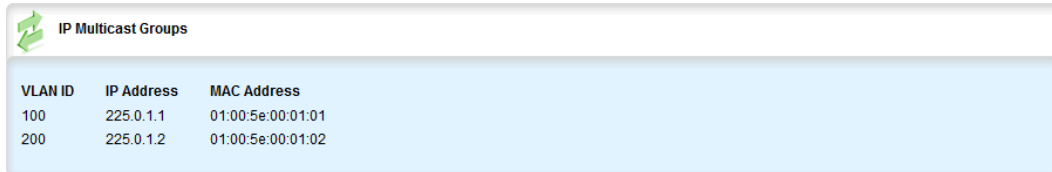
This table provides the following information:

Parameter	Description
VLAN ID	The VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	<b>Synopsis:</b> A string The multicast group MAC address.

## Section 5.25.7

## Viewing a List of IP Multicast Groups

To view a list of all IP multicast groups, navigate to **switch » mcast-filtering » ip-mcast-groups**. If IP multicast groups have been configured, the **IP Multicast Groups** table appears.



VLAN ID	IP Address	MAC Address
100	225.0.1.1	01:00:5e:00:01:01
200	225.0.1.2	01:00:5e:00:01:02

**Figure 698: IP Multicast Groups Table**

This table provides the following information:

## Section 5.26

## Managing VRRP

The Virtual Router Redundancy Protocol is a gateway redundancy protocol. VRRP provides a gateway failover mechanism that is invisible to the hosts and other devices that send traffic through that gateway. The Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure associated with statically routed networks by providing automatic failover using alternate routers. The RUGGEDCOM ROX II VRRP daemon (keepalived) is an [RFC 5798](http://tools.ietf.org/html/rfc5798) [http://tools.ietf.org/html/rfc5798] version 2 and version 3 compliant implementation of VRRP.

**NOTE**

*RFC 5798 defines the standard for VRRP version 3 on IPv4 and IPv6. Only IPv4 is supported in this release of RUGGEDCOM ROX II.*

The following sections describe how to configure VRRP:

- [Section 5.26.1, “VRRP Concepts”](#)
- [Section 5.26.2, “Viewing the Status of VRRP”](#)
- [Section 5.26.3, “Enabling/Disabling VRRP”](#)
- [Section 5.26.4, “Managing VRRP Trackers”](#)
- [Section 5.26.5, “Managing VRRP Groups”](#)
- [Section 5.26.6, “Managing VRRP Instances”](#)
- [Section 5.26.7, “Managing VRRP Monitors”](#)
- [Section 5.26.8, “Managing Track Scripts”](#)
- [Section 5.26.9, “Managing Virtual IP Addresses”](#)

Section 5.26.1

## VRRP Concepts

The following sections describe some of the concepts important to the implementation of VRRP in RUGGEDCOM ROX II:

- [Section 5.26.1.1, “Static Routing vs. VRRP”](#)
- [Section 5.26.1.2, “VRRP Terminology”](#)

Section 5.26.1.1

### 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 5.26.1.2

### VRRP Terminology

Each physical router running VRRP is known as a VRRP Router. Two or more VRRP Routers can be configured to form a *Virtual Router*. Each VRRP Router may participate in one or more Virtual Routers.

Each Virtual Router has a user-configured Virtual Router Identifier (VRID) and a Virtual IP address or set of IP addresses on the shared LAN. Hosts on the shared LAN are configured to use these addresses as the default gateway.

Each router in the Virtual Router Group has a specific priority, which is a number between 1 and 255. The router with the highest priority (or highest number) is elected the Master, while all other routers are considered Backups.

On RUGGEDCOM RX5000/MX5000/MX5000RE devices with RUGGEDCOM ROX II v2.3 or higher installed, if the router with the highest priority is in a fault state, the backup VRRP Router can delay its transition to becoming the Master router. The length of the delay is user-defined.

VRRP can also monitor a specified interface and give up control of a gateway IP to another VRRP Router if that interface goes down.

>> An Example of VRRP

In the following example, host 1 uses a gateway of 1.1.1.253 and host 2 uses a gateway of 1.1.1.252. The 1.1.1.253 gateway is provided by VRID 10. In normal practice, router 1 will provide this virtual IP since its priority for VRID 10 is higher than that of router 2. If router 1 becomes inoperative or if its w1ppp link fails, it will relinquish control of gateway IP 1.1.1.253 to router 2.

In a similar fashion host 2 can use the VRID 11 gateway address of 1.1.1.252, which will normally be supplied by router 2.

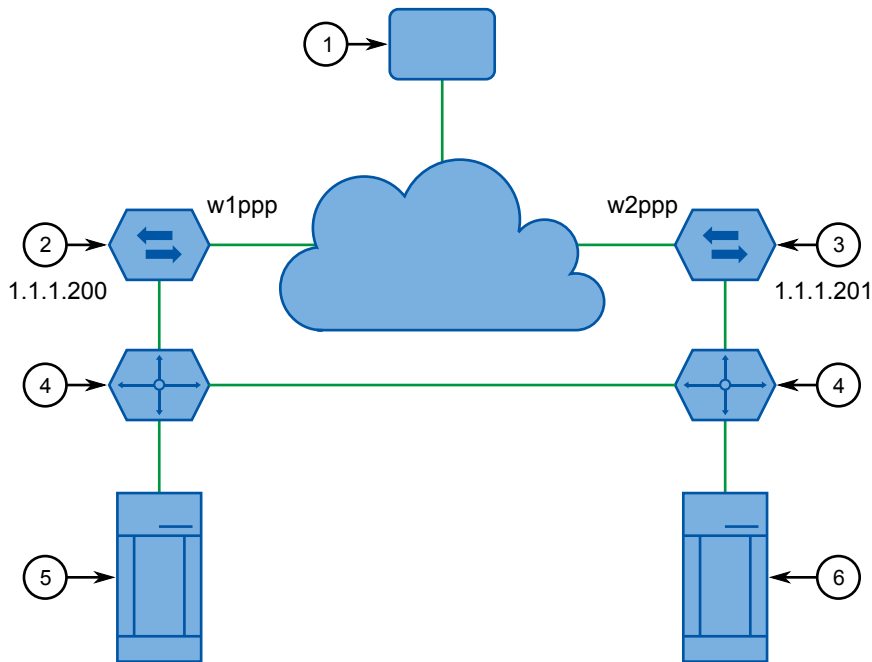


Figure 699: VRRP Example

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
<ul style="list-style-type: none"><li>VRID 10 Gateway IP: 1.1.1.253</li><li>VRID 10 Priority: 100</li><li>VRID 10 Monitor Interface: w1ppp</li><li>VRID 11 Gateway IP: 1.1.1.252</li><li>VRID 11 Priority: 50</li></ul>	<ul style="list-style-type: none"><li>VRID 10 Gateway IP: 1.1.1.253</li><li>VRID 10 Priority: 50</li><li>VRID 11 Gateway IP: 1.1.1.252</li><li>VRID 11 Priority: 100</li><li>VRID 11 Monitor Interface: w2ppp</li></ul>

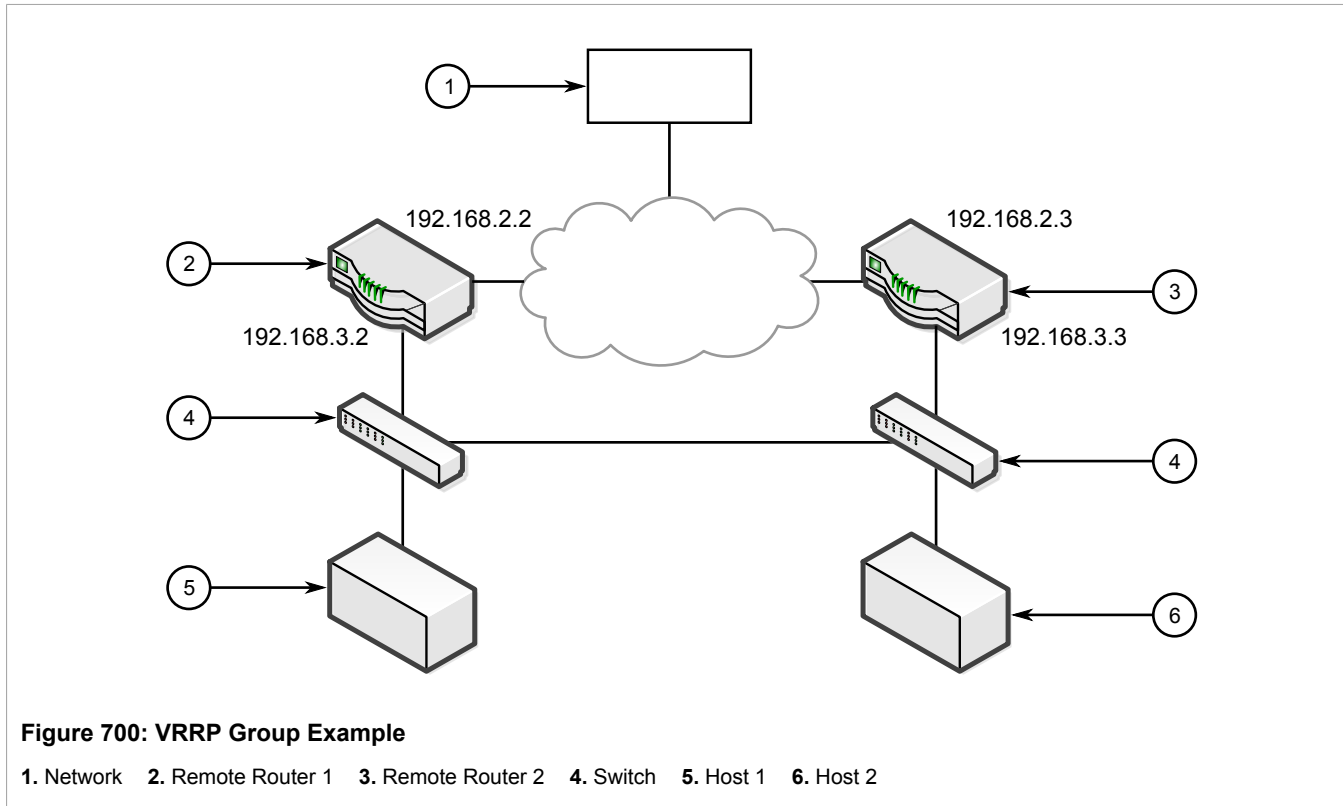
Traffic from host 1 is sent through router 1, and traffic from host 2 is sent through router 2. A failure of either router or their WAN link will be recovered by the other router.

Note that both routers can always be reached by the hosts at their *real* IP addresses.

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

>> An Example of VRRP Groups

In the next example, both host 1 and host 2 use a gateway of 192.168.3.10. The external side can access the internal side by gateway 192.168.2.10. VRID\_20 and VRID\_21 are grouped together. Normally, router 1 will provide both an internal and external access gateway, as its priority is higher than those on Router 2. When either the internal or external side of Router 1 becomes inoperative, Router 1 will remove give control of both 192.168.2.10 and 192.168.3.10 gateways to Router 2.



In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
<ul style="list-style-type: none"><li>• VRID_20 Gateway IP: 192.168.2.10</li><li>• VRID_20 Priority: 100</li><li>• VRID_21 Gateway IP: 192.168.3.10</li><li>• VRID_21 Priority: 100</li></ul>	<ul style="list-style-type: none"><li>• VRID_20 Gateway IP: 192.168.2.10</li><li>• VRID_20 Priority: 50</li><li>• VRID_21 Gateway IP: 192.168.3.10</li><li>• VRID_21 Priority: 50</li></ul>

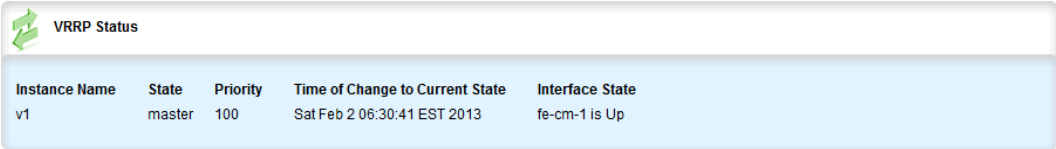
Other VRRP parameters are the Advertisement Interval and Gratuitous ARP Delay. The advertisement interval is the time between which advertisements are sent. A backup router will assume the role of Master three advertisement intervals after the Master fails. If a monitored interface goes down, a Master router will immediately signal an election and allow a Backup router to assume the Master roles.

The router issues a set of gratuitous ARPs when moving between Master and Backup roles. These unsolicited ARPs teach the hosts and switches in the network of the current MAC address and port associated with the gateway. The router will issue a second set of ARPs after the time specified by the Gratuitous ARP delay.

Section 5.26.2

# Viewing the Status of VRRP

To view the status of VRRP, navigate to **services » vrrp » status**. The **VRRP Status** form appears.



VRRP Status				
Instance Name	State	Priority	Time of Change to Current State	Interface State
v1	master	100	Sat Feb 2 06:30:41 EST 2013	fe-cm-1 is Up

Figure 701: VRRP Status Form

This table provides the following information:

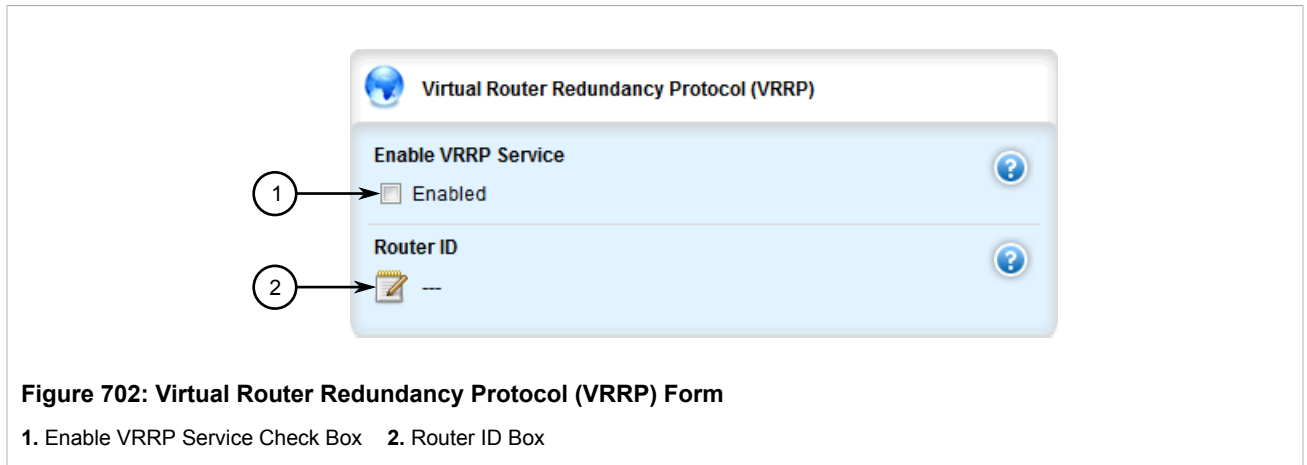
Parameter	Description
Instance Name	<b>Synopsis:</b> A string The VRRP instance name.
State	<b>Synopsis:</b> A string The VRRP instance state.
Priority	<b>Synopsis:</b> A string The VRRP instance priority.
Time of Change to Current State	<b>Synopsis:</b> A string The time of change to the current state.
Interface State	<b>Synopsis:</b> A string The VRRP interface state.

Section 5.26.3

# Enabling/Disabling VRRP

To enable or disable VRRP, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp**. The **Virtual Router Redundancy Protocol (VRRP)** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Enable VRRP Service	<b>Synopsis:</b> typeless Enables or disables the VRRP service.
Router ID	<b>Synopsis:</b> A string The router ID for VRRP logs.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.26.4

## 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.*

The following sections describe how to configure and manage VRRP trackers:

- [Section 5.26.4.1, "Viewing a List of VRRP Trackers"](#)
- [Section 5.26.4.2, "Adding a VRRP Tracker"](#)
- [Section 5.26.4.3, "Deleting a VRRP Tracker"](#)



#### Section 5.26.4.1

### Viewing a List of VRRP Trackers

To view a list of VRRP trackers, navigate to **services » vrrp » trackers**. If trackers have been configured, the **Tracker** table appears.



Tracker Name	Track Type	Network	Interface	Interval	Weight	Rise	Fall
tracker1	route	10.0.0.0/8	dummy0	1	not found	not found	not found

**Figure 703: Tracker Table**

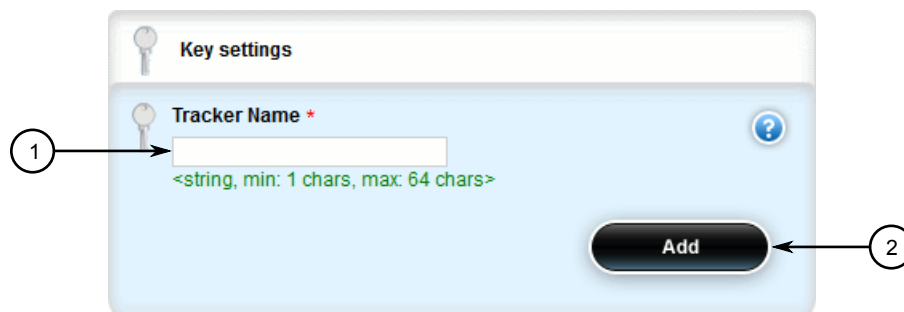
If no VRRP trackers have been configured, add trackers as needed. For more information, refer to [Section 5.26.4.2, “Adding a VRRP Tracker”](#).

#### Section 5.26.4.2

### Adding a VRRP Tracker

To add a VRRP tracker, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » trackers** and click **<Add tracker>**. The **Key Settings** form appears.



**Figure 704: Key Settings Form**

1. Tracker Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Tracker Name	<b>Synopsis:</b> A string 1 to 64 characters long The name of the tracker.

4. Click **Add** to add the tracker. The **Tracker** form appears.

**Figure 705: Tracker Form**

1. Tracker Type List   2. Network Box   3. Interface List   4. Interval List   5. Weight Box   6. Rise Box   7. Fall Box

- Configure the following parameter(s) as required:

Parameter	Description
Track Type	<b>Synopsis:</b> { route } <b>Default:</b> route The type of condition for the tracker to check.
Network	<b>Synopsis:</b> A string 9 to 18 characters long The network to track. The tracker checks for a route to this network in the routing table.
Interface	The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
Interval	<b>Synopsis:</b> An integer between 1 and 120 The number of seconds between tracker queries.
Weight	<b>Synopsis:</b> An integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the tracker falls. When positive, the priority increases by this amount when the tracker rises. When not set, the state changes to the fault state when the tracker falls.

Parameter	Description
Rise	<b>Synopsis:</b> An integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
Fall	<b>Synopsis:</b> An integer between 1 and 65535 The number of unsuccessful tracker queries before changing the router priority.

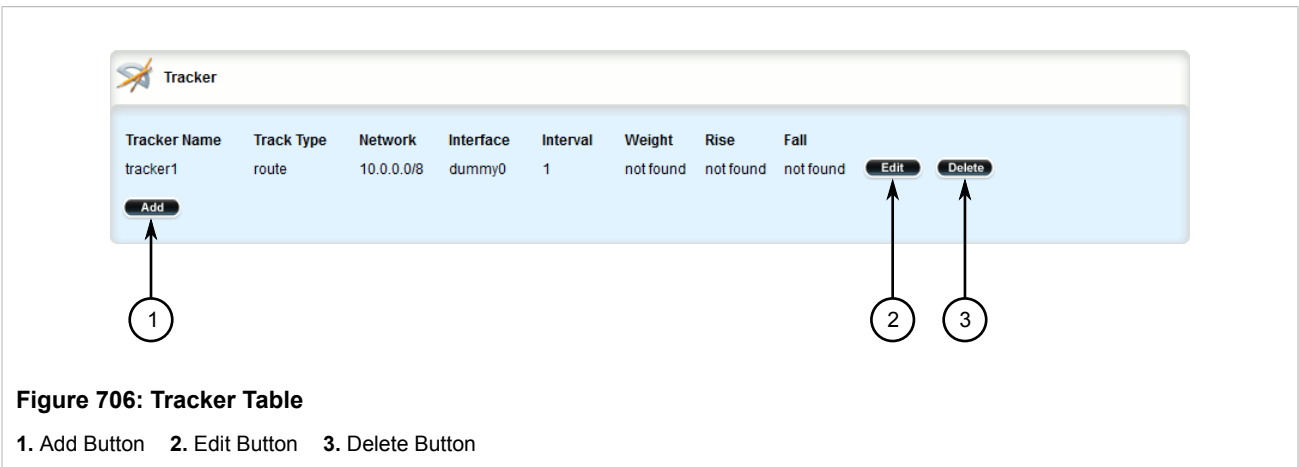
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.26.4.3

## Deleting a VRRP Tracker

To delete a VRRP tracker, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » vrrp » trackers**. The **Tracker** table appears.



- Click **Delete** next to the chosen tracker.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.26.5

## 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.

The following sections describe how to configure and manage VRRP groups:

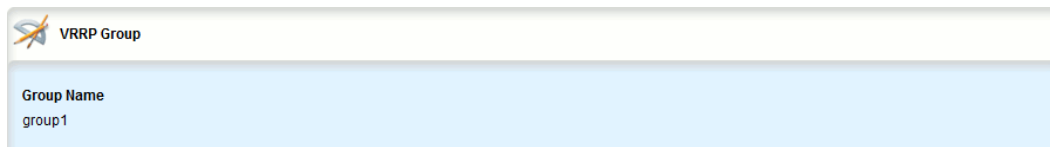
- [Section 5.26.5.1, “Viewing a List of VRRP Groups”](#)

- [Section 5.26.5.2, “Adding a VRRP Group”](#)
- [Section 5.26.5.3, “Deleting a VRRP Group”](#)

#### Section 5.26.5.1

### Viewing a List of VRRP Groups

To view a list of VRRP groups, navigate to **services » vrrp » group**. If groups have been configured, the **VRRP Group** table appears.



VRRP Group	
Group Name	group1

**Figure 707: VRRP Group Table**

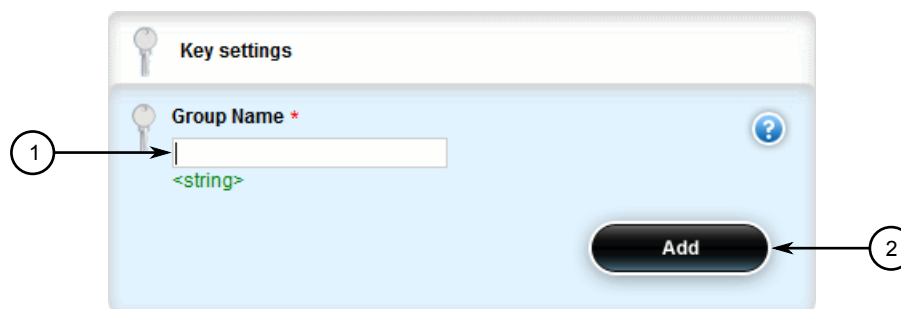
If no VRRP groups have been configured, add groups as needed. For more information, refer to [Section 5.26.5.2, “Adding a VRRP Group”](#).

#### Section 5.26.5.2

### Adding a VRRP Group

To add a VRRP group, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » group** and click **<Add group>**. The **Key Settings** form appears.



**Figure 708: Key Settings Form**

1. Group Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Group Name	<b>Synopsis:</b> A string 1 to 64 characters long The VRRP group name.

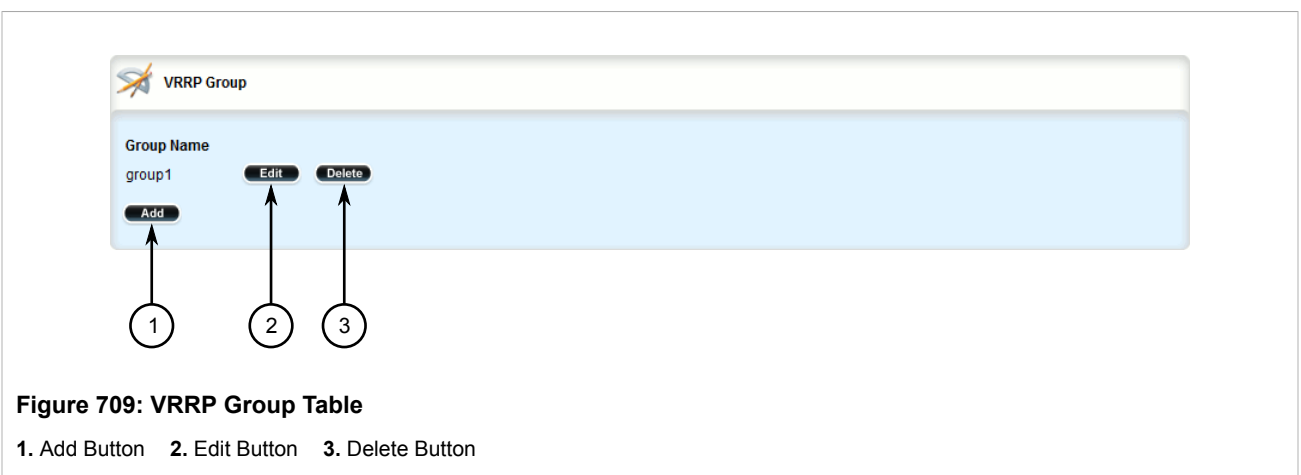
- Click **Add** to add the group.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.26.5.3

## Deleting a VRRP Group

To delete a VRRP group, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » vrrp » group**. The **VRRP Group** table appears.



- Click **Delete** next to the chosen group.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.26.6

## Managing VRRP Instances

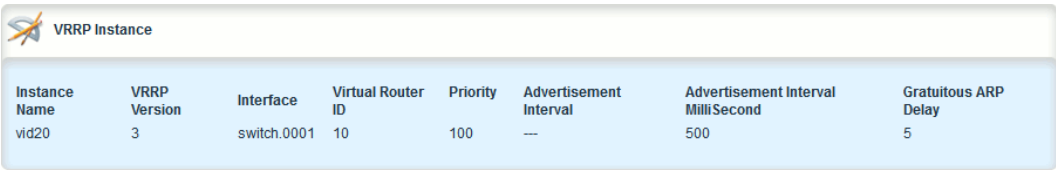
The following sections describe how to configure and manage VRRP instances:

- [Section 5.26.6.1, “Viewing a List of VRRP Instances”](#)
- [Section 5.26.6.2, “Adding a VRRP Instance”](#)
- [Section 5.26.6.3, “Deleting a VRRP Instance”](#)

## Section 5.26.6.1

### Viewing a List of VRRP Instances

To view a list of VRRP instances, navigate to **services » vrrp » instance**. If instance have been configured, the **VRRP Instance** table appears.



A screenshot of a web interface titled "VRRP Instance" showing a table with configuration details for a VRRP instance named "vid20".

Instance Name	VRRP Version	Interface	Virtual Router ID	Priority	Advertisement Interval	Advertisement Interval MilliSecond	Gratuitous ARP Delay
vid20	3	switch.0001	10	100	—	500	5

Figure 710: VRRP Instance Table

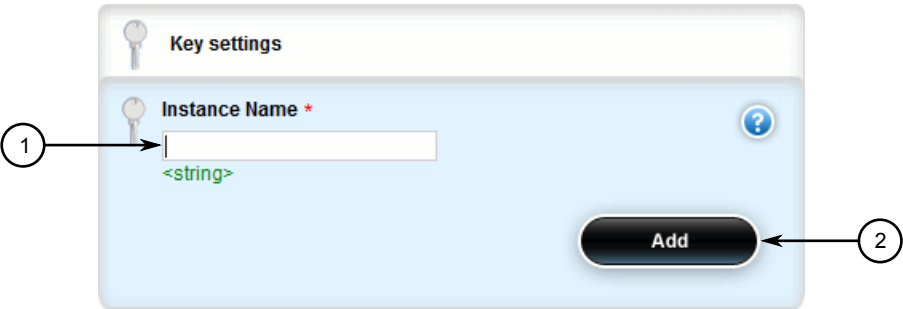
If no VRRP instances have been configured, add instances as needed. For more information, refer to [Section 5.26.6.2, “Adding a VRRP Instance”](#).

Section 5.26.6.2

Adding a VRRP Instance

To add a VRRP instance, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Make sure a VRRP group has been configured. For more information, refer to [Section 5.26.5.2, “Adding a VRRP Group”](#).
- 3. Navigate to *services » vrrp » instance* and click **<Add instance>**. The **Key Settings** form appears.



A screenshot of the "Key settings" form in the web interface. It features a text input field for "Instance Name" with a red asterisk indicating it is required, and a blue question mark icon. Below the field is a green placeholder text "<string>". To the right of the field is a dark blue "Add" button. Numbered callouts point to the input field (1) and the "Add" button (2).

Figure 711: Key Settings Form

1. Instance Name Box    2. Add Button

- 4. Configure the following parameter(s) as required:

Parameter	Description
Instance Name	<b>Synopsis:</b> A string 1 to 64 characters long The name of the VRRP instance - the name must not include spaces.

- 5. Click **Add** to add the instance. The **VRRP Instance** form appears.

The screenshot shows the 'VRRP Instance' configuration form. It contains the following fields and settings, with numbered callouts indicating their positions:

- 1** points to the **VRRP Version \*** field, which is set to 3 (with a sub-value of 2).
- 2** points to the **Interface \*** dropdown menu, which is set to 'switch.0001'.
- 3** points to the **Virtual Router ID \*** field, which is set to 41.
- 4** points to the **Priority \*** field, which is set to 9.
- 5** points to the **Advertisement Interval MilliSecond \*** field, which is set to 100 (with a sub-value of 1000).
- 6** points to the **Gratuitous ARP Delay \*** field, which is set to 5 (with a sub-value of 5).
- 7** points to the **No Preempt** checkbox, which is checked (Enabled).
- 8** points to the **Preempt Delay \*** field, which is set to 0 (with a sub-value of 0).
- 9** points to the **Fault to Master Delay \*** field, which is set to 0 (with a sub-value of 0).
- 10** points to the **Use Virtual MAC** checkbox, which is checked (Enabled).
- 11** points to the **VRRP Group** dropdown menu, which is set to an empty value.

**Figure 712: VRRP Instance Form**

1. VRRP Version   2. Interface List   3. Virtual Router ID Box   4. Priority Box   5. Advertisement Interval Box   6. Gratuitous ARP Delay Box   7. No Preempt Box   8. Preempt Delay Box   9. Fault to Master Delay Box   10. Use Virtual MAC Check Box   11. VRRP Group List

6. Configure the following parameter(s) as required:



**NOTE**

*A preemption occurs when either:*

- a backup VRRP router gains higher priority and transitions to the Master state
- VRRP is initiated and this router has higher priority than that of any VRRP router on the network



#### NOTE

The VRRP Instance Form displays some fields differently depending on whether version 2 or version 3 is chosen in the version field.

- Choosing VRRP version 2 displays the **Advertisement Interval** field.
- Choosing VRRP version 3 displays the **Advertisement Interval Millisecond** field.

Parameter	Description
VRRP Version	<b>Synopsis:</b> An integer between 2 and 3 <b>Default:</b> 2 Configure VRRP version for this instance.
Interface	The interface that will host the VRIP when the router becomes the VRRP Master.
Virtual Router ID	<b>Synopsis:</b> An integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID.
Priority	<b>Synopsis:</b> An integer between 0 and 255 The priority for the VRRP instance. When electing the master, the highest priority wins. The configurable range is 1 to 255. A value of zero (0) is invalid.
Advertisement Interval	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1 VRRP2 advertisement interval, in seconds.
Advertisement Interval MilliSecond	<b>Synopsis:</b> An integer between 20 and 3000 <b>Default:</b> 1000 <b>Prerequisite:</b> Value of advert-interval-millisecond must be multiple of 10. VRRP3 advertisement interval in millisecond, must be multiple of 10.
Gratuitous ARP Delay	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 5 Gratuitous ARP delay, in seconds. Sets the delay after the router changes state before a second set of gratuitous ARPs are sent.
No Preempt	<b>Synopsis:</b> typeless When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
Preempt Delay	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0 The time, in seconds, after startup until preemption.
Fault to Master Delay	<b>Synopsis:</b> An integer between 0 and 1000 <b>Default:</b> 0 The delay, in seconds, before a transition from the fault state to the master state occurs, thereby preempting the current master.
Use Virtual MAC	<b>Synopsis:</b> typeless



Parameter	Description
	When enabled, the router uses a virtual MAC address for the VRIP interface.
VRRP Group	Binds this VRRP instance to a VRRP group.

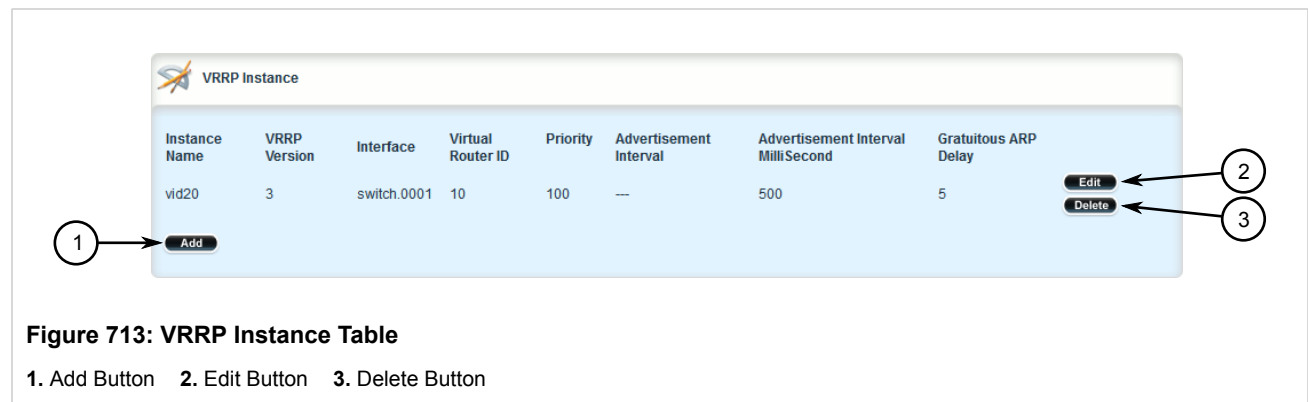
7. Add one or more VRRP monitors. For more information, refer to [Section 5.26.7.2, “Adding a VRRP Monitor”](#).
8. Add one or more track scripts. For more information, refer to [Section 5.26.8.2, “Adding a Track Script”](#).
9. Add one or more virtual IP addresses. For more information, refer to [Section 5.26.9.2, “Adding a Virtual IP Address”](#).
10. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
11. Click **Exit Transaction** or continue making changes.

## Section 5.26.6.3

## Deleting a VRRP Instance

To delete a VRRP instance, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » instance**. The **VRRP Instance** table appears.



**Figure 713: VRRP Instance Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen instance.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.26.7

## 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.

The following sections describe how to configure and manage VRRP monitors:

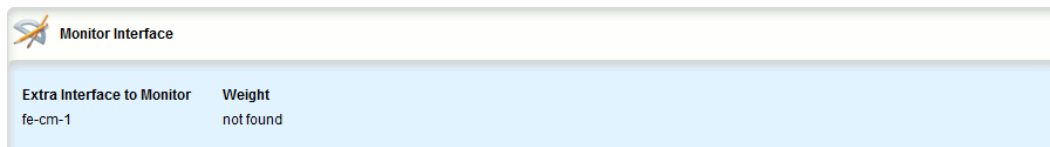
- [Section 5.26.7.1, “Viewing a List of VRRP Monitors”](#)

- [Section 5.26.7.2, “Adding a VRRP Monitor”](#)
- [Section 5.26.7.3, “Deleting a VRRP Monitor”](#)

#### Section 5.26.7.1

### Viewing a List of VRRP Monitors

To view a list of VRRP monitors, navigate to **services » vrrp » instance » {name} » monitor**, where {name} is the name of the VRRP instance. If monitors have been configured, the **Monitor Interface** table appears.



Monitor Interface	
Extra Interface to Monitor	Weight
fe-cm-1	not found

**Figure 714: Monitor Interface Table**

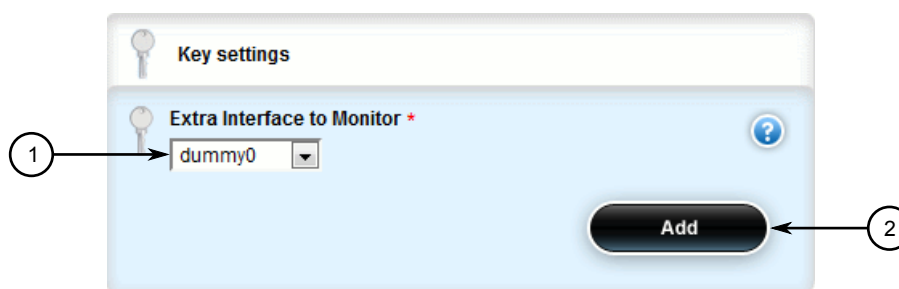
If no VRRP monitors have been configured, add monitors as needed. For more information, refer to [Section 5.26.7.2, “Adding a VRRP Monitor”](#).

#### Section 5.26.7.2

### Adding a VRRP Monitor

To add a VRRP monitor, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » instance » {name} » monitor**, where {name} is the name of the VRRP instance.
3. Click **<Add monitor>**. The **Key Settings** form appears.



Key settings

Extra Interface to Monitor \*

dummy0

Add

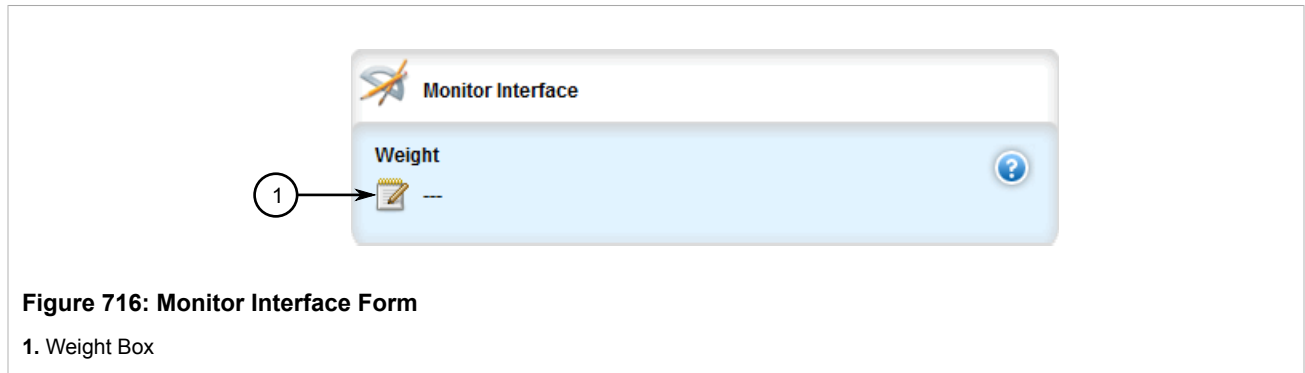
**Figure 715: Key Settings Form**

1. Extra Interface to Monitor Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Extra Interface to Monitor	The name of the interface.

- Click **Add** to add the monitor. The **Monitor Interface** form appears.



- Configure the following parameter(s) as required:

Parameter	Description
Weight	<p><b>Synopsis:</b> An integer between -254 and 254</p> <p>The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the interface falls. 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 falls.</p>

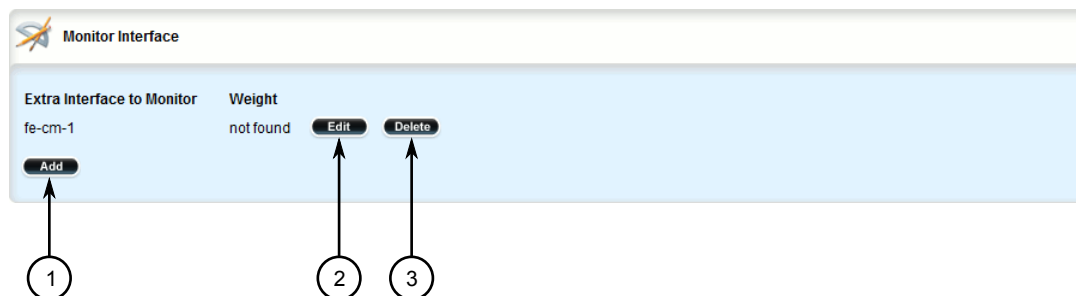
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.26.7.3

## Deleting a VRRP Monitor

To delete a VRRP monitor, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » vrrp » instance » {name} » monitor**, where {name} is the name of the VRRP instance. The **Monitor Interface** table appears.



**Figure 717: Monitor Interface Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen monitor.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.26.8

## Managing Track Scripts

Track scripts are used to associate VRRP trackers with VRRP instances.

The following sections describe how to configure and manage track scripts:

- [Section 5.26.8.1, “Viewing a List of Track Scripts”](#)
- [Section 5.26.8.2, “Adding a Track Script”](#)
- [Section 5.26.8.3, “Deleting a Track Script”](#)

#### Section 5.26.8.1

### Viewing a List of Track Scripts

To view a list of track scripts, navigate to **services » vrrp » instance » {name} » track-script**, where {name} is the name of the VRRP instance. If track scripts have been configured, the **Track Script** table appears.

Tracker	Weight
tracker1	not found

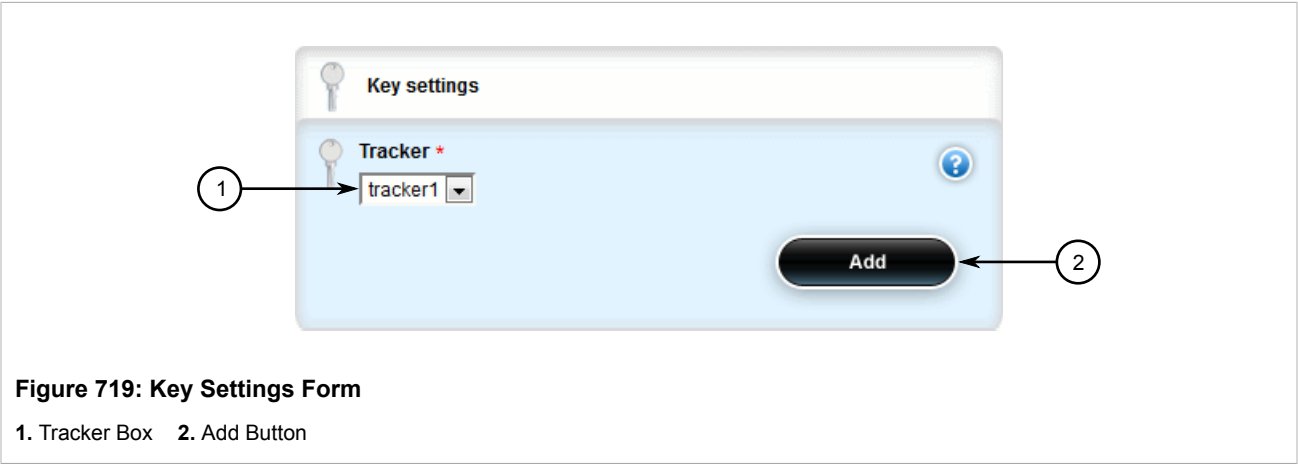
**Figure 718: Track Script Table**

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to [Section 5.26.7.2, “Adding a VRRP Monitor”](#).

Section 5.26.8.2

Adding a Track Script

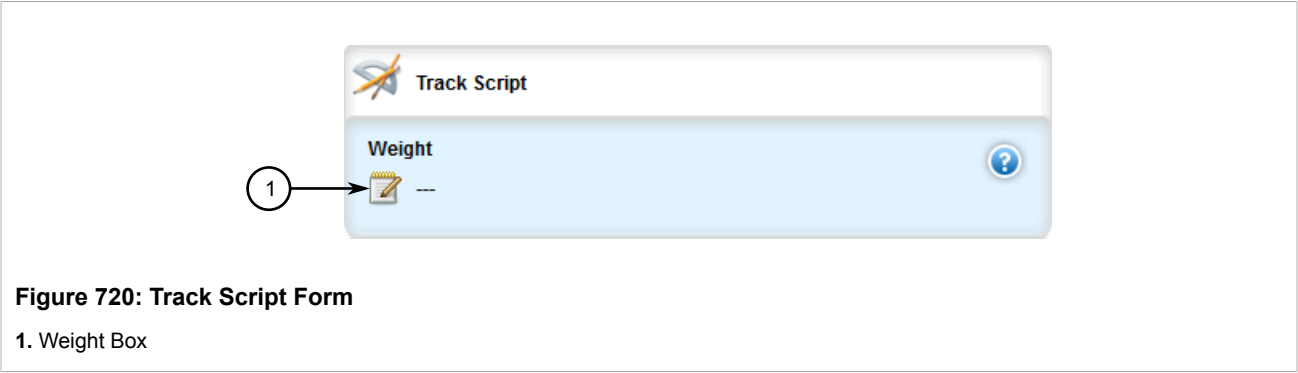
- To add a track script, do the following:
1. Change the mode to **Edit Private** or **Edit Exclusive**.
  2. Navigate to **services » vrrp » instance » {name} » track-script**, where {name} is the name of the VRRP instance.
  3. Click **<Add track-script>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Tracker	Select a tracker to monitor VRRP instance.

5. Click **Add** to add the track script. The **Track Script** form appears.



6. Configure the following parameter(s) as required:

Parameter	Description
Weight	<b>Synopsis:</b> An integer between 254 and 254  This setting overwrites the weight setting in the tracker. If negative, the priority decreases by this amount when the tracker falls. If positive, the priority increases by this amount when the tracker rises. If not set, the weight value in the tracker will be used.

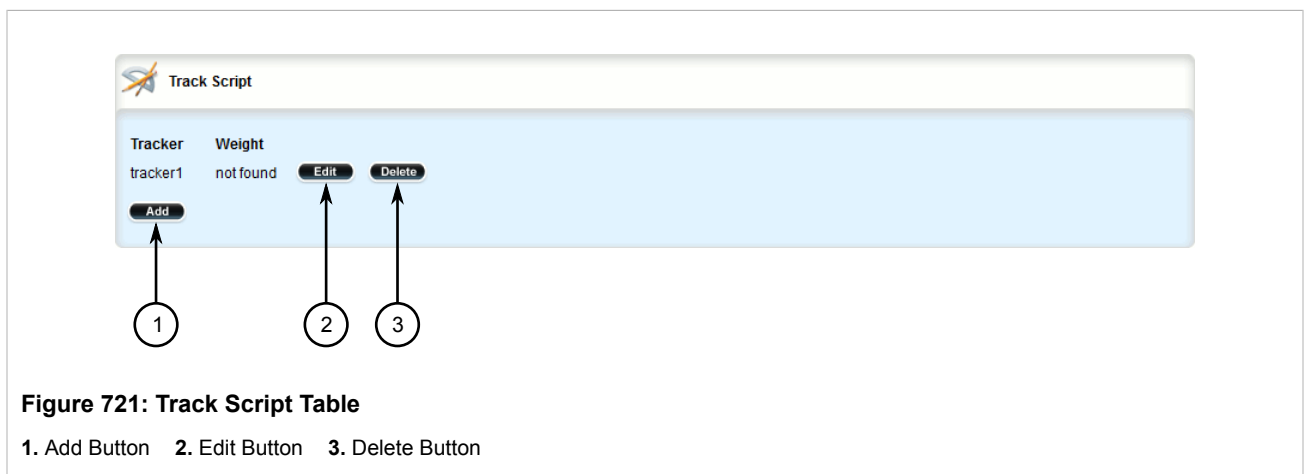
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.26.8.3

## Deleting a Track Script

To delete a track script, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » instance » {name} » track-script**, where {name} is the name of the VRRP instance. The **Track Script** table appears.



3. Click **Delete** next to the chosen track script.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.26.9

## Managing Virtual IP Addresses

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

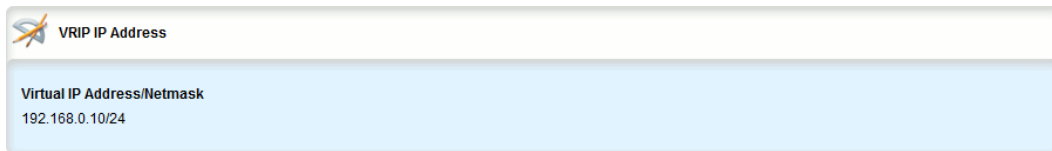
The following sections describe how to configure and manage virtual IP addresses:

- [Section 5.26.9.1, “Viewing a List of Virtual IP Addresses”](#)
- [Section 5.26.9.2, “Adding a Virtual IP Address”](#)
- [Section 5.26.9.3, “Deleting a Virtual IP Address”](#)

## Section 5.26.9.1

## Viewing a List of Virtual IP Addresses

To view a list of virtual IP addresses, navigate to **services » vrrp » instance » {name} » vrip**, where {name} is the name of the VRRP instance. If addresses have been configured, the **VRIP IP Address** table appears.



Virtual IP Address/Netmask
192.168.0.10/24

**Figure 722: VRIP IP Address Table**

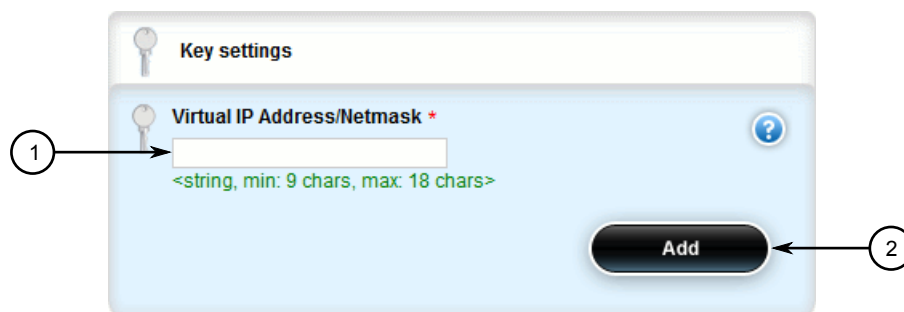
If no virtual IP addresses have been configured, add addresses as needed. For more information, refer to [Section 5.26.9.2, “Adding a Virtual IP Address”](#).

## Section 5.26.9.2

## Adding a Virtual IP Address

To add a virtual IP address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » instance » {name} » vrip**, where {name} is the name of the VRRP instance.
3. Click **<Add vrip>**. The **Key Settings** form appears.



**Figure 723: Key Settings Form**

1. Virtual IP Address/Netmask Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Virtual IP Address/Netmask	<b>Synopsis:</b> A string 9 to 18 characters long The virtual IP address/netmask.

5. Click **Add** to add the virtual IP address.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

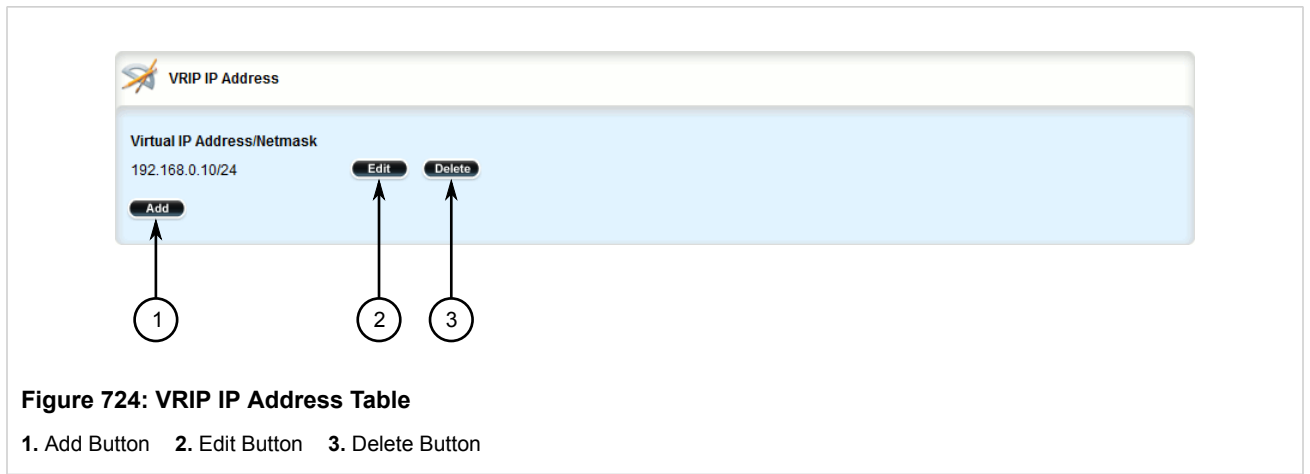
7. Click **Exit Transaction** or continue making changes.

### Section 5.26.9.3

## Deleting a Virtual IP Address

To delete a virtual IP address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » vrrp » instance » {name} » vrip**, where {name} is the name of the VRRP instance. The **VRIP IP Address** table appears.



3. Click **Delete** next to the chosen address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.27

## Managing Link Failover Protection

Link failover provides an easily configurable means of raising a backup link upon the failure of a designated main link. The main and backup links can only be Ethernet.

Link failover can back up to multiple remote locations, managing multiple main-to-backup link relationships.

Link failover can also be used to migrate the default route from the main link to the backup link.

The time after a main link failure to backup link startup, and the time after a main link recovery to backup link stoppage, are configurable. The link failover function also provides failover status information and a test of the failover settings.

The following sections describe how to configure link failover protection:

- [Section 5.27.1, “Viewing the Link Failover Log”](#)
- [Section 5.27.2, “Viewing the Link Failover Status”](#)
- [Section 5.27.3, “Managing Link Failover Parameters”](#)
- [Section 5.27.4, “Managing Link Failover Backup Interfaces”](#)



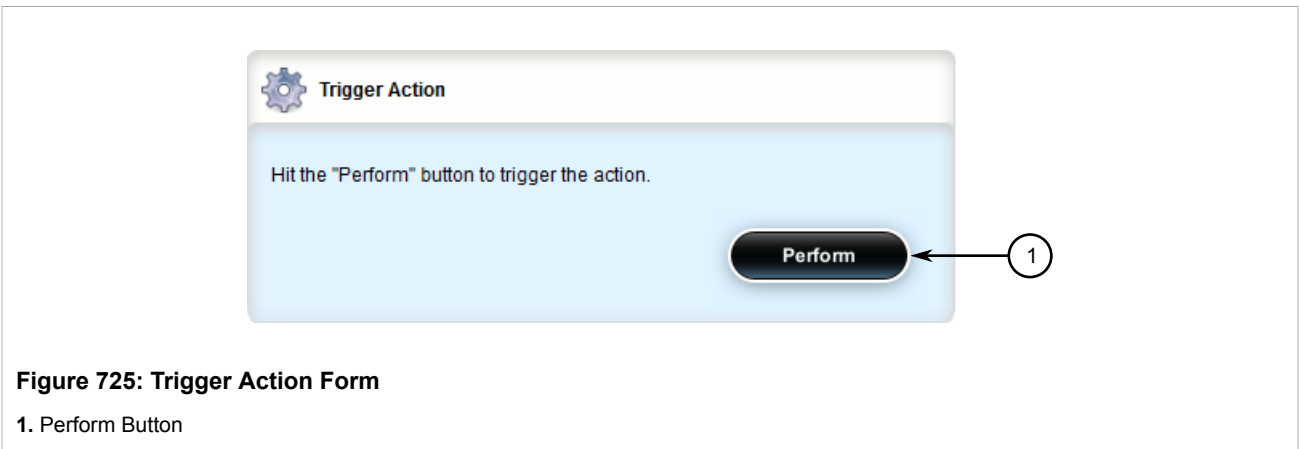
- [Section 5.27.5, “Managing Link Failover Ping Targets”](#)
- [Section 5.27.6, “Testing Link Failover”](#)
- [Section 5.27.7, “Canceling a Link Failover Test”](#)

### Section 5.27.1

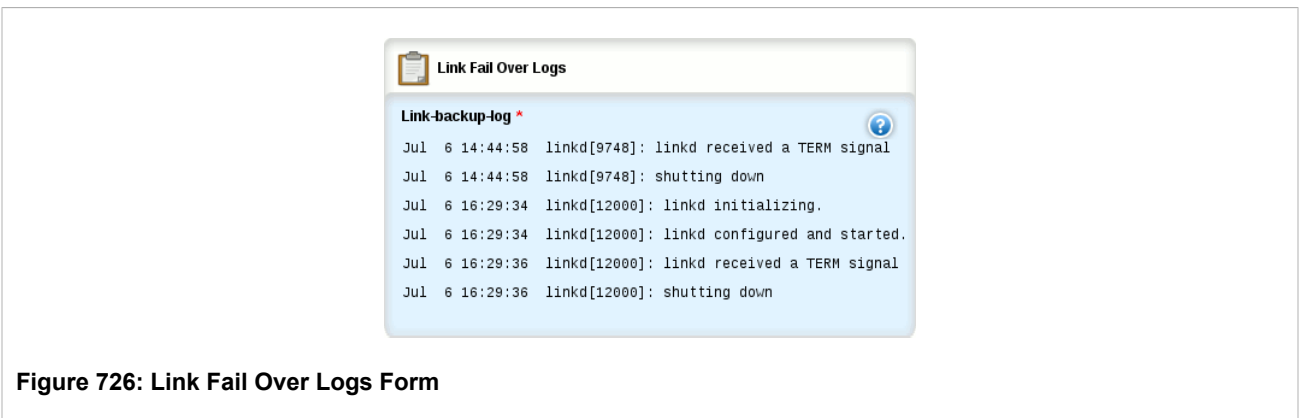
## Viewing the Link Failover Log

To view the link failover log, do the following:

1. Navigate to **services » link-failover » {interface}**, where *{interface}* is the name of the interface.
2. Click **log** in the menu. The **Trigger Action** form appears.



3. Click **Perform**. The **Link Failover Logs** form appears.



### Section 5.27.2

## Viewing the Link Failover Status

The Link Failover Status form displays the current link failover status. To view the link failover status, navigate to **services » link-failover » {interface} » status**, where *{interface}* is the name of the interface. The **Link Fail Over Status** form appears.

Link Fail Over Status		
1	<b>Main-link-status</b> up	?
2	<b>Backup-link-status</b> up	?
3	<b>Main-ping-test</b> ok	?
4	<b>Time-of-last-state-change</b> Mon Oct 18 12:22:19 2012	?
5	<b>Link-backup-state</b> Main path is active	?
6	<b>Backup-interface-in-use</b> switch.0002	?

Figure 727: Link Fail Over Status Form

1. Main Link Status    2. Backup Link Status    3. Main Ping Test    4. Time of Last State Change    5. Link Backup State    6. Backup Interface in Use

This form provides the following information:

Parameter	Description
main-link-status	<b>Synopsis:</b> A string The main link status.
backup-link-status	<b>Synopsis:</b> A string The backup link status.
main-ping-test	<b>Synopsis:</b> A string The results of pinging the target using the main interface.
time-of-last-state-change	<b>Synopsis:</b> A string The time of the last state change.
link-backup-state	<b>Synopsis:</b> A string The backup link state.
backup-interface-in-use	<b>Synopsis:</b> A string The name of the backup interface that is being used.

Section 5.27.3

# Managing Link Failover Parameters

The following sections describe how to configure and manage parameters for link failover protection:

- [Section 5.27.3.1, “Viewing a List of Link Failover Parameters”](#)

- [Section 5.27.3.2, “Adding a Link Failover Parameter”](#)
- [Section 5.27.3.3, “Deleting a Link Failover Parameter”](#)

Section 5.27.3.1

Viewing a List of Link Failover Parameters

To view a list of link failover parameters, navigate to **services » link-failover**. If parameters have been configured, the **Link Failover Information** table appears.

Link Failover Information							
Main	Enabled	Ping-timeout	Ping-interval	Ping-retry	Start-delay	Main-down-timeout	Main-up-timeout
switch.0001	enabled	2	60	3	180	60	60

Figure 728: Link Failover Information Table

If no parameters have been configured, add parameters as needed. For more information, refer to [Section 5.27.3.2, “Adding a Link Failover Parameter”](#).

Section 5.27.3.2

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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » link-failover** and click **<Add link-failover>**. The **Key Settings** form appears.

Figure 729: Key Settings Form

1. Main List    2. Add Button

3. Select the main interface from the list.

4. Click **Add** to add the main interface. The **Link Fail Over Settings** form appears.

The screenshot shows the 'Link Fail Over Settings' form. It has a title bar with a logo and the text 'Link Fail Over Settings'. Below the title bar, there are seven settings, each with a label, a value, a default value in parentheses, and a help icon (a question mark in a blue circle). The settings are: 1. 'Enabled' with a checkbox and the value 'Enabled'. 2. 'Ping-timeout \*' with a value of '2' and a default of '(2)'. 3. 'Ping-interval \*' with a value of '60' and a default of '(60)'. 4. 'Ping-retry \*' with a value of '3' and a default of '(3)'. 5. 'Start-delay \*' with a value of '180' and a default of '(180)'. 6. 'Main-down-timeout \*' with a value of '60' and a default of '(60)'. 7. 'Main-up-timeout \*' with a value of '60' and a default of '(60)'. Each setting has a small icon of a notepad and pencil next to the value.

**Figure 730: Link Fail Over Settings Form**

1. Enabled Check Box   2. Ping Timeout Box   3. Ping Interval Box   4. Ping Retry Box   5. Start Delay Box   6. Main Down Timeout Box   7. Main Up Timeout Box

5. Configure the following parameter(s) as required:

Parameter	Description
enabled	<b>Synopsis:</b> typeless Enables this link backup.
Ping Timeout	<b>Synopsis:</b> An integer between 1 and 65536 <b>Default:</b> 2 The time interval, in seconds, before immediately retrying a ping.
Ping Interval	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 60 The time interval, in seconds, between ping tests.
Ping Retry	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 3

Parameter	Description
	The number of ping retries before constructing a path failure.
Start Delay	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 180 The delay time, in seconds, when first starting link failover.
Main Down Timeout	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 60 The delay time, in seconds, that the main trunk is down before starting the backup trunk.
Main Up Timeout	<b>Synopsis:</b> An integer between 0 and 65536 <b>Default:</b> 60 The delay time, in seconds, to confirm that the main trunk is up (returned to service) before stopping the backup trunk.

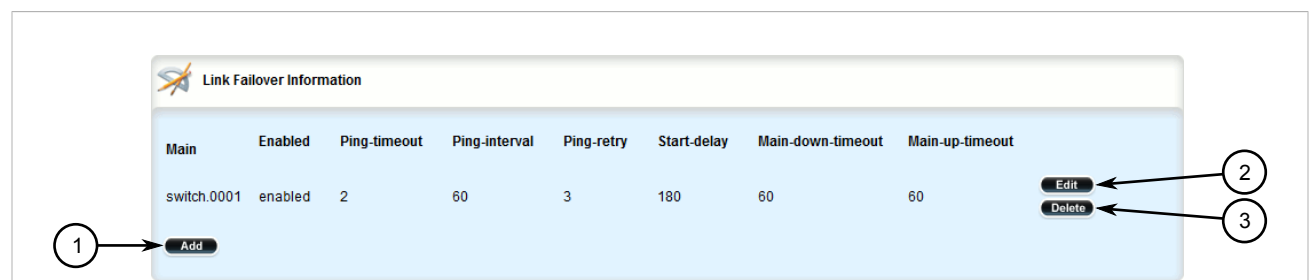
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.27.3.3

## Deleting a Link Failover Parameter

To delete a link failover parameter, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » link-failover**. The **Link Failover Information** table appears.



**Figure 731: Link Failover Information Table**

1. Add Button    2. Edit Button    3. Delete Button

- Click **Delete** next to the chosen parameter.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.27.4

## 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.

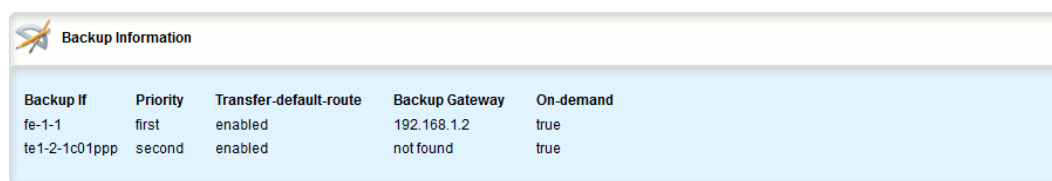
The following sections describe how to configure and manage backup interfaces for link failover protection:

- [Section 5.27.4.1, “Viewing a List of Link Failover Backup Interfaces”](#)
- [Section 5.27.4.2, “Adding a Link Failover Backup Interface”](#)
- [Section 5.27.4.3, “Deleting a Link Failover Backup Interface”](#)

## Section 5.27.4.1

### Viewing a List of Link Failover Backup Interfaces

To view a list of link failover backup interfaces, navigate to **services » link-failover » {interface} » backup**, where *{interface}* is the name of the interface. If backup interfaces have been configured, the **Backup Information** table appears.



Backup If	Priority	Transfer-default-route	Backup Gateway	On-demand
fe-1-1	first	enabled	192.168.1.2	true
te1-2-1c01ppp	second	enabled	not found	true

**Figure 732: Backup Information Table**

If no backup interfaces have been configured, add backup interfaces as needed. For more information, refer to [Section 5.27.4.2, “Adding a Link Failover Backup Interface”](#).

## Section 5.27.4.2

### Adding a Link Failover Backup Interface

To set a link failover backup interface, do the following:

**CAUTION!**

*Configuration hazard – risk of connection loss. If a RUGGEDCOM APE module is installed, either avoid configuring switch.0001 as a link failover backup interface or configure a different VLAN for the APE module. By default, APE modules utilize VLAN 1 (switch.0001) and always keep the interface in the UP state. This would interfere with the link failover mechanism.*

*To configure a different VLAN for the APE module, change the PVID for the associated switched Ethernet port. For information, refer to [Section 3.18.2, “Configuring a Switched Ethernet Port”](#).*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » link-failover » {interface} » backup**, where *{interface}* is the name of the interface.
3. Click **<Add backup>**. The **Key Settings** form appears.

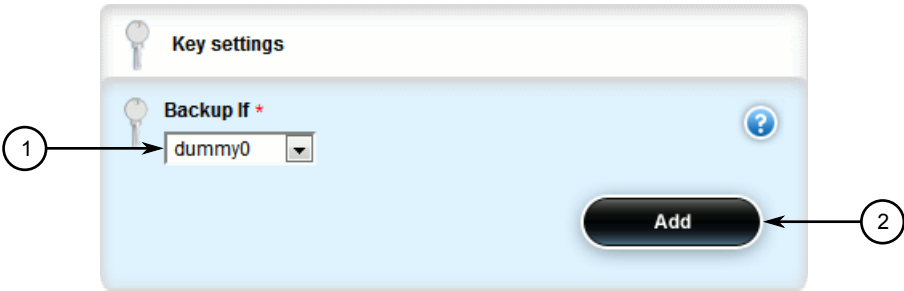


Figure 733: Key Settings Form

1. Backup Interface List    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
backuplf	The interface used to back up the main interface.

5. Click **Add**. The **Backup Settings** form appears.

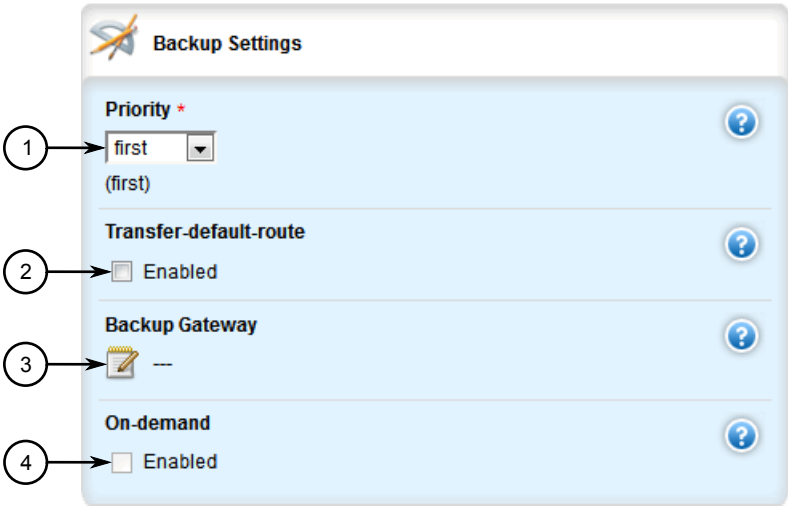


Figure 734: Backup Settings Form

1. Priority List    2. Transfer Default Route Check Box    3. Backup Gateway Box    4. On Demand Check Box

6. Configure the following parameter(s) as required:



**NOTE**

Do not configure the **Backup Gateway** parameter for Point to Point (P2P) links.



**NOTE**

The **On Demand** parameter is set at the interface itself.

Parameter	Description
priority	<b>Synopsis:</b> { third, second, first } <b>Default:</b> first The priority which is applied to the backup interface when switching.
Transfer Default Route	<b>Synopsis:</b> typeless The transfer default gateway on the switching main and backup interface. The default route on the device must have a <i>distance</i> greater than one.
Backup Gateway	<b>Synopsis:</b> A string 1 to 15 characters long The IP address of the backup gateway.
on-demand	<b>Synopsis:</b> true or 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.

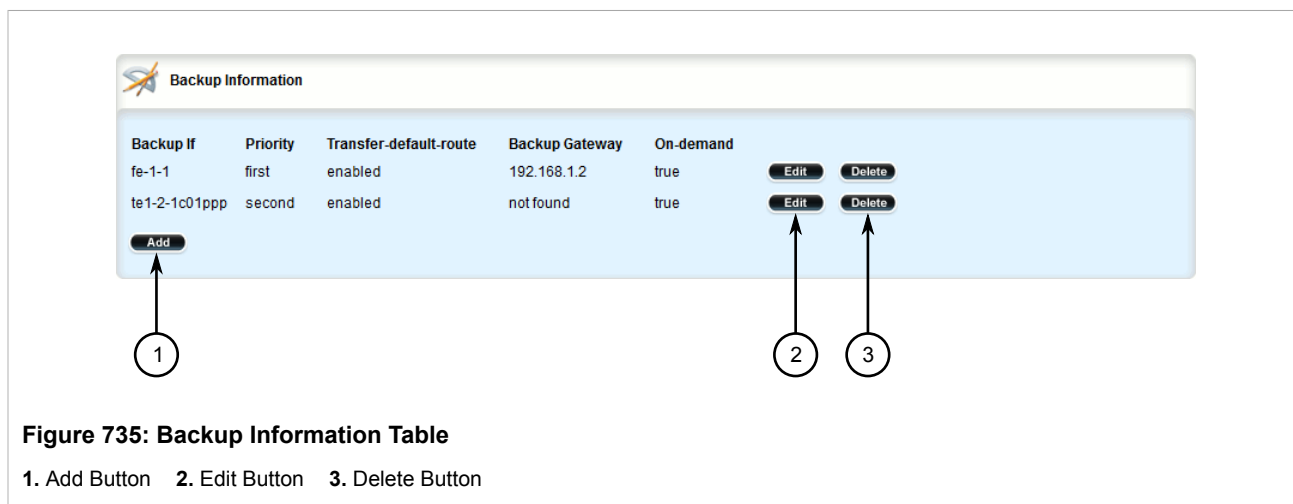
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.27.4.3

### Deleting a Link Failover Backup Interface

To delete a link failover backup interface, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **services » link-failover » {interface} » backup**, where *{interface}* is the name of the interface. The **Backup Information** table appears.



- Click **Delete** next to the chosen backup interface.



- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.27.5

## 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.

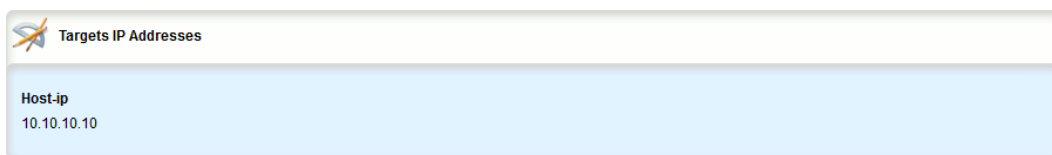
The following sections describe how to configure and manage ping targets for link failover protection:

- [Section 5.27.5.1, “Viewing a List of Link Failover Ping Targets”](#)
- [Section 5.27.5.2, “Adding a Link Failover Ping Target”](#)
- [Section 5.27.5.3, “Deleting a Link Failover Ping target”](#)

## Section 5.27.5.1

### Viewing a List of Link Failover Ping Targets

To view a list of link failover ping targets, navigate to **services » link-failover » {interface} » target**, where **{interface}** is the name of the interface. If ping targets have been configured, the **Targets IP Addresses** table appears.



Host-ip
10.10.10.10

**Figure 736: Targets IP Addresses Table**

If no ping targets have been configured, add targets as needed. For more information, refer to [Section 5.27.5.2, “Adding a Link Failover Ping Target”](#).

## Section 5.27.5.2

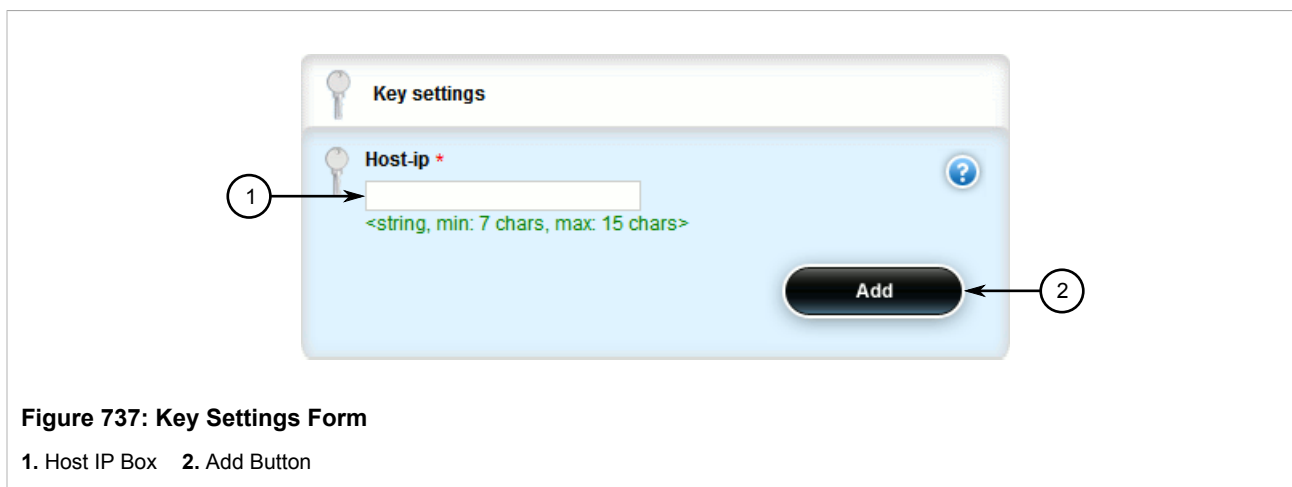
### Adding a Link Failover Ping Target

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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » link-failover » {interface} » target**, where {interface} is the name of the interface.
3. Click **<Add target>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
host-ip	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the target host to verify the main path.

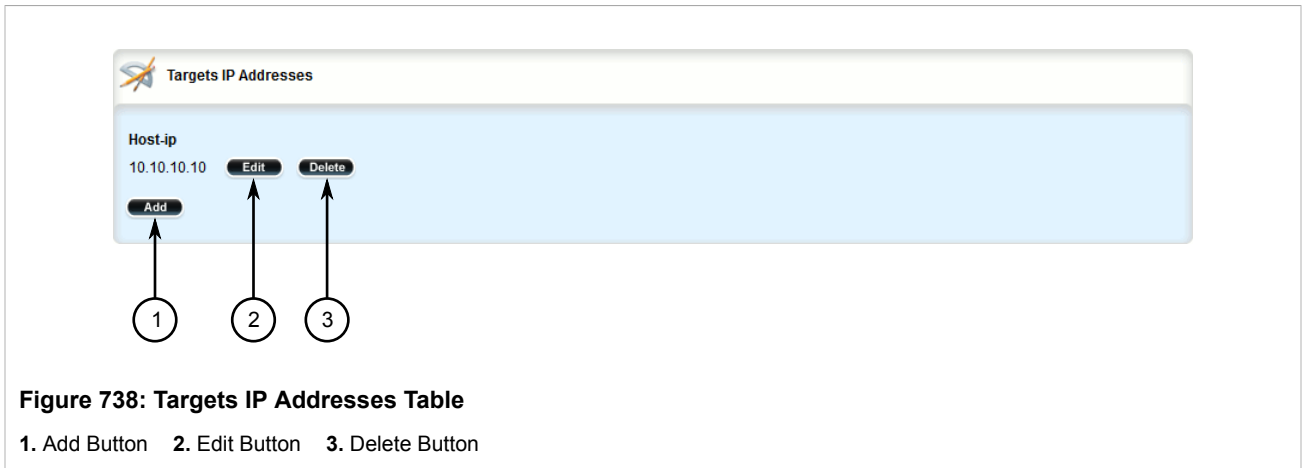
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 5.27.5.3

### Deleting a Link Failover Ping target

To delete a link failover ping target, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **services » link-failover » {interface} » target**, where {interface} is the name of the interface. The **Targets IP Addresses** table appears.



3. Click **Delete** next to the chosen ping target.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.27.6

## 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 5.27.2, “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 5.27.7, “Canceling a Link Failover Test”](#).*

*Canceling the test returns the interfaces to their pre-test condition.*

1. In normal mode or edit mode, navigate to **services » link-failover{interface id} » start-test**, where *{interface id}* is interface to be tested. The **Link Failover Test Settings** and **Trigger Action** forms appear.

**Figure 739: Link Failover Test Settings Form**

1. Test Duration Box    2. Start Test Delay Box

**Figure 740: Trigger Action Form**

1. Perform Button

- Configure the following parameter(s) as required:

Parameter	Description
test-duration	<b>Synopsis:</b> An integer between 1 and 65536 <b>Default:</b> 5 The amount of time (in minutes) to run before restoring service to the main trunk.
start-test-delay	<b>Synopsis:</b> An integer between 1 and 65536 <b>Default:</b> 1 The amount of waiting time (in minutes) before running the test.

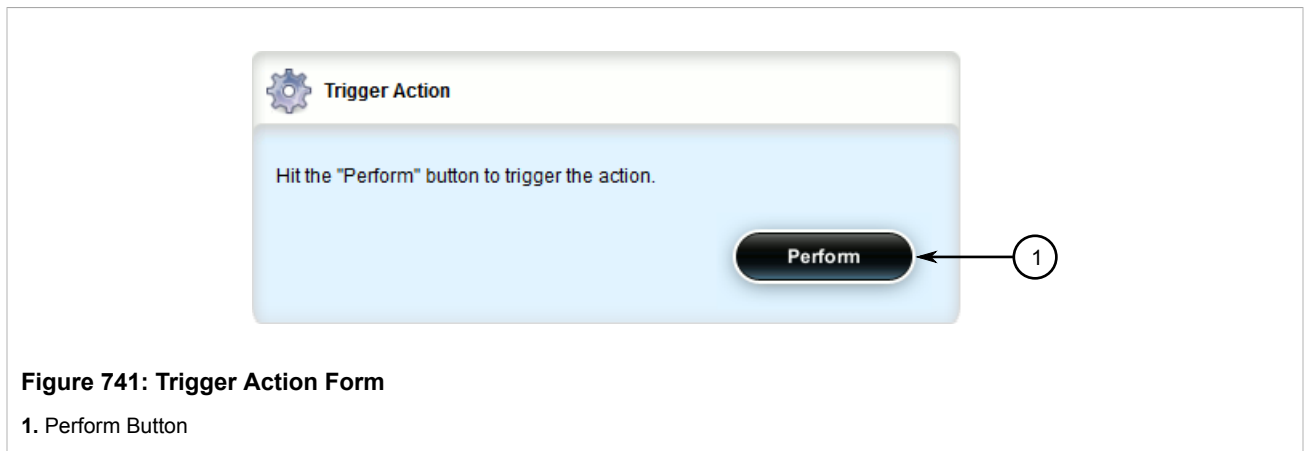
- On the **Trigger Action** form, click **Perform** to begin the test.

#### Section 5.27.7

## Canceling a Link Failover Test

To cancel a link failover test, do the following:

- In normal mode or edit mode, navigate to **services » link-failover » {interface} » cancel-test**, where **{interface}** is the name of the interface. The **Trigger Action** forms appear.



2. Click **Perform** to cancel the test.

## Section 5.28

# 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 5.28.1, “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 5.12.11, “Managing NTP Servers”](#).*

The following sections describe how to configure and manage an IPsec tunnel:

- [Section 5.28.1, “IPsec Tunneling Concepts”](#)
- [Section 5.28.2, “Configuring IPsec Tunnels”](#)
- [Section 5.28.3, “Configuring Certificates and Keys”](#)
- [Section 5.28.4, “Viewing the IPsec Tunnel Status”](#)
- [Section 5.28.5, “Managing Pre-Shared Keys”](#)
- [Section 5.28.6, “Managing Connections”](#)
- [Section 5.28.7, “Managing the Internet Key Exchange \(IKE\) Protocol”](#)
- [Section 5.28.8, “Managing the Encapsulated Security Payload \(ESP\) Protocol”](#)
- [Section 5.28.9, “Configuring the Connection Ends”](#)
- [Section 5.28.10, “Managing Private Subnets”](#)

Section 5.28.1

## 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. Openswan 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.

The following sections provide more information about IPsec and its implementation in RUGGEDCOM ROX II:

- [Section 5.28.1.1, "IPsec Modes"](#)
- [Section 5.28.1.2, "Supported Encryption Protocols"](#)
- [Section 5.28.1.3, "Public and Secret Key Cryptography"](#)
- [Section 5.28.1.4, "X509 Certificates"](#)
- [Section 5.28.1.5, "NAT Traversal"](#)
- [Section 5.28.1.6, "Remote IPsec Client Support"](#)
- [Section 5.28.1.7, "IPsec and Router Interfaces"](#)

Section 5.28.1.1

### 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 5.28.1.2

### Supported Encryption Protocols

Openswan supports the following standard encryption protocols:

- **3DES (Triple DES)**

Uses three 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 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 5.28.1.3

## 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 5.28.5, “Managing Pre-Shared Keys”](#).

Section 5.28.1.4

## 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 5.28.1.5

## 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 5.28.2, “Configuring IPsec Tunnels”](#).

Section 5.28.1.6

## 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 5.16.6, “Configuring the Firewall for a VPN”](#).

#### Section 5.28.1.7

## 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 5.28.6, “Managing Connections”](#).

#### Section 5.28.2

## Configuring IPsec Tunnels

To configure IPsec tunnels, do the following:



### NOTE

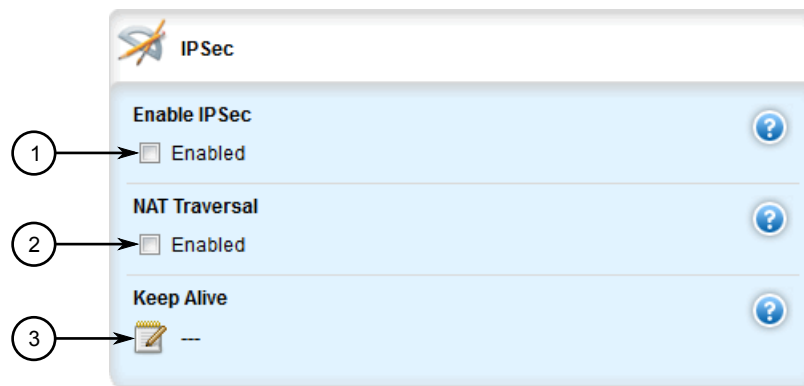
*RUGGEDCOM ROX II supports the creation of policy-based VPNs, which can be characterized as follows:*

- *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 5.16, “Managing Firewalls”](#).*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec**. The **IPsec** forms appear.



**Figure 742: IPsec Form**

1. Enable IPsec Check Box    2. NAT Traversal Check Box    3. Keep Alive Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable IPsec	<b>Synopsis:</b> typeless Enables IPsec.
NAT Traversal	<b>Synopsis:</b> typeless Enables NAT Traversal.
Keep Alive	<b>Synopsis:</b> An integer between 1 and 86400 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.

4. Configure one or more pre-shared keys. For more information, refer to [Section 5.28.5.2, “Adding a Pre-Shared Key”](#).
5. Configure one or more encrypted connections. For more information, refer to [Section 5.28.6.2, “Adding a Connection”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.28.3

## Configuring Certificates and Keys

To configure certificates and keys for IPsec Tunnels, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Add a CA certificate and Certificate Revocation List (CRL). For more information, refer to [Section 4.7.1.3, “Adding a CA Certificate and CRL”](#)
3. Add a private key. For more information, refer to [Section 4.7.2.2, “Adding a Private Key”](#).

4. Add a certificate. For more information, refer to [Section 4.7.4.3, “Adding a Certificate”](#).
5. Add a public key. For more information, refer to [Section 4.7.3.2, “Adding a Public Key”](#).
6. Navigate to **tunnel » ipsec » connection » {connection} » {end}**, where {connection} is the name of the connection and {end} is either the left (local router) or right (remote router) connection end. The **System Public Key** and **System Identifier** forms appear.

**Figure 743: System Public Key Form**

1. Type List   2. Certificate List (Hidden)   3. RSA Signature List (Hidden)

**Figure 744: System Identifier Form**

1. Type List   2. Hostname or IP Address

7. On the **System Public Key** form, set **Type** to **certificate**. The **Certificate** parameter appears.
8. Under the **Certificate** list, select the appropriate certificate.
9. On the **System Identifier** form, set **Type** to **from-certificate**.
10. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
11. Click **Exit Transaction** or continue making changes.

#### Section 5.28.4

## Viewing the IPsec Tunnel Status

To view the status of the IPsec tunnel, navigate to **tunnel » ipsec**. The **IPSec Status** form appears.

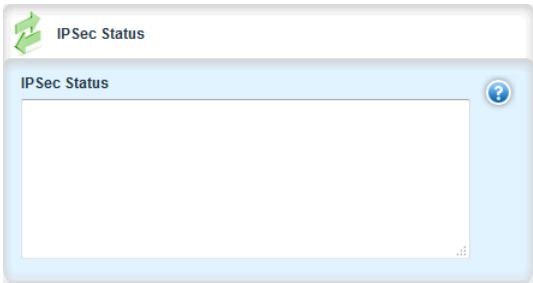


Figure 745: IPSec Status Form

This form provides a detailed log of all IPsec activity.

Section 5.28.5

# 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 5.28.1.3, “Public and Secret Key Cryptography”](#).

The following sections describe how to configure and manage pre-shared keys for IPsec tunnels:

- [Section 5.28.5.1, “Viewing a List of Pre-Shared Keys”](#)
- [Section 5.28.5.2, “Adding a Pre-Shared Key”](#)
- [Section 5.28.5.3, “Deleting a Pre-Shared Key”](#)

Section 5.28.5.1

## Viewing a List of Pre-Shared Keys

To view a list of pre-shared keys, navigate to **tunnel » ipsec » preshared-key**. If pre-shared keys have been configured, the **Preshared Key** table appears.

Preshared Key		
Remote Address	Local Address	Secret Key
192.168.12.1	192.168.12.2	\$4\$yosvKJcO1G0p9upunpxuZB/4aCKEnXopoSVkn...

Figure 746: Preshared Key Table

If no pre-shared keys have been configured, add pre-shared keys as needed. For more information, refer to [Section 5.28.5.2, “Adding a Pre-Shared Key”](#).

Section 5.28.5.2

## Adding a Pre-Shared Key

To add a pre-shared key, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » preshared-key** and click **<Add preshared-key>**. The **Key Settings** form appears.

The image shows a web form titled "Key settings" with a key icon. It contains two text input fields: "Remote Address \*" and "Local Address \*". Below each field is a green validation message: "(any | <string, min: 1 chars> | <string, min: 1 chars, max: 15 chars>)". A blue question mark icon is to the right of each field. At the bottom right is a black "Add" button. Three numbered callouts point to the form: (1) points to the Remote Address field, (2) points to the Local Address field, and (3) points to the Add button.

**Figure 747: Key Settings Form**

1. Remote Address Box   2. Local Address Box   3. Add Button

3. In the **Key Settings** form, configure the following parameters as required:

Parameter	Description
Remote Address	<b>Synopsis:</b> { any } or a string 7 to 15 characters long or a string 1 to 4095 characters long The remote address.
Local Address	<b>Synopsis:</b> { any } or a string 7 to 15 characters long or a string 1 to 4095 characters long The local address.

4. Click **Add** to create the new pre-shared key. The **Preshared Key** form appears.

The image shows a web form titled "Preshared Key" with a key icon. It contains a large text input field labeled "Secret Key \*". A blue question mark icon is to the right of the field. A numbered callout (1) points to the Secret Key field.

**Figure 748: Preshared Key Form**

1. Secret Key Box

5. In the **Preshared Key** form, configure the following parameters as required:

Parameter	Description
Secret Key	<b>Synopsis:</b> A string The pre-shared key.

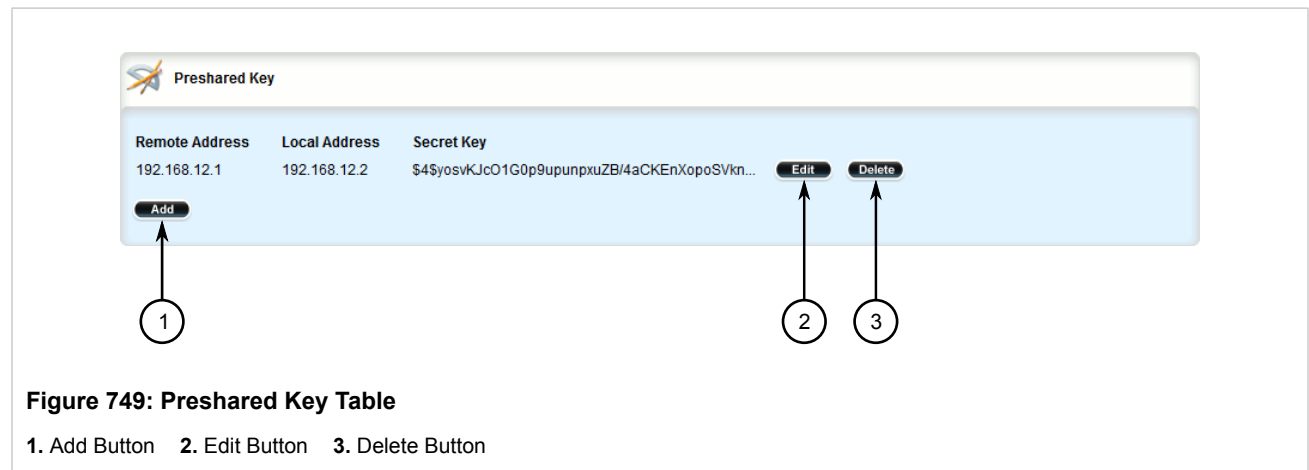
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.28.5.3

## Deleting a Pre-Shared Key

To delete a pre-shared key, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **tunnel » ipsec » preshared-key**. The **Preshared Key** table appears.



- Click **Delete** next to the chosen pre-shared key.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.28.6

## Managing Connections

An IPsec connection is an encrypted connection between two devices who share the same pre-authorized authentication key.

The following sections describe how to configure and manage connections for an IPsec connection:

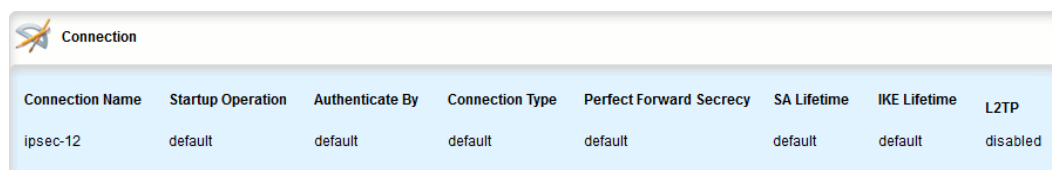
- [Section 5.28.6.1, “Viewing a List of Connections”](#)
- [Section 5.28.6.2, “Adding a Connection”](#)
- [Section 5.28.6.3, “Configuring Dead Peer Detection”](#)

- [Section 5.28.6.4, “Deleting a Connection”](#)

## Section 5.28.6.1

## Viewing a List of Connections

To view a list of connections configured for a VPN, navigate to **tunnel » ipsec » connection**. If connections have been configured, the **Connection** table appears.



Connection Name	Startup Operation	Authenticate By	Connection Type	Perfect Forward Secrecy	SA Lifetime	IKE Lifetime	L2TP
ipsec-12	default	default	default	default	default	default	disabled

**Figure 750: Connection Table**

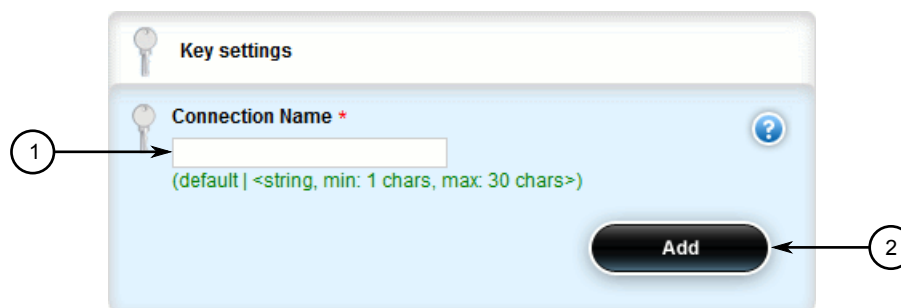
If no connections have been configured, add connections as needed. For more information, refer to [Section 5.28.6.2, “Adding a Connection”](#).

## Section 5.28.6.2

## Adding a Connection

To add a new connection for a VPN, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection** and click **<Add connection>**. The **Key Settings** form appears.



The screenshot shows the 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a form field labeled 'Connection Name \*' with a blue question mark icon to its right. Below the field is the text '(default | <string, min: 1 chars, max: 30 chars>)' in green. To the right of the field is a blue 'Add' button. A circled '1' with an arrow points to the 'Connection Name' field, and a circled '2' with an arrow points to the 'Add' button.

**Figure 751: Key Settings Form**

1. Connection Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Connection Name	<b>Synopsis:</b> { default } or a string 1 to 30 characters long The connection name. If the name is 'default', all settings are considered the default for all other connections.

4. Click **Add** to create the new connection. The **Connection** form appears.

The screenshot shows the 'Connection' configuration form. It has a title bar with a logo and the word 'Connection'. Below the title bar are several sections, each with a label and a dropdown menu or checkbox. Numbered callouts point to the following fields:

- 1. Startup Operation \* (dropdown menu)
- 2. Authenticate By \* (dropdown menu)
- 3. Connection Type \* (dropdown menu)
- 4. Perfect Forward Secrecy \* (dropdown menu)
- 5. SA Lifetime \* (dropdown menu)
- 6. IKE Lifetime \* (dropdown menu)
- 7. L2TP (checkbox)
- 8. Monitor Interface (dropdown menu)

**Figure 752: Connection Form**

1. Startup Operation List   2. Authenticate By List   3. Connection Type List   4. Perfect Forward Secrecy List   5. SA Lifetime Box  
6. IKE Lifetime Box   7. L2TP Check Box   8. Monitor Interface List

5. Configure the following parameter(s) as required:

Parameter	Description
Startup Operation	<b>Synopsis:</b> { ignore, add, start, route, default } <b>Default:</b> default The action to take when IPsec is initialized. The default value is 'ignore' unless overwritten by the default connection setting.
Authenticate By	<b>Synopsis:</b> { default, rsasig, secret } <b>Default:</b> default The authentication method. The default value is 'default' unless overwritten by the default connection setting.
Connection Type	<b>Synopsis:</b> { tunnel, transport, passthrough, default }

Parameter	Description
	<p><b>Default:</b> default</p> <p>The connection type/mode. Options include:</p> <ul style="list-style-type: none"> <li>&lt;itemizedlist&gt;&lt;listitem&gt;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.&lt;/listitem&gt;</li> <li>&lt;listitem&gt;transport: Encrypts traffic on a host-to-host tunnel.&lt;/listitem&gt;</li> <li>&lt;listitem&gt;passthrough: Traffic is not encrypted.&lt;/listitem&gt;&lt;/itemizedlist&gt;</li> </ul>
address-family	<p><b>Synopsis:</b> { ipv4, ipv6 }</p> <p><b>Default:</b> ipv4</p> <p>The address-family to run for the connection. Accepted values include 'ipv4' (default) and 'ipv6'. All addresses used in the connection must have the same address family.</p>
Perfect Forward Secrecy	<p><b>Synopsis:</b> { default, yes, no }</p> <p><b>Default:</b> default</p> <p>Enables/disables Perfect Forwarding Secrecy (PFS). When enabled, IPsec negotiates new keys for each session. If an attacker compromises a key, only the session protected by the key is revealed. Not all clients support PFS. The default value is 'yes' unless overwritten by the default connection setting.</p>
SA Lifetime	<p><b>Synopsis:</b> { default } or an integer between 1081 and 31104000</p> <p><b>Default:</b> default</p> <p>The lifetime in seconds for the Security Association (SA) key. This determines how long a particular instance of a connection should last, from successful negotiation to expiry. Normally, the connection is renegotiated before it expires. The default value is 28800 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the SA lifetime is longer.</p>
IKE Lifetime	<p><b>Synopsis:</b> { default } or an integer between 60 and 86400</p> <p><b>Default:</b> default</p> <p>The lifetime in seconds for the IKE protocol. This determines how long the IKE keying channel of a connection should last before being renegotiated. The default value is 3600 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the IKE lifetime is longer.</p>
L2TP	<p><b>Synopsis:</b> typeless</p> <p>Enables/disables L2TP for this connection.</p>
Monitor Interface	<p>The interface to monitor. If the selected interface goes down and then up, this connection will be restarted.</p>

- If required, enable and configure dead peer detection. For more information, refer to [Section 5.28.6.3, “Configuring Dead Peer Detection”](#).
- If required, configure the Internet Key Exchange (IKE) protocol by adding one or more algorithms. For more information, refer to [Section 5.28.7.2, “Adding an IKE Algorithm”](#)
- If required, configure Encapsulated Security Payload (ESP) encryption for the connection. For more information, refer to [Section 5.28.8, “Managing the Encapsulated Security Payload \(ESP\) Protocol”](#)
- If required, configure the left (local router) and right (remote router) ends of the connection. For more information, refer to [Section 5.28.9, “Configuring the Connection Ends”](#)



10. If required, configure L2TP tunnels. For more information, refer to [Section 5.30.2, “Configuring L2TP Tunnels”](#).
11. If certificates and keys are required, make sure they are configured on the device. For more information, refer to [Section 5.28.3, “Configuring Certificates and Keys”](#).
12. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
13. Click **Exit Transaction** or continue making changes.

## Section 5.28.6.3

## Configuring Dead Peer Detection

Dead Peer Detection (DPD), as defined in [RFC 3706](http://tools.ietf.org/html/rfc3706) [http://tools.ietf.org/html/rfc3706] is used to detect dead Internet Key Exchange (IKE) peers. In this method, peers exchange DPD Request (ISAKMP R-U-THERE) and DPD Response (ISAKMP R-U-THERE-ACK) messages. If a DPD Response is not received by a peer after a specified time and/or number of attempts, the other peer is considered *dead*. The remaining peer can either hold the connection until other peer responds, clear the connection, restart the connection and renegotiate the Security Association (SA), or restart all SA's to the dead peer.

In RUGGEDCOM ROX II, DPD Requests are sent when there is no traffic detected by the peer. How long to wait before sending a DPD Request and how long to wait for a DPD Response is user configurable.

It is generally recommended that DPD be configured to clear connections with any dead peers.

To configure dead peer detection for an IPsec connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {name}**, where **{name}** is the name of the connection. The **Dead Peer Detect** form appears.

Dead Peer Detect

1 → **Enable**  
☒ Enabled  
(false)

2 → **Interval**  
30  
(30)

3 → **Timeout**  
120  
(120)

4 → **Action**  
restart  
(restart)

**Figure 753: Dead Peer Detect Form**

1. Enabled Check Box   2. Interval Box   3. Timeout Box   4. Action List

- Configure the following parameter(s) as required:

**NOTE**

*The timeout period must be two minutes longer than the interval period.*

Parameter	Description
Enable	<b>Synopsis:</b> true or false <b>Default:</b> false Enables Dead Peer Detection (DPD) for this connection.
Interval	<b>Synopsis:</b> An integer between 1 and 3600 <b>Default:</b> 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	<b>Synopsis:</b> An integer between 1 and 28800 <b>Default:</b> 120 The time in seconds to wait before a peer is declared dead. <b>Prerequisite:</b> The timeout period must be more than two times the interval.
Action	<b>Synopsis:</b> { hold, clear, restart, restart-all-sa } <b>Default:</b> restart The action to be taken when a DPD enabled peer is declared dead. Options include: <ul style="list-style-type: none"><li>hold: The route will be put on hold status.</li><li>clear: The route and Security Association (SA) will both be cleared</li><li>restart: The SA will immediately be renegotiated</li><li>restart-all-sa: All SA's to the dead peer will be renegotiated</li></ul>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.28.6.4

## Deleting a Connection

To delete a connection for a VPN, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **tunnel » ipsec » connection**. The **Connection** table appears.

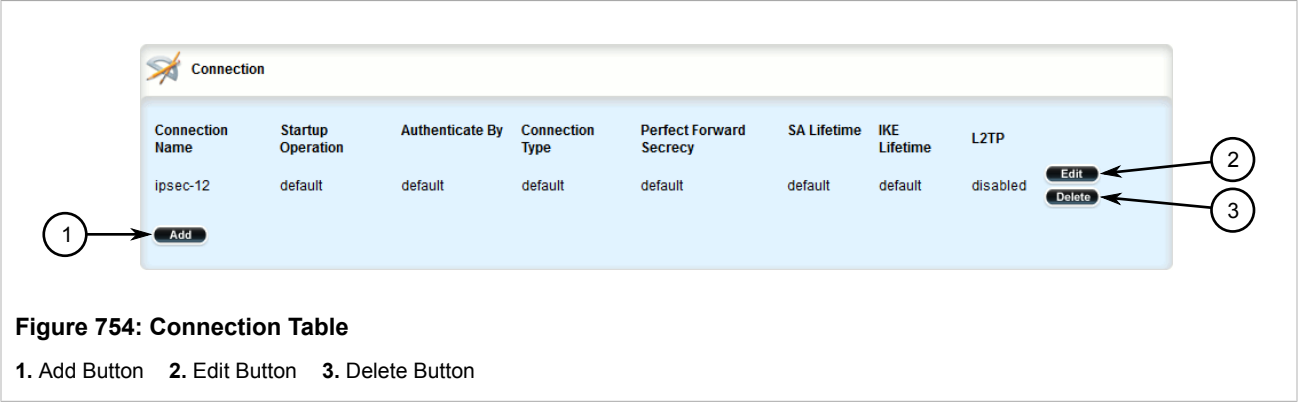


Figure 754: Connection Table

1. Add Button    2. Edit Button    3. Delete Button

- 3. Click **Delete** next to the chosen connection.
- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

Section 5.28.7

# 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.

The following sections describe how to configure and manage the Internet Key Exchange (IKE) protocol:

- [Section 5.28.7.1, “Viewing a List of IKE Algorithms”](#)
- [Section 5.28.7.2, “Adding an IKE Algorithm”](#)
- [Section 5.28.7.3, “Deleting an IKE Algorithm”](#)

Section 5.28.7.1

## Viewing a List of IKE Algorithms

To view a list of algorithms for the Internet Key Exchange (IKE) protocol, navigate to **tunnel » ipsec » connection » {connection} » ike » algorithm**, where {connection} is the name of the connection. If algorithms have been configured, the **Algorithm** table appears.

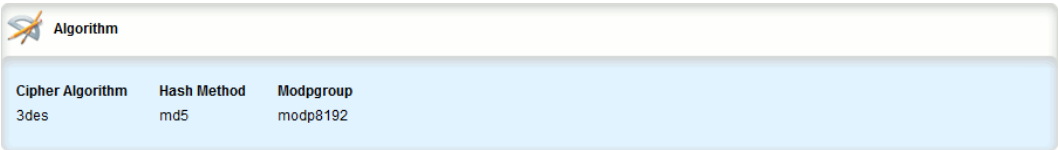


Figure 755: Algorithm Table

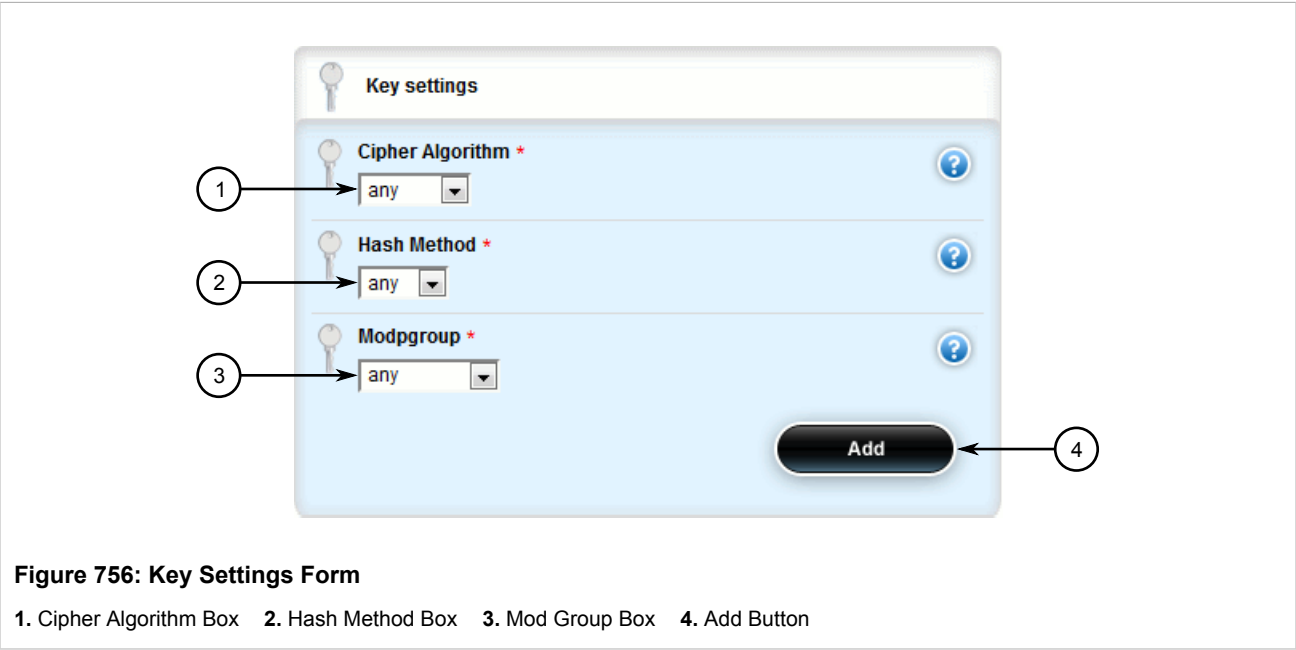
If no algorithms have been configured, add algorithms as needed. For more information, refer to [Section 5.28.7.2, “Adding an IKE Algorithm”](#).

Section 5.28.7.2

### Adding an IKE Algorithm

To add a new algorithm for the Internet Key Exchange (IKE) protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {connection} » ike**, where {connection} is the name of the connection.
3. Click **<Add algorithm>**. The **Key Settings** form appears.



**Figure 756: Key Settings Form**

1. Cipher Algorithm Box   2. Hash Method Box   3. Mod Group Box   4. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Cipher Algorithm	<b>Synopsis:</b> { 3des, aes, aes256, aes192, aes128, any } The cipher algorithm. The default value is '3des' or 'aes' unless overwritten by the default connection setting.
Hash Method	<b>Synopsis:</b> { sha1, md5, any } The hash method. The default value is 'sha1' or 'md5' unless overwritten by the default connection setting.
Modpgroup	<b>Synopsis:</b> { modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, any } The Modular Exponential (MODP) group. The default value is 'modp1024' or 'modp1536' unless overwritten by the default connection setting.

5. Click **Add** to create the new algorithm.

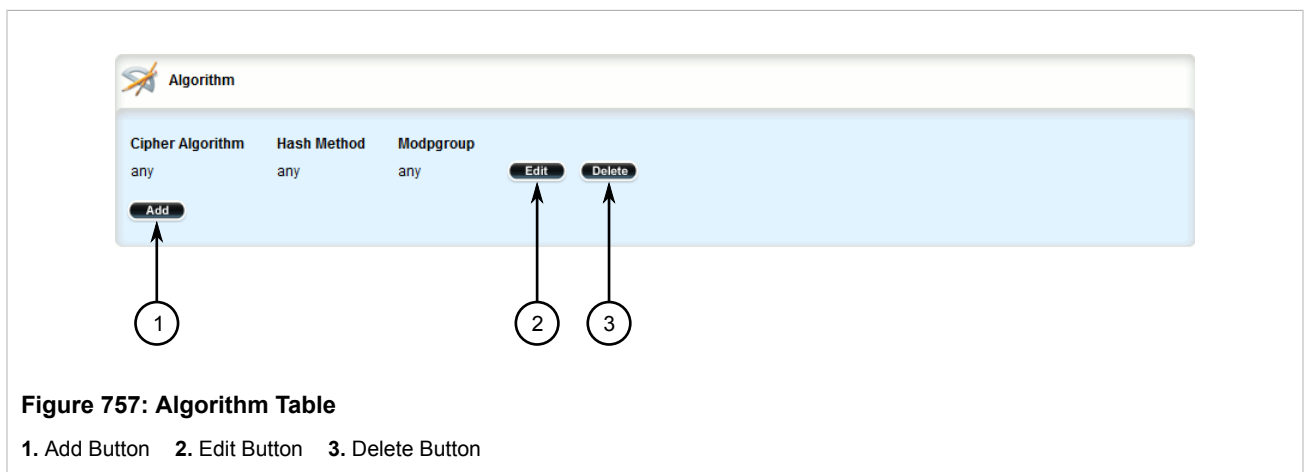
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.28.7.3

## Deleting an IKE Algorithm

To delete an algorithm for the Internet Key Exchange (IKE) protocol, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **tunnel » ipsec » connection » {connection} » ike**, where {connection} is the name of the connection. The **Algorithm** table appears.



- Click **Delete** next to the chosen algorithm.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.28.8

## 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.

The following sections describe how to configure and manage the ESP protocol:

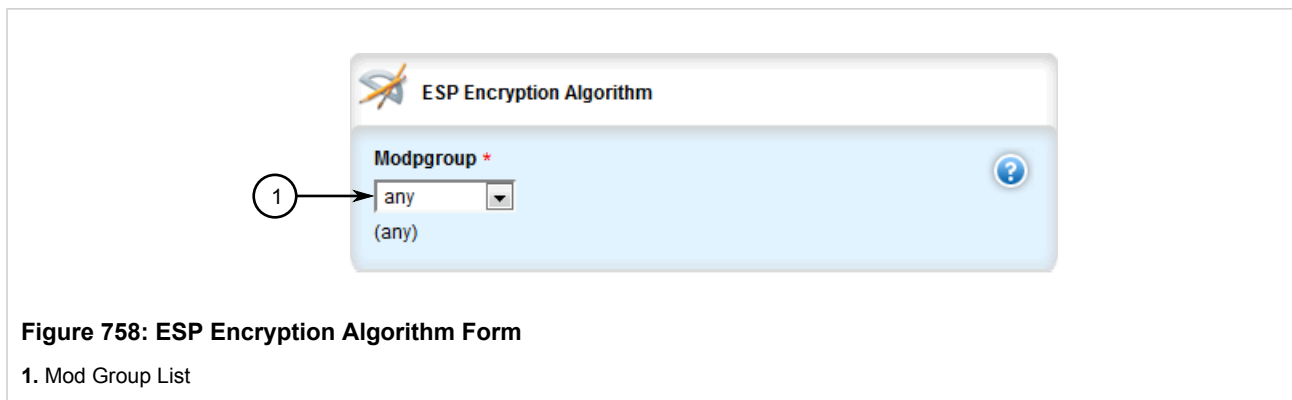
- [Section 5.28.8.1, “Configuring ESP Encryption”](#)
- [Section 5.28.8.2, “Viewing a List of ESP Algorithms”](#)
- [Section 5.28.8.3, “Adding ESP Algorithms”](#)
- [Section 5.28.8.4, “Deleting ESP Algorithms”](#)

### Section 5.28.8.1

## Configuring ESP Encryption

To configure the encryption algorithm for the Encapsulate Security Payload (ESP), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {connection} » esp**, where {connection} is the name of the connection. The **ESP Encryption Algorithm** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Modpgroup	<p><b>Synopsis:</b> { modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, any }</p> <p><b>Default:</b> any</p> <p>The Modular Exponential (MODP) group. The default value is 'modp1024' or 'modp1536' unless overwritten by the default connection setting.</p>

4. If required, add additional cipher algorithms. For more information on how to add algorithms, refer to [Section 5.28.8.3, “Adding ESP Algorithms”](#)
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.28.8.2

## Viewing a List of ESP Algorithms

To view a list of algorithms for the Encapsulate Security Payload (ESP) protocol, navigate to **tunnel » ipsec » connection » {connection} » esp » algorithm**, where {connection} is the name of the connection. If algorithms have been configured, the **Algorithm** table appears.

Algorithm	
Cipher Algorithm	Hash Method
aes256	sha1

**Figure 759: Algorithm Table**

If no algorithms have been configured, add algorithms as needed. For more information, refer to [Section 5.28.8.3, “Adding ESP Algorithms”](#).

### Section 5.28.8.3

## Adding ESP Algorithms

To add a new algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {connection} » esp » algorithm**, where {connection} is the name of the connection.
3. Click **<Add algorithm>**. The **Key Settings** form appears.

**Figure 760: Key Settings Form**

1. Cipher Algorithm Box    2. Hash Method Box    3. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Cipher Algorithm	<b>Synopsis:</b> { 3des, aes, aes256, aes192, aes128, any } The cipher algorithm. The default value is '3des' or 'aes' unless overwritten by the default connection setting.
Hash Method	<b>Synopsis:</b> { sha1, md5, any } The hash method. The default value is 'sha1' or 'md5' unless overwritten by the default connection setting.

5. Click **Add** to create the new algorithm.

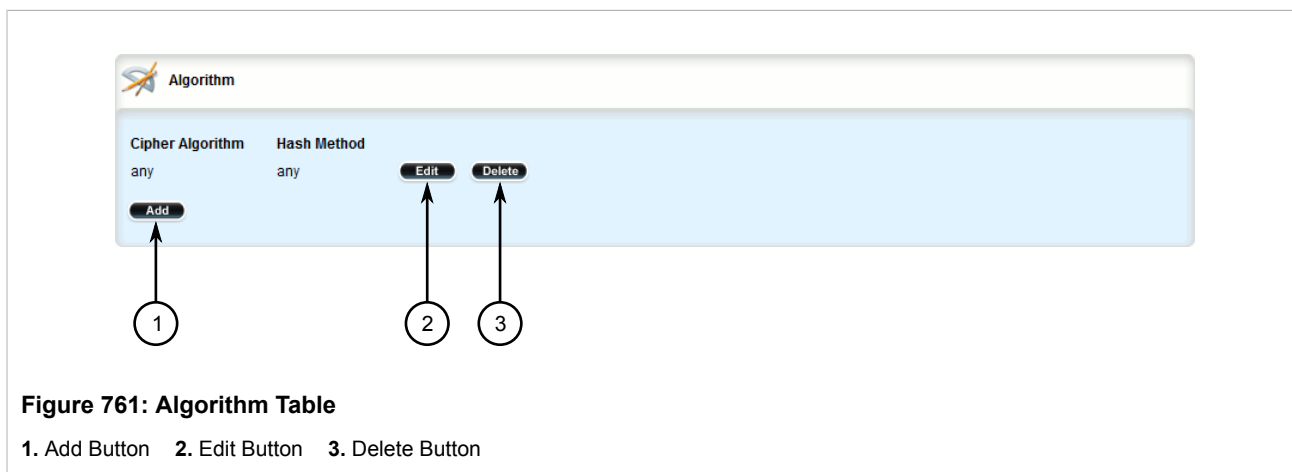
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

#### Section 5.28.8.4

### Deleting ESP Algorithms

To delete an algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {connection} » esp » algorithm**, where {connection} is the name of the connection. The **Algorithm** table appears.



3. Click **Delete** next to the chosen algorithm.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.28.9

### 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.



#### NOTE

*The configuration forms for the left and right connection ends are the same.*

To configure a connection end for an IPsec tunnel, do the following:

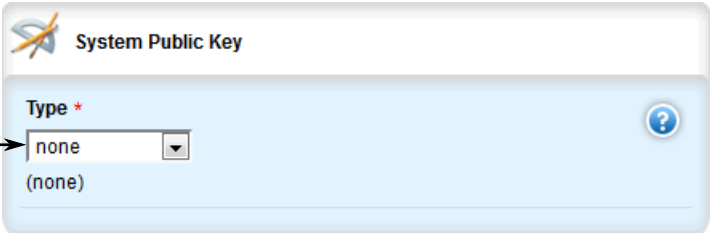
1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {name} » {end}**, where {name} is the name of the connection and {end} is either the left (local router) or right (remote router) connection end. The **Public IP Address**, **System Public Key**, **System Identifier**, **Next hop to Other System** and **Left/Right** forms appear.





The figure shows a web form titled "Public IP Address" with a blue header bar containing a logo and the title. Below the header, there are two main sections. The first section is labeled "Type \*" and contains a dropdown menu with "none" selected and "(none)" below it. A circled number "1" with an arrow points to the dropdown. The second section is labeled "Hostname or IP Address" and contains a text input field with a notepad icon and a dashed line. A circled number "2" with an arrow points to the input field. Both sections have a blue question mark icon in the top right corner.

**Figure 762: Public IP Address Form**  
1. Type List    2. Host Name or IP Address Box



The figure shows a web form titled "System Public Key" with a blue header bar containing a logo and the title. Below the header, there is a section labeled "Type \*" with a dropdown menu showing "none" and "(none)" below it. A circled number "1" with an arrow points to the dropdown. There is a blue question mark icon in the top right corner.

**Figure 763: System Public Key Form**  
1. Type List    2. Certificate List (Hidden)    3. RSA Signature List (Hidden)



The figure shows a web form titled "System Identifier" with a blue header bar containing a logo and the title. Below the header, there are two main sections. The first section is labeled "Type \*" and contains a dropdown menu with "default" selected and "(default)" below it. A circled number "1" with an arrow points to the dropdown. The second section is labeled "Hostname or IP Address" and contains a text input field with a notepad icon and a dashed line. A circled number "2" with an arrow points to the input field. Both sections have a blue question mark icon in the top right corner.

**Figure 764: System Identifier Form**  
1. Type List    2. Host Name or IP Address Box

**Figure 765: Nexthop to Other System Form**

1. Type List 2. IP Address Box

**Figure 766: Left/Right Form**

1. NAT Traversal Negotiation Method List

3. In the **Public IP Address** form, configure the following parameters:

Parameter	Description
Type	<b>Synopsis:</b> { none, default-route, any, address, hostname } <b>Default:</b> none The public IP address type.
Hostname or IP Address	<b>Synopsis:</b> A string 1 to 4095 characters long The public hostname or IP address.

4. In the **System Public Key** form, configure the following parameters:



**NOTE**

*Additional fields are displayed automatically based on the value specified under **Type**.*

Parameter	Description
Type	<b>Synopsis:</b> { none, rsasig, certificate-any, certificate } <b>Default:</b> none Key type.
RSA Signature	The RSA signature key name.
RSA Signature in ipsec format	<b>Synopsis:</b> A string 1 to 8192 characters long

Parameter	Description
	The RSA signature in IPsec format.
Certificate	The selected certificate.

5. In the **System Identifier** form, configure the following parameters:

Parameter	Description
type	<b>Synopsis:</b> { default, none, from-certificate, address, hostname, der-asn1-dn, user-fqdn } <b>Default:</b> default The system identifier type. The default value is 'left side public-ip' unless overwritten by the default connection setting.
Hostname, IP Address or Distinguished Name in Certificate	<b>Synopsis:</b> A string 1 to 1024 characters long The hostname, IP address or the Distinguished Name in the certificate.

6. In the *Nexthop to Other System* form, configure the following parameters:

Parameter	Description
Type	<b>Synopsis:</b> { default, default-route, address } <b>Default:</b> default The next hop type. The default value is 'right side public-ip' unless overwritten by the default connection setting.
IP Address	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the next hop that can be used to reach the destination network.

7. In the *Left/Right* form, configure the following parameters:

Parameter	Description
NAT Traversal Negotiation Method	<b>Synopsis:</b> { default, draft-ietf-ipsec-nat-t-ike-02, rfc-3947 } <b>Default:</b> default The NAT traversal negotiation method. Some IPsec endpoints prefer RFC 3947 over draft-ietf-ipsec-nat-t-ike-02 when connecting with Openswan, as these implementations use different identifiers when NAT is involved. For example, when a Windows XP/2003 client connects, Openswan reports the main mode peer ID is ID_FQDN: '@example.com', but when a Vista, Windows 7 or other RFC 3947 compliant client connects, Openswan 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 5.28.10.3, "Adding an Address for a Private Subnet"](#).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
10. Click **Exit Transaction** or continue making changes.

## Section 5.28.10

## 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.

The following sections describe how to configure and manage addresses for private subnets:

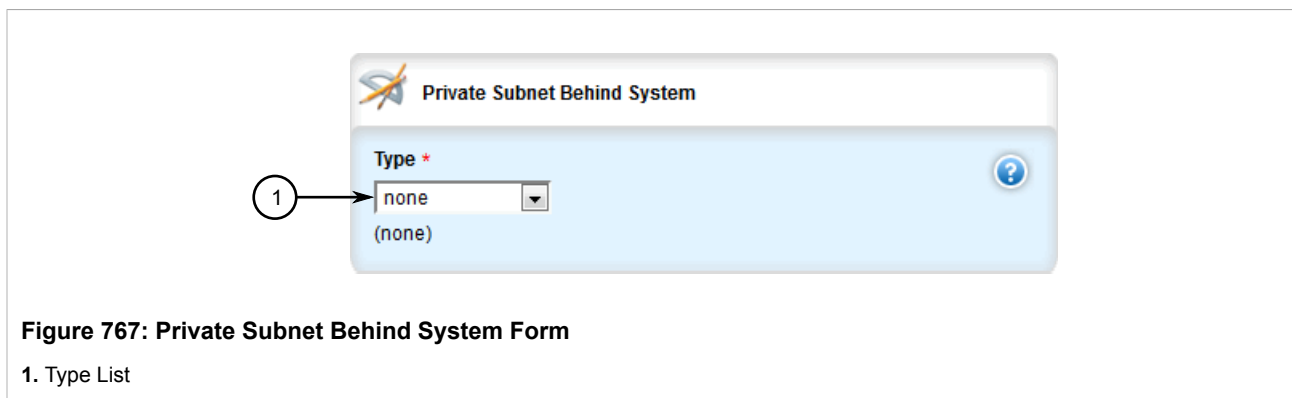
- [Section 5.28.10.1, “Configuring Private Subnets for Connection Ends”](#)
- [Section 5.28.10.2, “Viewing a List of Addresses for Private Subnets”](#)
- [Section 5.28.10.3, “Adding an Address for a Private Subnet”](#)
- [Section 5.28.10.4, “Deleting an Address for a Private Subnet”](#)

## Section 5.28.10.1

### 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection/{end} » subnet**, where *{end}* is the either the left (local router) or right (remote router) connection end. The **Private Subnet Behind System** form appears.



3. Configure the following parameter(s):

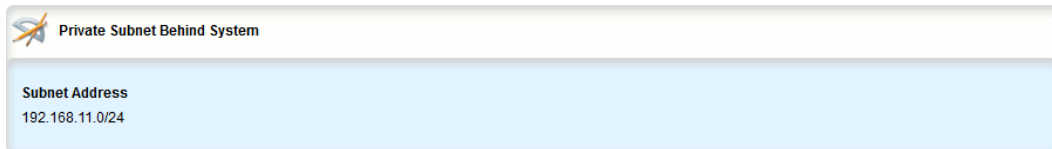
Parameter	Description
Subnet Address	<b>Synopsis:</b> A string 9 to 18 characters long The IP address/prefix.

4. Add one or more subnet addresses. For more information, refer to [Section 5.28.10.3, “Adding an Address for a Private Subnet”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

### Section 5.28.10.2

## Viewing a List of Addresses for Private Subnets

To view a list of addresses configured for private subnets, navigate to **tunnel » ipsec » connection » {connection} » {end} » subnet**, where *{connection}* is the name of the connection and *{end}* is either the left (local router) or right (remote router) connection end. If addresses have been configured, the **Private Subnet Behind System** table appears.



Private Subnet Behind System	
Subnet Address	192.168.11.0/24

**Figure 768: Private Subnet Behind System Table**

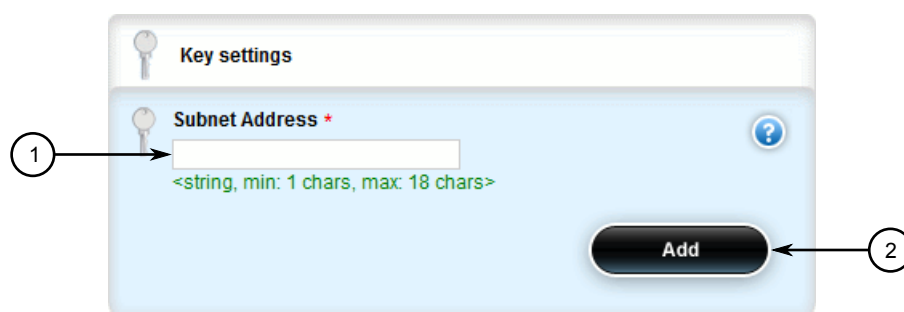
If no addresses have been configured, add addresses as needed. For more information, refer to [Section 5.28.10.3, “Adding an Address for a Private Subnet”](#).

### Section 5.28.10.3

## Adding an Address for a Private Subnet

To add a new address for a private subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » ipsec » connection » {connection} » {end} » subnet » network**, where *{connection}* is the name of the connection and *{end}* is either the left (local router) or right (remote router) connection end.
3. Click **<Add network>**. The **Key Settings** form appears.



Key settings

Subnet Address \*

<string, min: 1 chars, max: 18 chars>

Add

**Figure 769: Key Settings Form**

1. Subnet Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address	<b>Synopsis:</b> A string 9 to 18 characters long

Parameter	Description
	The IP address/prefix.

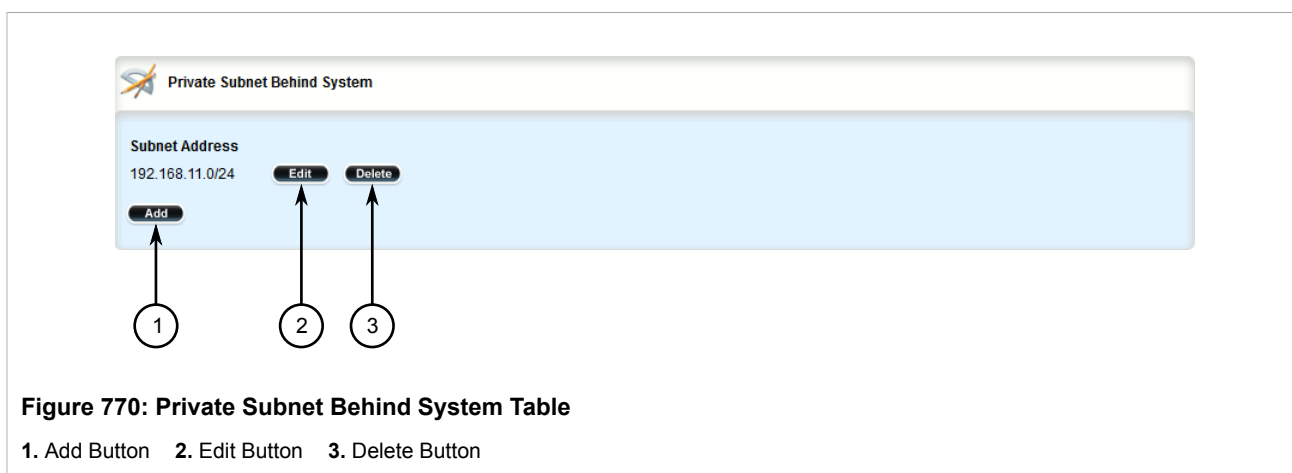
- Click **Add** to create the new address.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.28.10.4

## Deleting an Address for a Private Subnet

To delete an address for a private subnet, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **tunnel » ipsec » connection » {connection} » {end} » subnet**, where {connection} is the name of the connection and {end} is the either the left (local router) or right (remote router) connection end. The **Private Subnet Behind System** table appears.



- Click **Delete** next to the chosen address.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.29

## 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 5.39.2, “Viewing Statistics for Routable Interfaces”](#).

The following sections describe how to configure and manage 6in4 and 4in6 tunnels:

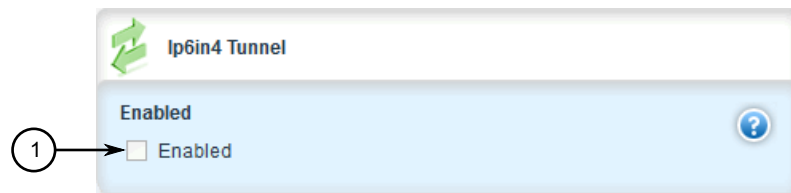
- [Section 5.29.1, “Enabling/Disabling 6in4 or 4in6 Tunnels”](#)
- [Section 5.29.2, “Viewing a List of 6in4 or 4in6 Tunnels”](#)
- [Section 5.29.3, “Viewing the Status of 6in4/4in6 Tunnels”](#)
- [Section 5.29.4, “Adding a 6in4 or 4in6 Tunnel”](#)
- [Section 5.29.5, “Deleting a 6in4 or 4in6 Tunnel”](#)

#### Section 5.29.1

## Enabling/Disabling 6in4 or 4in6 Tunnels

To enable or disable all 6in4 or 4in6 tunnels, do the following:

1. Change the mode to **Edit Public** or **Edit Exclusive**.
2. Navigate to **tunnel » ip6in4 | ip4in6**. The **IP6in4 Tunnel** or **IP4in6 Tunnel** form appears.



**Figure 771: IP6in4 Tunnel Form (Example)**

1. Enabled Check Box

3. Select or clear **Enabled**.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.29.2

## Viewing a List of 6in4 or 4in6 Tunnels

To view a list of 6in4 or 4in6 tunnels configured on the device, navigate to **tunnel » ip6in4 | ip4in6 » tunnel**. The **IP6in4 Tunnels** or **IP4in6 Tunnels** table appears.



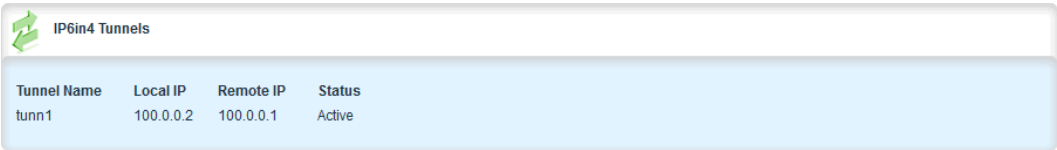
Name	Enabled	Local-ip	Remote-ip	Mtu
ruggedcom	true	192.168.30.14	172.23.30.14	1480

Figure 772: IP6in4 Tunnels Table (Example)

Section 5.29.3

## Viewing the Status of 6in4/4in6 Tunnels

To view the status of all 6in4 or 4in6 tunnels, navigate to *interfaces* » *ip6in4* | *ip4in6*. The **IP6in4 Tunnels** or **IP4in6 Tunnels** table appears.



Tunnel Name	Local IP	Remote IP	Status
tunn1	100.0.0.2	100.0.0.1	Active

Figure 773: IP6in4 Tunnels Table (Example)

Section 5.29.4

## Adding a 6in4 or 4in6 Tunnel

To add a 6in4 or 4in6 tunnel, do the following:

1. Change the mode to **Edit Public** or **Edit Exclusive**.
2. Navigate to *tunnel* » *ip6in4* | *ip4in6* » *tunnel* and click **<Add tunnel>**. The **Key Settings** form appears.



The screenshot shows the 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a form area with a key icon and the label 'Name \*'. There is a text input field for the name, with a hint '<string, min: 1 chars, max: 11 chars>' below it. To the right of the input field is a blue question mark icon. At the bottom right of the form is a black 'Add' button. Two numbered circles with arrows point to the input field (labeled '1') and the 'Add' button (labeled '2').

Figure 774: Key Settings Form

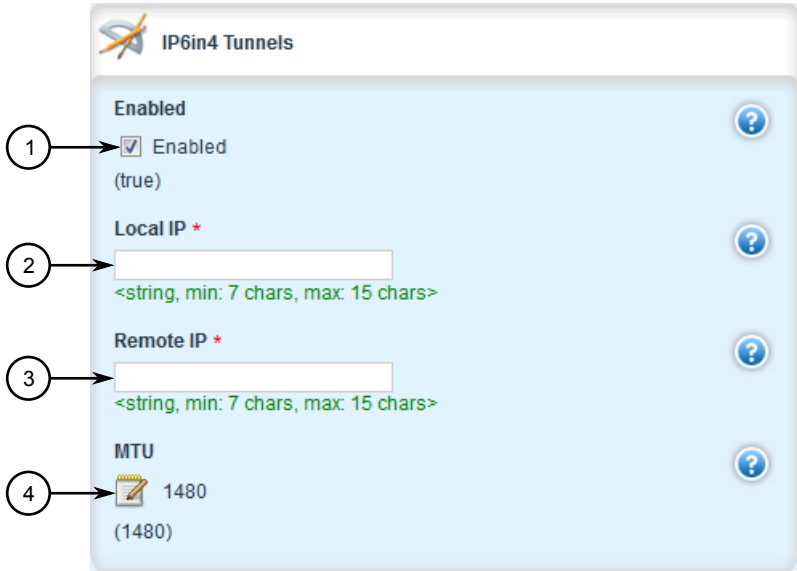
1. Name Box    2. Add Button

3. In the **Key Settings** form, configure the following parameters as required:



Parameter	Description
Tunnel Name	<b>Synopsis:</b> A string Tunnel name

4. Click **Add** to create the new tunnel. The **IP6in4 Tunnels** or **IP4in6 Tunnels** form appears.



**Figure 775: IP6in4 Tunnels Form (Example)**

1. Enabled Check Box    2. Local IP Box    3. Remote IP Box    4. MTU Box

5. In the **IP6in4 Tunnels** or **IP4in6 Tunnels** form, configure the following parameters as required:

Parameter	Description
Local IP	<b>Synopsis:</b> A string 7 to 15 characters long The interface upon which the tunnel is created
Remote IP	<b>Synopsis:</b> A string 7 to 15 characters long Ip address of remote tunnel end
Status	<b>Synopsis:</b> A string Current status of tunnel

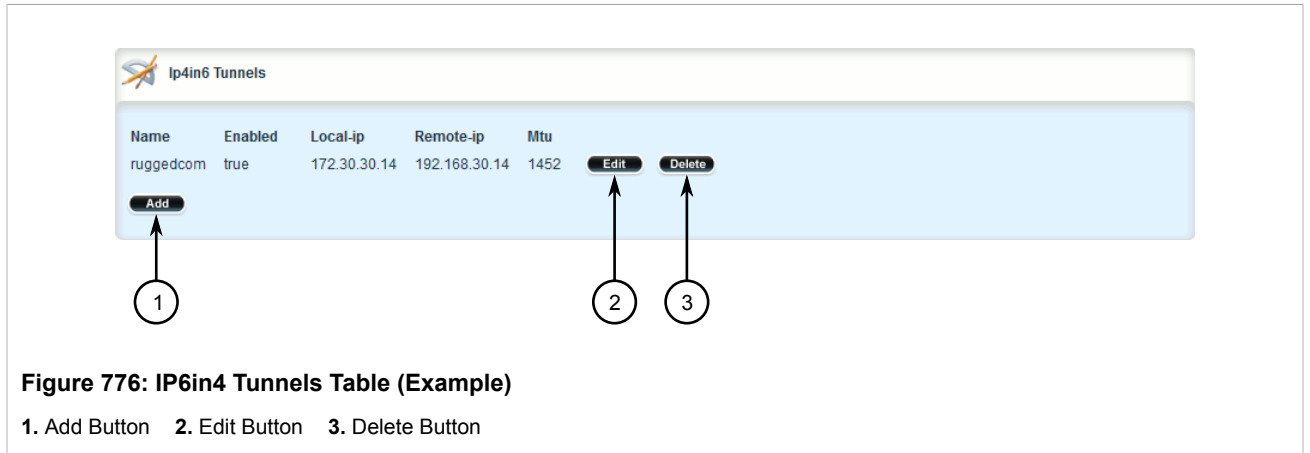
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

Section 5.29.5

## Deleting a 6in4 or 4in6 Tunnel

To delete a 6in4 or 4in6 tunnel, do the following:

1. Change the mode to **Edit Public** or **Edit Exclusive**.
2. Navigate to **tunnel » ip6in4 | ip4in6 » tunnel**. The **IP6in4 Tunnels** or **IP4in6 Tunnels** table appears.



3. Click **Delete** next to the chosen tunnel.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.30

## Managing Layer 2 Tunnels

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 tunnelling them over routed IP networks. The Layer 2 Tunnel Daemon supports the IEC61850 GOOSE protocol as well as a generic mechanism for tunnelling by Ethernet type.

The following sections describe how to configure and manage Layer 2 tunnels:

- [Section 5.30.1, “Viewing the Round Trip Time Statistics”](#)
- [Section 5.30.2, “Configuring L2TP Tunnels”](#)
- [Section 5.30.3, “Configuring L2TPv3 Tunnels”](#)
- [Section 5.30.4, “Configuring the Layer 2 Tunnel Daemon”](#)
- [Section 5.30.5, “Managing GOOSE Tunnels”](#)
- [Section 5.30.6, “Managing Remote Daemons for GOOSE Tunnels”](#)
- [Section 5.30.7, “Managing Generic Tunnels”](#)
- [Section 5.30.8, “Managing Remote Daemon IP Addresses for Generic Tunnels”](#)
- [Section 5.30.9, “Managing Remote Daemon Egress Interfaces for Generic Tunnels”](#)
- [Section 5.30.10, “Managing Ethernet Types for Generic Tunnels”](#)

Section 5.30.1

Viewing the Round Trip Time Statistics

The round trip time statistics reflect the measured round trip time to each remote daemon. The minimum, average, maximum and standard deviation of times is presented. Entries with a large difference between the **Transmitted** and **Received** parameters indicate potential problems.

To view the round trip time statistics, navigate to *tunnel » I2tunneld » status » round-trip-time*. The **Round Trip Time Statistics** form appears.



**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 5.30.8, “Managing Remote Daemon IP Addresses for Generic Tunnels”](#).*

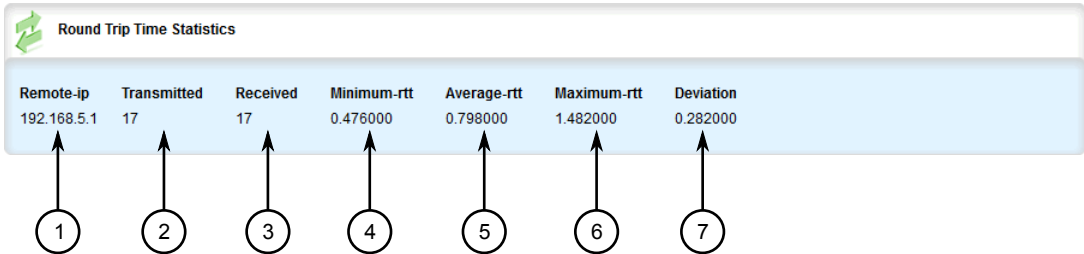


Figure 777: Round Trip Time Statistics Form

1. Remote IP   2. Transmitted   3. Received   4. Minimum RTT   5. Average RTT   6. Maximum RTT   7. Deviation

This table provides the following information:

Parameter	Description
remote-ip	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of remote daemon.
transmitted	The number of beacon frames transmitted through the tunnel.
received	The number of beacon frames received through the tunnel.
minimum-rtt	<b>Synopsis:</b> A string 1 to 32 characters long The Minimum Beacon Round-Trip-Time.
average-rtt	<b>Synopsis:</b> A string 1 to 32 characters long The Average Beacon Round-Trip-Time.
maximum-rtt	<b>Synopsis:</b> A string 1 to 32 characters long The Maximum Beacon Round-Trip-Time.
deviation	<b>Synopsis:</b> A string 1 to 32 characters long The standard deviation.

Section 5.30.2

## Configuring L2TP Tunnels

The Layer Two Tunneling Protocol (L2TP) is used primarily to tunnel Point-to-Point Protocol (PPP) packets through an IP network, although it is also capable of tunneling other layer 2 protocols.

RUGGEDCOM ROX II utilizes L2TPD in conjunction with Openswan 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.*

To configure L2TP tunnels, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tp**. The **DNS Server**, **WINS Server**, **PPP Options** and **L2TP** forms appear.

**Figure 778: DNS Server Form**

1. Primary Box    2. Secondary Box

**Figure 779: WINS Server Form**

1. Primary Box    2. Secondary Box

PPP Options

1 → **Authorize Locally** ☐ Enabled ?

2 → **MTU \*** 1410 (1410) ?

3 → **MRU \*** 1410 (1410) ?

**Figure 780: PPP Options Form**  
1. Authorize Locally Check Box   2. MTU Box   3. MRU Box

L2TP

1 → **Enable L2TP** ☐ Enabled ?

2 → **Local IP Address** --- ?

3 → **First IP Address** --- ?

4 → **Maximum Number of Connections** --- ?

5 → **Closing-wait-timeout \*** 60 (60) ?

**Figure 781: L2TP Form**  
1. Enable L2TP Check Box   2. Local IP Address Box   3. First IP Address Box   4. Maximum Number of Connections Box  
5. Closing Wait Timeout Box

3. On the **DNS Server** form, configure the following parameter(s) as required:

Parameter	Description
Primary	<b>Synopsis:</b> A string 7 to 15 characters long The primary DNS server.

Parameter	Description
Secondary	<b>Synopsis:</b> A string 7 to 15 characters long The secondary DNS server.

4. On the **WINS Server** form, configure the following parameter(s) as required:

Parameter	Description
Primary	<b>Synopsis:</b> A string 7 to 15 characters long The primary WINS server.
Secondary	<b>Synopsis:</b> A string 7 to 15 characters long The secondary WINS server.

5. On the **PPP Options** form, 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 4.8.2, “Configuring RADIUS Authentication for PPP Services”](#).*

Parameter	Description
Authorize Locally	<b>Synopsis:</b> typeless Authorizes locally instead of using radius server.
MTU	<b>Synopsis:</b> An integer between 68 and 1500 <b>Default:</b> 1410 The Maximum Transmit Unit (MTU) or maximum packet size transmitted.
MRU	<b>Synopsis:</b> An integer between 68 and 1500 <b>Default:</b> 1410 The Maximum Receive Unit (MRU) or maximum packet size passed when received.

6. On the **L2TP** form, configure the following parameter(s) as required:

Parameter	Description
Enable L2TP	<b>Synopsis:</b> typeless Enables L2TP.
Local IP Address	<b>Synopsis:</b> 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 Address	<b>Synopsis:</b> 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.
Maximum Number of Connections	<b>Synopsis:</b> An integer between 1 and 10 The maximum number of connections.
closing-wait-timeout	<b>Synopsis:</b> An integer between 5 and 120 <b>Default:</b> 60

Parameter	Description
	The number of seconds to wait before the tunnel is cleaned up after the tunnel moves to closing-wait state.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.30.3

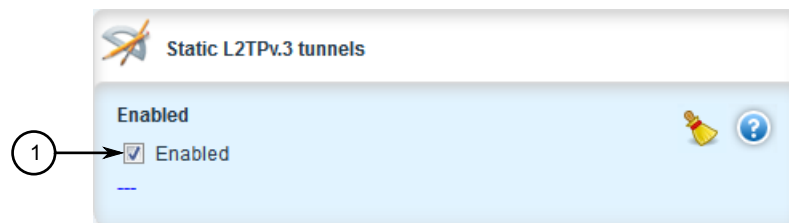
## Configuring L2TPv3 Tunnels

L2TPv3 improves the performance of bridging Ethernet frames over a WAN interface. Ethernet frames are bridged over an IP network at high data packet rates and low CPU consumption. IEC61850 GOOSE messages exchange and LAN extension are some applications of this feature.

RUGGEDCOM ROX II supports Static L2TPv3 tunnel over UDP starting with version 2.5. Static tunnel is an unmanaged tunnel type. All tunnel information, such as tunnel id, session id, cookies etc., must be agreed in advance between two endpoints to establish a tunnel. There are no control messages exchanged with this type of tunnel.

To configure L2TPv3 tunnels, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **tunnel » l2tpv3 » static**. The **Static L2TPv3 Tunnels Enable** form appears.



**Figure 782: Static L2TPv3 Tunnel Enable Form**

1. Enable Check Box

- Check the **Enable** check box.
- Navigate to **tunnel » l2tpv3 » static » tunnel** and select **Add tunnel**. The **Key Settings** form appears.

The screenshot shows a web interface titled "Key settings". Below the title is a key icon and the label "Tunnel-name \*". To the right of the label is a blue question mark icon. Below the label is a text input field containing the number "1". Below the input field is a green string constraint message: "<string, min: 1 chars, max: 3 chars>". To the right of the input field is a black "Add" button. A circled number "1" with an arrow points to the input field, and a circled number "2" with an arrow points to the "Add" button.

**Figure 783: Key Settings Form**  
1. Tunnel-Name Box    2. Add Button

On the **Key Settings** form, configure the following parameter(s) as required:

Parameter	Description
Tunnel Name	<b>Synopsis:</b> A string 1 to 3 characters long Tunnel name, contains any lower case letter or numerical digit. Prefix 'l2t-' will be added to tunnel name and session name to create l2tpv3 system interface name (ie. l2tp-1-1)

5. Click **Add** to create the tunnel. The **Static L2TPv3 Tunnels** form appears.



The screenshot shows the 'Static L2TPv3 tunnels' configuration form. It contains the following fields and their values:

- Enabled:** A checked checkbox, with the value '(true)' displayed below it. Callout 1 points to the checkbox.
- Tunnel-id \*:** A text box containing the value '1'. Callout 2 points to the text box.
- Remote-tunnel-id \*:** A text box containing the value '1'. Callout 3 points to the text box.
- Transport-encap:** A dropdown menu showing 'ip' with '(udp)' below it. Callout 4 points to the dropdown.
- Local-ip \*:** A text box containing the value '192.168.3.146'. Callout 5 points to the text box.
- Local-port:** A text box containing the value '62001'. Callout 6 points to the text box.
- Remote-ip \*:** A text box containing the value '192.168.3.145'. Callout 7 points to the text box.
- Remote-port:** A text box containing the value '62001'. Callout 8 points to the text box.

Each field has a blue question mark icon to its right. The 'Local-port' and 'Remote-port' fields also have a yellow bell icon to their right.

Figure 784: Static L2TPv3 Tunnels Form

1. Enabled Check Box   2. Tunnel ID Box   3. Remote Tunnel ID Box   4. Transport Encapsulation List   5. Local IP Box   6. Local Port Box   7. Remote IP Box   8. Remote Port Box

6. On the **Static L2TPv3 Tunnels** form, configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables/Disables the tunnel
Tunnel ID	<b>Synopsis:</b> An integer between 1 and 65535 The local tunnel-id
Remote Tunnel ID	<b>Synopsis:</b> An integer between 1 and 65535 Tunnel-id of remote tunnel endpoint
Transport Encapsulation	<b>Synopsis:</b> { udp, ip } <b>Default:</b> udp The transport protocol (UDP or IP) to encapsulate the tunnel messages

Parameter	Description
Local IP	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long Ip address of local interface
Local Port	<b>Synopsis:</b> An integer between 1024 and 65535 Local listening transport port for tunnel service
Remote IP	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long Ip address of remote tunnel endpoint
Remote Port	<b>Synopsis:</b> An integer between 1024 and 65535 The listening transport port of remote device for tunnel service

7. Navigate to **tunnel » l2tpv3 » static » tunnel » {tunnel name} » session** and select **Add session**. The **Key Settings** form appears.

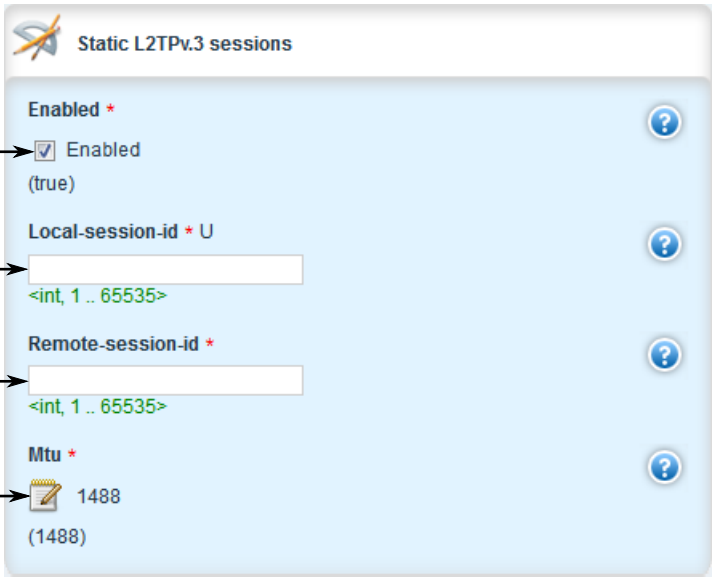
**Figure 785: Key Settings Form**

1. Session Name Box    2. Add Button

On the **Key Settings** form, configure the following parameter(s) as required:

Parameter	Description
Session Name	<b>Synopsis:</b> A string 1 to 2 characters long Session name, contains any lower case letter or numerical digit. Prefix 'l2t-' will be added to tunnel name and session name to create l2tpv3 system interface name (ie. l2tp-1-1)

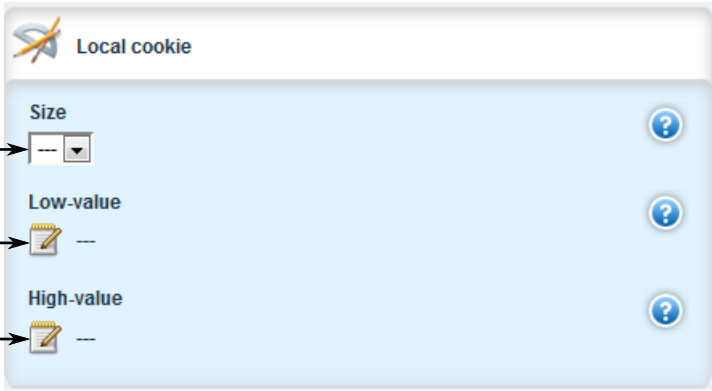
8. Click **Add** to create the session. The **Static L2TPv3 Sessions**, **Local Cookie**, and **Remote Cookie** forms appear.



The image shows a web interface form titled "Static L2TPv3 sessions". It contains four main configuration fields, each with a help icon (question mark in a blue circle) to its right. The fields are: 1. "Enabled \*" with a checked checkbox and the text "(true)". 2. "Local-session-id \* U" with a text input field containing "<int, 1 .. 65535>". 3. "Remote-session-id \*" with a text input field containing "<int, 1 .. 65535>". 4. "Mtu \*" with a text input field containing "1488" and "(1488)".

**Figure 786: Static L2TPv3 Sessions Form**

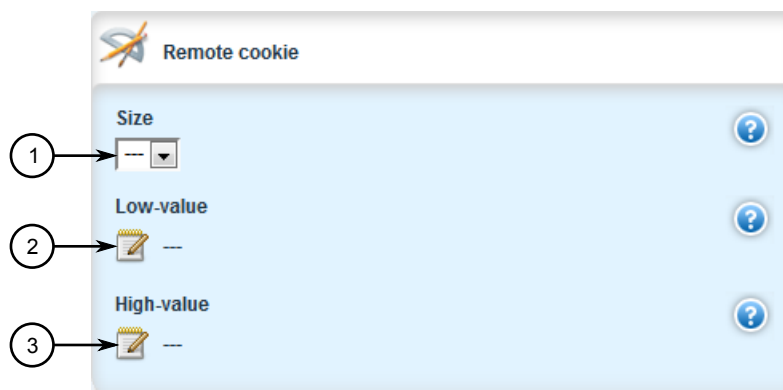
1. Enabled Check Box   2. Local Session ID Box   3. Remote Session ID Box   4. Mtu Box



The image shows a web interface form titled "Local cookie". It contains three main configuration fields, each with a help icon (question mark in a blue circle) to its right. The fields are: 1. "Size" with a dropdown menu showing "--". 2. "Low-value" with a text input field containing "--". 3. "High-value" with a text input field containing "--".

**Figure 787: Local Cookie Form**

1. Size Selection Box   2. Low Value Box   3. High Value Box



**Figure 788: Remote Cookie Form**

1. Size Selection Box   2. Low Value Box   3. High Value Box

9. On the **Static L2TPv3 Sessions** form, configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables/Disables the session
Local Session ID	<b>Synopsis:</b> An integer between 1 and 65535 The local session-id provides the necessary context for all further packet processing
Remote Session ID	<b>Synopsis:</b> An integer between 1 and 65535 The remote session-id is used to identify the received data messages from remote session endpoint
L2TP-Specific Sub Layer	<b>Synopsis:</b> { default, none } <b>Default:</b> default L2TP specific sublayer processing type
mtu	<b>Synopsis:</b> An integer between 68 and 1500 <b>Default:</b> 1488 MTU of network interface

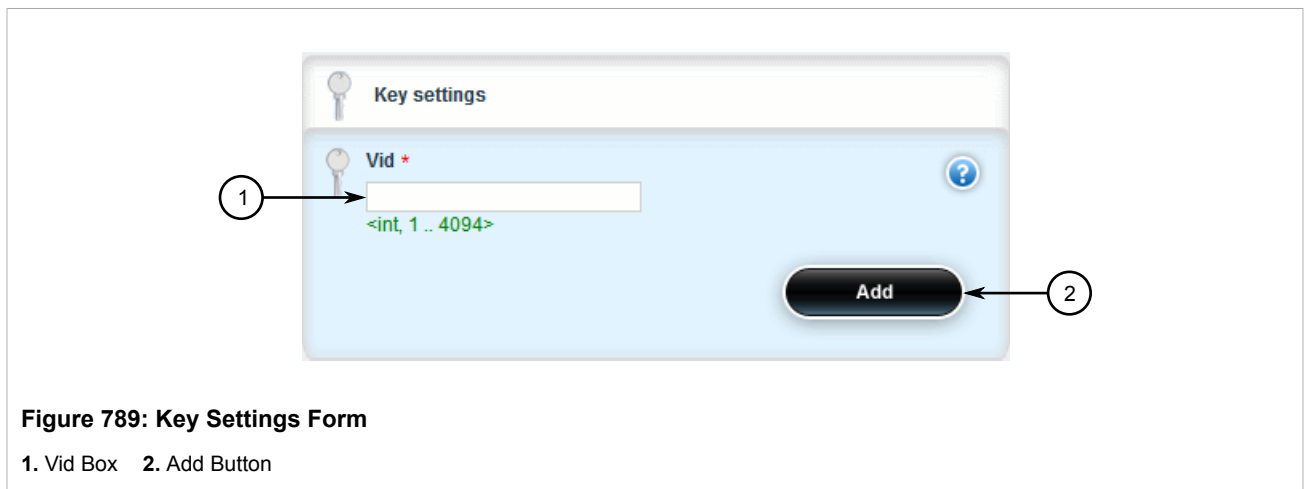
10. On the **Local Cookie** form, configure the following parameter(s) as required:

Parameter	Description
Size	<b>Synopsis:</b> { 4, 8 } Cookie size in byte.
Low Value	Lower value of cookie. This value must match with low-value of other endpoint's remote cookie
High Value	Higher value of cookie if the cookie size is 8. This value must match with high-value of other endpoint's remote cookie

11. On the **Remote Cookie** form, configure the following parameter(s) as required:

Parameter	Description
Size	<b>Synopsis:</b> { 4, 8 } Cookie size in byte
Low Value	Lower value of cookie. This value must match with low-value of other endpoint's local cookie
High Value	Higher value of cookie if its size is 8. This value must match with high-value of other endpoint's local cookie

12. Navigate to **tunnel » l2tpv3 » static » tunnel » {tunnel name} » session » {session name} » vlan** and select **Add vlan**. The **Key Settings** form appears.



On the **Key Settings** form, configure the following parameter(s) as required:

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

For more information about VLANs, refer to [Section 5.36, “Managing VLANs”](#).

13. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
14. Click **Exit Transaction** or continue making changes.

#### Section 5.30.4

## Configuring the Layer 2 Tunnel Daemon

To configure the Layer 2 tunnel daemon, do the following:

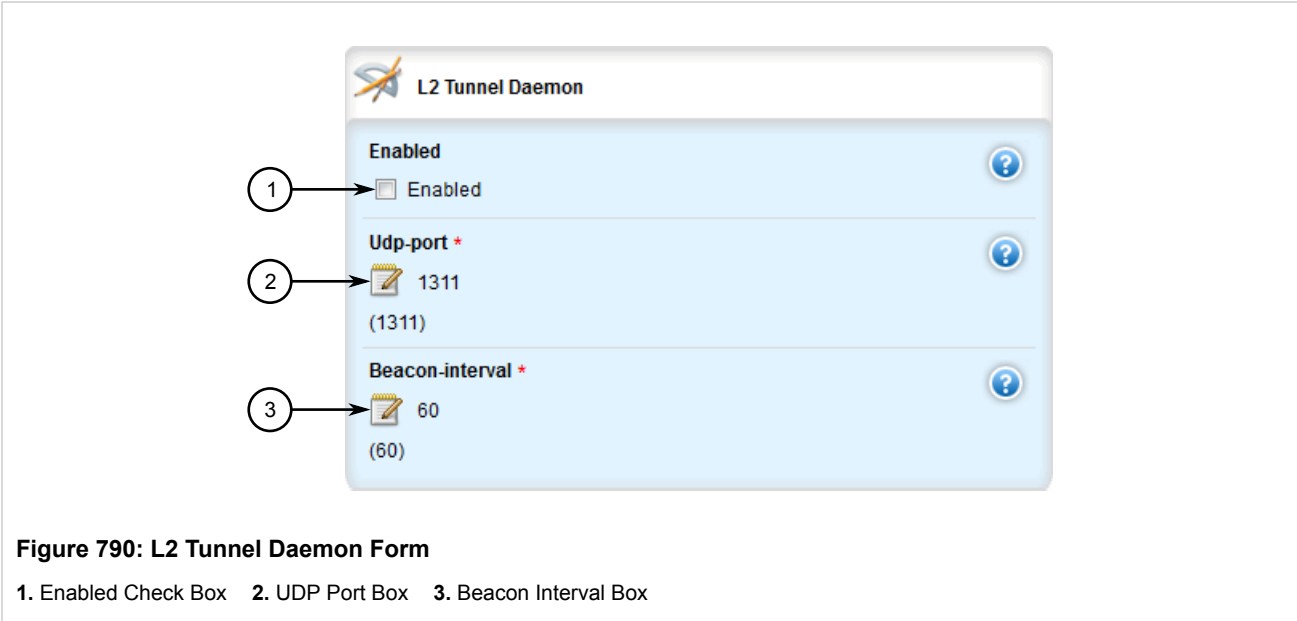


### IMPORTANT!

*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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld**. The **L2 Tunnel Daemon** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
enabled	<b>Synopsis:</b> typeless Enables the Layer 2 protocols server.
UDP Port	<b>Synopsis:</b> An integer between 1 and 65535 <b>Default:</b> 1311 The UDP port to communicate with the other daemon.
Beacon Interval	<b>Synopsis:</b> { off } or an integer between 10 and 3600 <b>Default:</b> 60 The Round Trip Time (RTT) of the sent message

4. Add GOOSE or generic tunnels as required. For more information, refer to [Section 5.30.5.3, “Adding a GOOSE Tunnel”](#) or [Section 5.30.7.3, “Adding a Generic Tunnel”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

Section 5.30.5

# 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

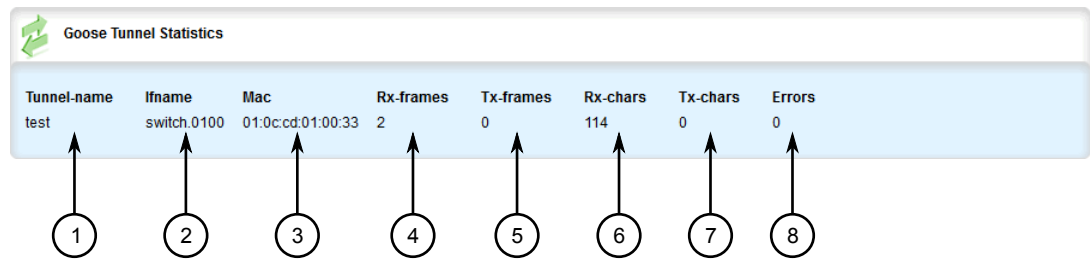
The following sections describe how to configure and manage GOOSE tunnels:

- [Section 5.30.5.1, “Viewing the GOOSE Tunnel Statistics”](#)
- [Section 5.30.5.2, “Viewing a List of GOOSE Tunnels”](#)
- [Section 5.30.5.3, “Adding a GOOSE Tunnel”](#)
- [Section 5.30.5.4, “Deleting a GOOSE Tunnel”](#)

#### Section 5.30.5.1

### Viewing the GOOSE Tunnel Statistics

To view the GOOSE tunnel statistics, navigate to **tunnel » l2tunneld » status » goose**. The **GOOSE Tunnel Statistics** form appears.



**Figure 791: GOOSE Tunnel Statistics Form**  
1. Tunnel Name   2. Interface Name   3. MAC   4. RX Frames   5. TX Frames   6. RX Characters   7. TX Characters   8. Errors

This table provides the following information:

Parameter	Description
tunnel-name	<b>Synopsis:</b> A string 1 to 32 characters long The GOOSE tunnel name.
ifname	<b>Synopsis:</b> A string 1 to 15 characters long The name of the VLAN interface.
mac	<b>Synopsis:</b> A string The Multicast Destination MAC Address of the Goose message.
rx-frames	The number of frames received through the tunnel.
tx-frames	The number of frames transmitted through the tunnel.
rx-chars	The number of bytes received through the tunnel.
tx-chars	The number of bytes transmitted through the tunnel.
errors	The number of errors through the tunnel.

Section 5.30.5.2  
**Viewing a List of GOOSE Tunnels**

To view a list of GOOSE tunnels, navigate to **tunnel » l2tunneld » goose**. If tunnels have been configured, the **GOOSE Tunnel** table appears.



**Figure 792: GOOSE Tunnel Table**

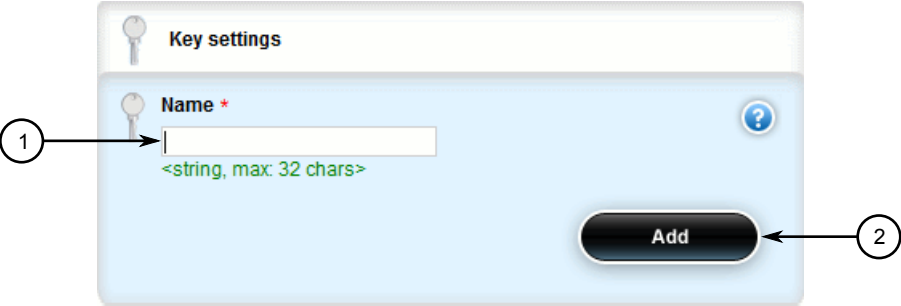
If no GOOSE tunnels have been configured, add tunnels as needed. For more information, refer to [Section 5.30.5.3, “Adding a GOOSE Tunnel”](#).



Section 5.30.5.3

Adding a GOOSE Tunnel

- To configure a GOOSE tunnel, do the following:
1. Change the mode to **Edit Private** or **Edit Exclusive**.
  2. Navigate to *tunnel » I2tunneld » goose* and click **<Add tunnel>**. The **Key Settings** form appears.



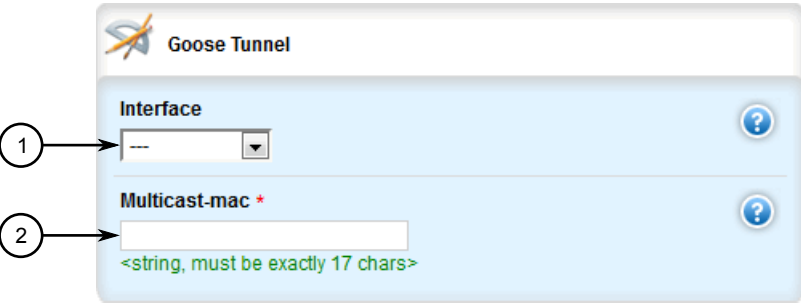
**Figure 793: Key Settings Form**

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 32 characters long Description of the GOOSE tunnel.

4. Click **Add** to create the tunnel. The **GOOSE Tunnel** form appears.



**Figure 794: GOOSE Tunnel Form**

1. Interface List    2. Multicast MAC Address Box

5. Configure the following parameter(s) as required:

Parameter	Description
Interface	The interface to listen on for GOOSE frames.
Multicast MAC	<b>Synopsis:</b> A string

Parameter	Description
	The multicast MAC address to listen for.

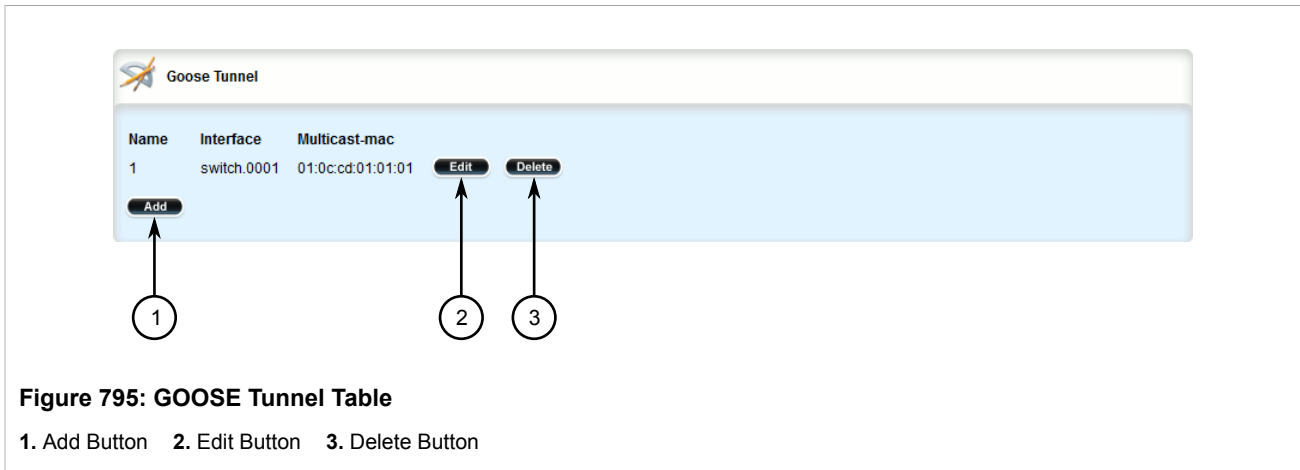
6. If necessary, configure one or more remote daemons for the tunnel. For more information, refer to [Section 5.30.6.2, “Adding a Remote Daemon”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 5.30.5.4

## Deleting a GOOSE Tunnel

To delete a GOOSE tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » goose**. The **GOOSE Tunnel** table appears.



3. Click **Delete** next to the chosen tunnel.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.30.6

## 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.

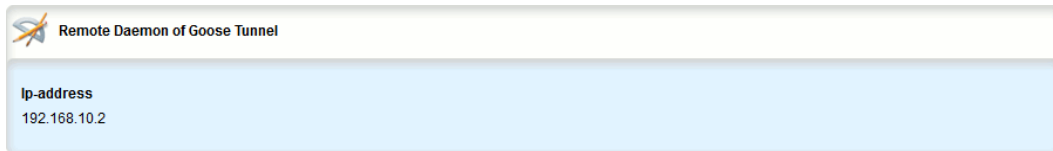
The following sections describe how to configure and manage remote daemons for GOOSE tunnels:

- [Section 5.30.6.1, “Viewing a List of Remote Daemons”](#)
- [Section 5.30.6.2, “Adding a Remote Daemon”](#)
- [Section 5.30.6.3, “Deleting a Remote Daemon”](#)

### Section 5.30.6.1

## Viewing a List of Remote Daemons

To view a list of remote daemons configured for a GOOSE tunnel, navigate to **tunnel » l2tunneld » goose » {name} » remote-daemon**, where {name} is the name of the GOOSE tunnel. If remote daemons have been configured, the **Remote Daemon of Goose Tunnel** table appears.



Remote Daemon of Goose Tunnel	
ip-address	192.168.10.2

**Figure 796: Remote Daemon of Goose Tunnel Table**

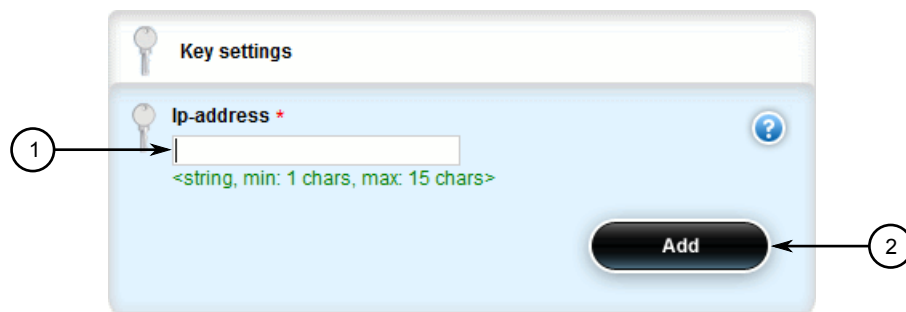
If no remote daemons have been configured, add daemons as needed. For more information, refer to [Section 5.30.6.2, “Adding a Remote Daemon”](#).

### Section 5.30.6.2

## Adding a Remote Daemon

To configure a remote daemon for a GOOSE tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » goose » {tunnel} » remote-daemon**, where {tunnel} is the name of the GOOSE tunnel.
3. Click **<Add remote-daemon>**. The **Key Settings** form appears.



**Figure 797: Key Settings Form**

1. IP Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the remote Layer 2 protocol server.

5. Click **Add** to create the daemon.

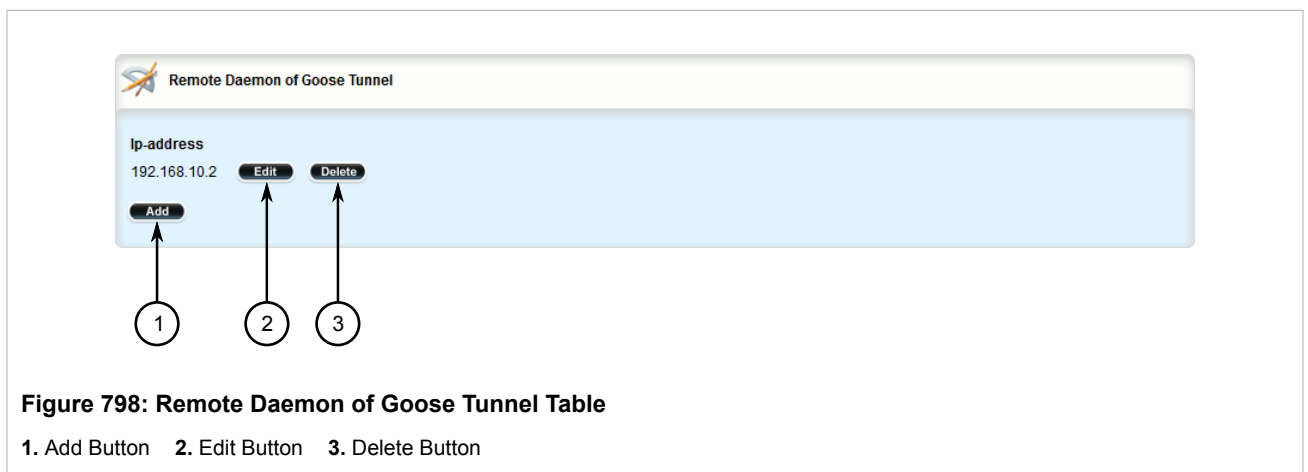
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.30.6.3

## Deleting a Remote Daemon

To delete a remote daemon, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » goose » {name} » remote-daemon**, where {name} is the name of the GOOSE tunnel. The **Remote Daemon of Goose Tunnel** table appears.



3. Click **Delete** next to the chosen daemon.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.30.7

## 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)

The following sections describe how to configure and manage generic tunnels:

- [Section 5.30.7.1, “Viewing the Generic Tunnel Statistics”](#)
- [Section 5.30.7.2, “Viewing a List of Generic Tunnels”](#)
- [Section 5.30.7.3, “Adding a Generic Tunnel”](#)

- [Section 5.30.7.4, “Deleting a Generic Tunnel”](#)

Section 5.30.7.1

Viewing the Generic Tunnel Statistics

To view the generic tunnel statistics, navigate to *tunnel » l2tunneld » status » generic*. The **Generic L2 Tunnel Statistics** form appears.

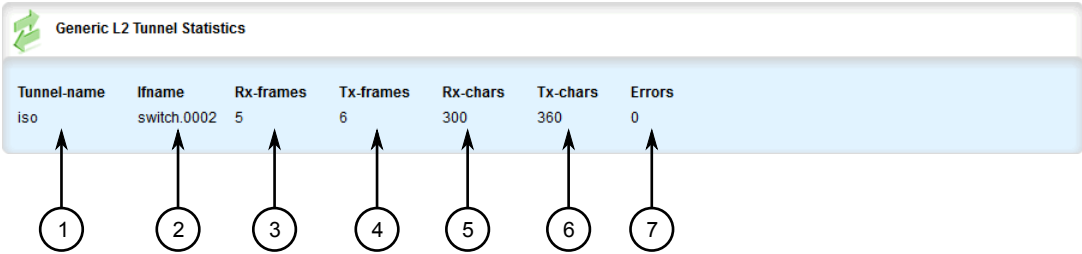


Figure 799: Generic L2 Tunnel Statistics Form

1. Tunnel Name    2. Interface Name    3. RX Frames    4. TX Frames    5. RX Characters    6. TX Characters    7. Errors

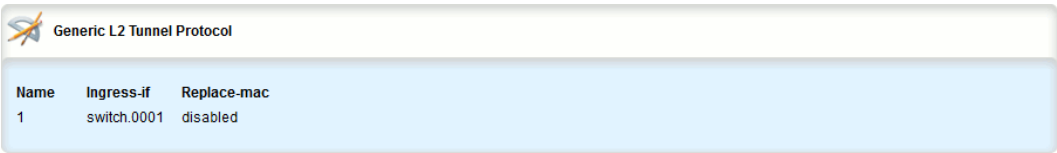
This table provides the following information:

Parameter	Description
tunnel-name	<b>Synopsis:</b> A string 1 to 32 characters long The generic tunnel name.
ifname	<b>Synopsis:</b> A string 1 to 15 characters long The name of the ingress interface.
rx-frames	The number of frames received through the tunnel.
tx-frames	The number of frames transmitted through the tunnel.
rx-chars	The number of bytes received through the tunnel.
tx-chars	The number of bytes transmitted through the tunnel.
errors	The number of errors received through the tunnel.

Section 5.30.7.2

Viewing a List of Generic Tunnels

To view a list of generic tunnels, navigate to *tunnel » l2tunneld » generic*. If tunnels have been configured, the **Generic L2 Tunnel Protocol** table appears.



Name	Ingress-if	Replace-mac
1	switch.0001	disabled

Figure 800: Generic L2 Tunnel Protocol Table

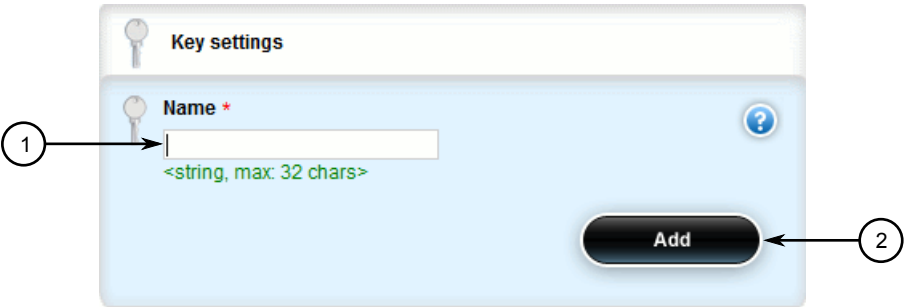
If no generic tunnels have been configured, add tunnels as needed. For more information, refer to [Section 5.30.7.3, “Adding a Generic Tunnel”](#).

Section 5.30.7.3

Adding a Generic Tunnel

To configure a generic tunnel, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *tunnel » I2tunneld » generic* and click **<Add tunnel>**. The **Key Settings** form appears.



Key settings

Name \*

<string, max: 32 chars>

Add

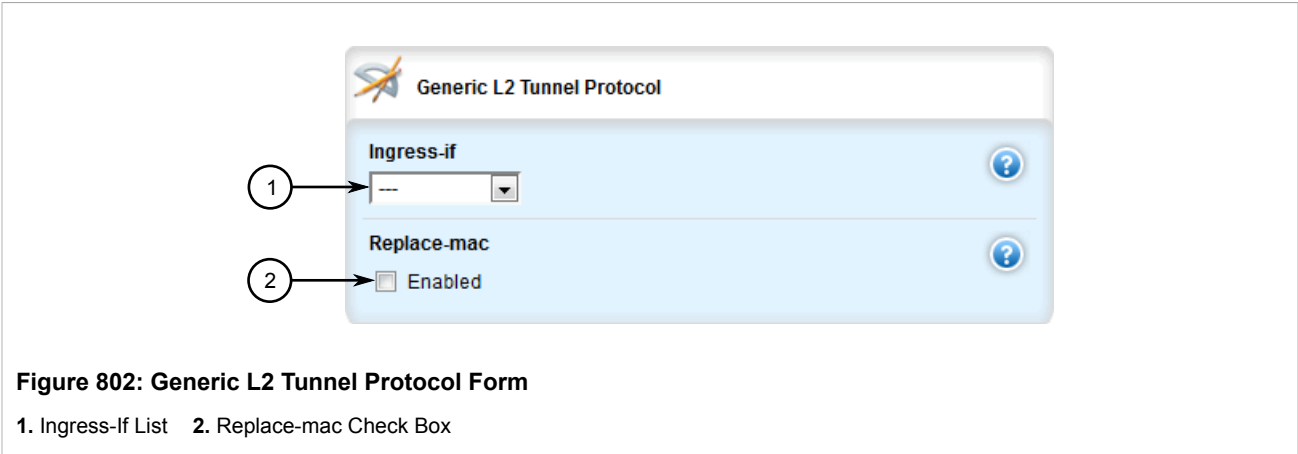
Figure 801: Key Settings Form

1. Name Box    2. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 32 characters long A description of the generic tunnel.

- 4. Click **Add** to create the tunnel. The **Generic L2 Tunnel Protocol** form appears.



**Figure 802: Generic L2 Tunnel Protocol Form**

1. Ingress-If List    2. Replace-mac Check Box

5. Configure the following parameter(s) as required:

Parameter	Description
Ingress Interface	The interface to listen on for Ethernet type frames.
Replace MAC	<b>Synopsis:</b> typeless Replaces the sender's MAC with the out-interface's MAC.

- 6. If necessary, configure one or more remote daemon IP addresses for the tunnel. For more information, refer to [Section 5.30.8.2, “Adding an IP Address”](#).
- 7. If necessary, define one or more Ethernet types to be forwarded. For more information, refer to [Section 5.30.10.2, “Adding an Ethernet Type”](#).
- 8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 9. Click **Exit Transaction** or continue making changes.

Section 5.30.7.4

**Deleting a Generic Tunnel**

To delete a generic tunnel, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *tunnel » l2tunneld » generic*. The **Generic L2 Tunnel Protocol** table appears.

Name	Ingress-if	Replace-mac	Edit	Delete
1	switch.0001	disabled		

1. Add Button 2. Edit Button 3. Delete Button

**Figure 803: Generic L2 Tunnel Protocol Table**

1. Add Button 2. Edit Button 3. Delete Button

3. Click **Delete** next to the chosen tunnel.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.30.8

## 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).*

The following sections describe how to configure and manage remote daemon IP addresses for generic tunnels:

- [Section 5.30.8.1, “Viewing a List of IP Addresses”](#)
- [Section 5.30.8.2, “Adding an IP Address”](#)
- [Section 5.30.8.3, “Deleting an IP Address”](#)

#### Section 5.30.8.1

### Viewing a List of IP Addresses

To view a list of remote L2 protocol server IP addresses for a generic tunnel configuration, navigate to **tunnel » l2tunneld » generic » {name} » remote-daemon » ip-address**, where {name} is the name of the generic tunnel. If IP addresses have been configured, the **Remote Daemon IP Address** table appears.



Remote Daemon IP Address	
ip-address	172.112.10.1

**Figure 804: Remote Daemon IP Address Table**

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to [Section 5.30.7.3, “Adding a Generic Tunnel”](#).

#### Section 5.30.8.2

### Adding an IP Address

To add the IP address of a remote L2 protocols server to a generic tunnel configuration, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » generic » {name} » remote-daemon » ip-address**, where {name} is the name of the generic tunnel.
3. Click **<Add ip-address>**. The **Key Settings** form appears.

**Figure 805: Key Settings Form**

1. IP Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the remote L2 protocol server.

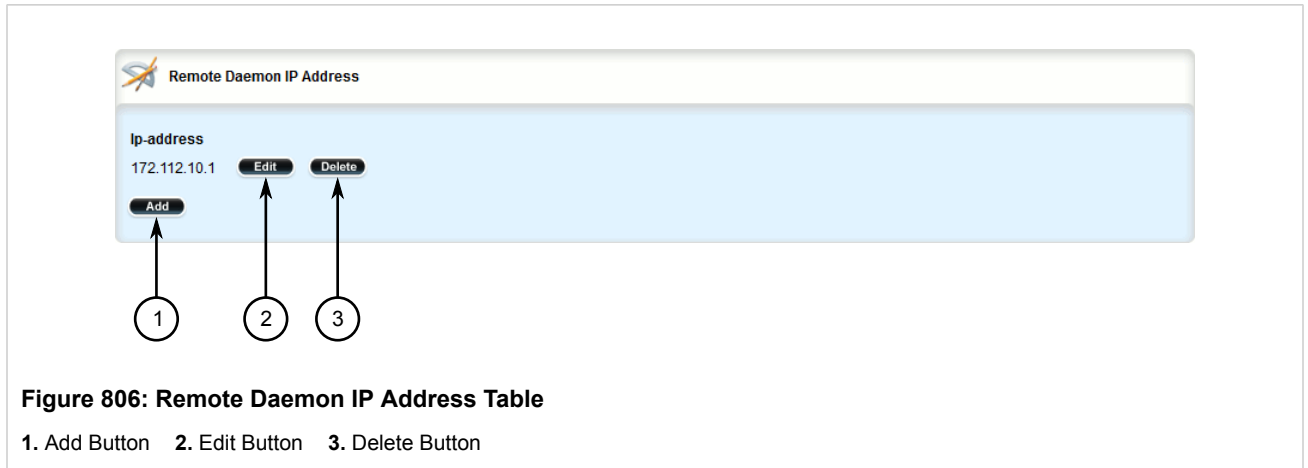
5. Click **Add** to add the IP address.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.30.8.3

## Deleting an IP Address

To delete the IP address of a remote L2 protocols server from a generic tunnel configuration, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » generic » {name} » remote-daemon » ip-address**, where {name} is the name of the generic tunnel. The **Remote Daemon IP Address** table appears.



3. Click **Delete** next to the chosen IP address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.30.9

## Managing Remote Daemon Egress Interfaces for Generic Tunnels

The following sections describe how to configure and manage remote daemon egress interfaces for generic tunnels:

- [Section 5.30.9.1, “Viewing a List of Egress Interfaces”](#)
- [Section 5.30.9.2, “Adding an Egress Interface”](#)
- [Section 5.30.9.3, “Deleting an Egress Interface”](#)

### Section 5.30.9.1

## Viewing a List of Egress Interfaces

To view a list of egress interfaces configured for a generic tunnel, navigate to **tunnel » l2tunneld » generic » {name} » remote-daemon » egress-if**, where {name} is the name of the generic tunnel. If egress interfaces have been configured, the **Generic L2 Tunnel Egress Interface** table appears.

Generic L2 Tunnel Egress Interface
Egress-if switch.0003

**Figure 807: Generic L2 Tunnel Egress Interface Table**

If no egress interfaces have been configured, add interfaces as needed. For more information, refer to [Section 5.30.9.2, “Adding an Egress Interface”](#).

### Section 5.30.9.2

## Adding an Egress Interface

To add an egress interface for a generic tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » generic » {name} » remote-daemon » egress-if**, where {name} is the name of the generic tunnel.
3. Click **<Add egress-if>**. The **Key Settings** form appears.

**Figure 808: Key Settings Form**

1. Egress Interface Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Egress Interface	The egress interface for Ethernet type frames.

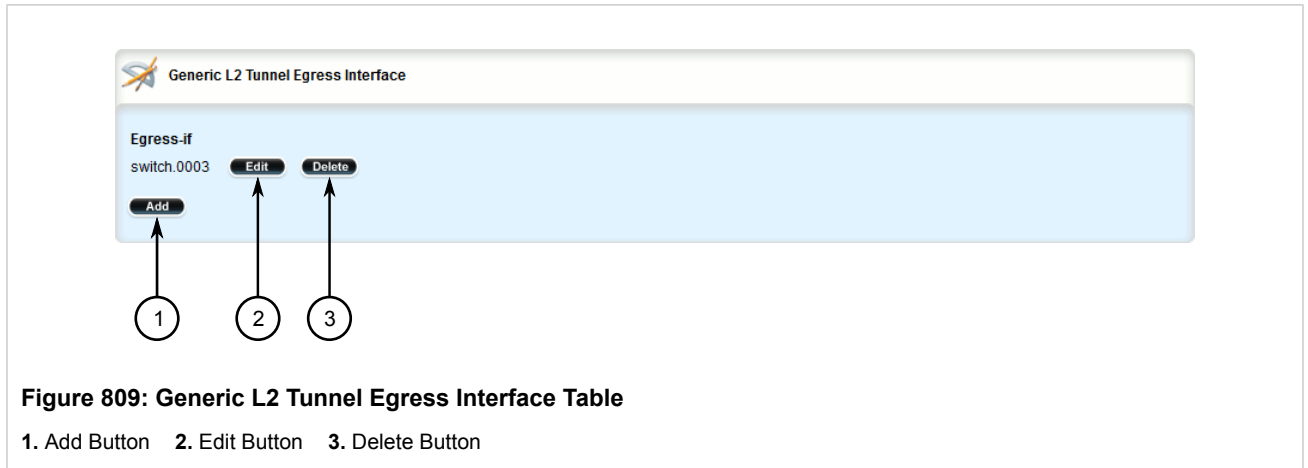
5. Click **Add** to add the egress interface.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.30.9.3

## Deleting an Egress Interface

To delete an egress interface for a generic tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » generic » {name} » remote-daemon » egress-if**, where {name} is the name of the generic tunnel. The **Generic L2 Tunnel Egress Interface** table appears.



3. Click **Delete** next to the chosen egress interface.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.30.10

## Managing Ethernet Types for Generic Tunnels

The following sections describe how to configure and manage Ethernet types for generic tunnels:

- [Section 5.30.10.1, "Viewing a List of Ethernet Types"](#)
- [Section 5.30.10.2, "Adding an Ethernet Type"](#)
- [Section 5.30.10.3, "Deleting an Ethernet Type"](#)

### Section 5.30.10.1

## Viewing a List of Ethernet Types

To view a list of Ethernet types configured for a generic tunnel, navigate to **tunnel » l2tunneld » generic » {name} » ethernet-type**, where {name} is the name of the generic tunnel. If Ethernet types have been configured, the **L2 Ethernet Type** table appears.

**Figure 810: L2 Ethernet Type Table**

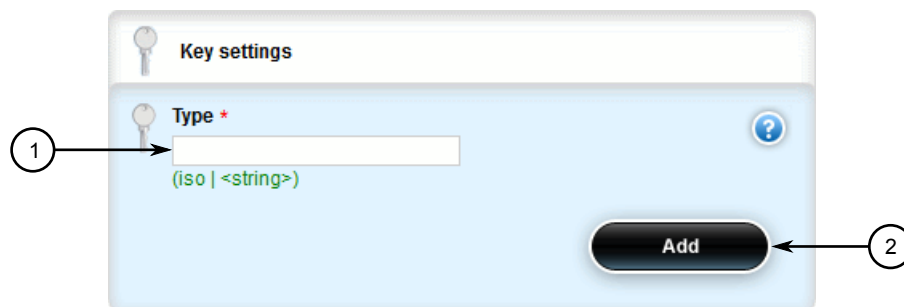
If no Ethernet types have been configured, add types as needed. For more information, refer to [Section 5.30.10.2, “Adding an Ethernet Type”](#).

### Section 5.30.10.2

## Adding an Ethernet Type

To add an Ethernet type for a generic tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » generic » {name} » ethernet-type**, where {name} is the name of the generic tunnel.
3. Click **<Add ethernet-type>**. The **Key Settings** form appears.

**Figure 811: Key Settings Form**

1. Type Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Type	<b>Synopsis:</b> { iso } or a string The Ethernet type to be forwarded (ie. 0xFEFE).

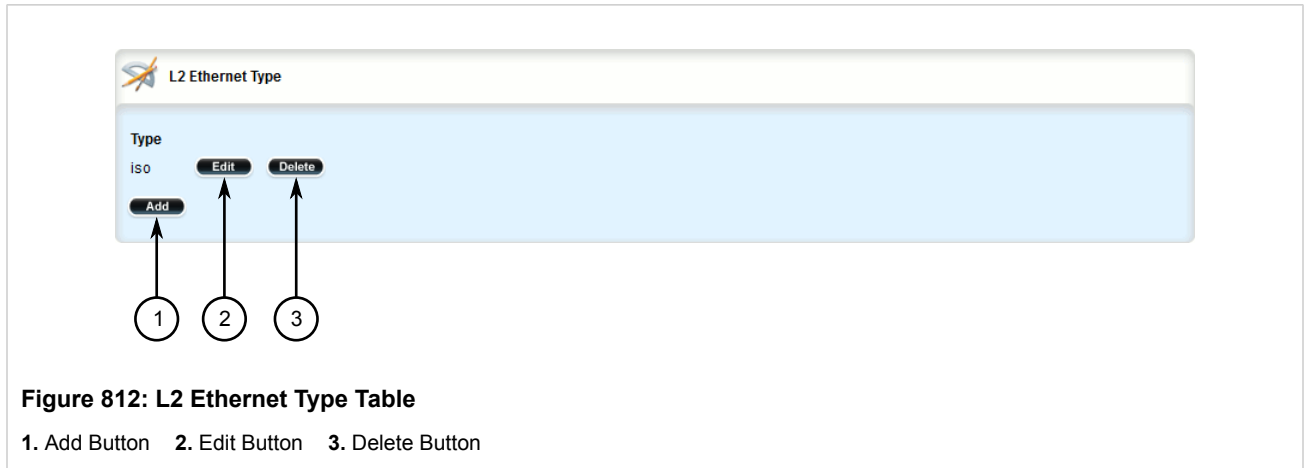
5. Click **Add** to add the Ethernet type.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

Section 5.30.10.3

## Deleting an Ethernet Type

To delete an Ethernet type for a generic tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » l2tunneld » generic » {name} » ethernet-type**, where {name} is the name of the generic tunnel. The **L2 Ethernet Type** table appears.



3. Click **Delete** next to the chosen Ethernet type.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.31

## 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 813: Example – GRE Tunnel Configuration

1. Router 1    2. Router 2

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.

The following sections describe how to configure and manage Generic Routing Encapsulation (GRE) tunnels:

- [Section 5.31.1, “Viewing Statistics for GRE Tunnels”](#)
- [Section 5.31.2, “Viewing a List of GRE Tunnels”](#)
- [Section 5.31.3, “Adding a GRE Tunnel”](#)
- [Section 5.31.4, “Deleting a GRE Tunnel”](#)

Section 5.31.1

# Viewing Statistics for GRE Tunnels

To view the statistics collected for GRE tunnels, navigate to **interfaces » gre**. The **GRE Tunnels Statistics** form appears.

GRE Tunnels Statistics							
Name	Tunnel-status	Rx-packets	Rx-errors	Rx-drops	Tx-packets	Tx-errors	Tx-drops
g1	Active	0	0	0	855	51	0
g2	Active	0	0	0	0	791	0

Figure 814: GRE Tunnels Statistics Form

This table provides the following information:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 10 characters long The GRE tunnel interface name.
tunnel-status	<b>Synopsis:</b> A string The status of the tunnel.
rx-packets	The number of packets received through the tunnel.
rx-errors	The error packets received through the tunnel.
rx-drops	The number of packets dropped by the tunnel.
tx-packets	The number of packets transmitted through the tunnel.
tx-errors	The number of error packets transmitted through the tunnel.
tx-drops	The number of packets dropped by the tunnel.

## Section 5.31.2

## Viewing a List of GRE Tunnels

To view a list of GRE tunnels, navigate to **tunnel » gre**. If tunnels have been configured, the **Generic Routing Encapsulation Interfaces** table appears.



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	disabled	0

**Figure 815: Generic Routing Encapsulation Interfaces Table**

If no GRE tunnels have been configured, add tunnels as needed. For more information, refer to [Section 5.31.3, “Adding a GRE Tunnel”](#).

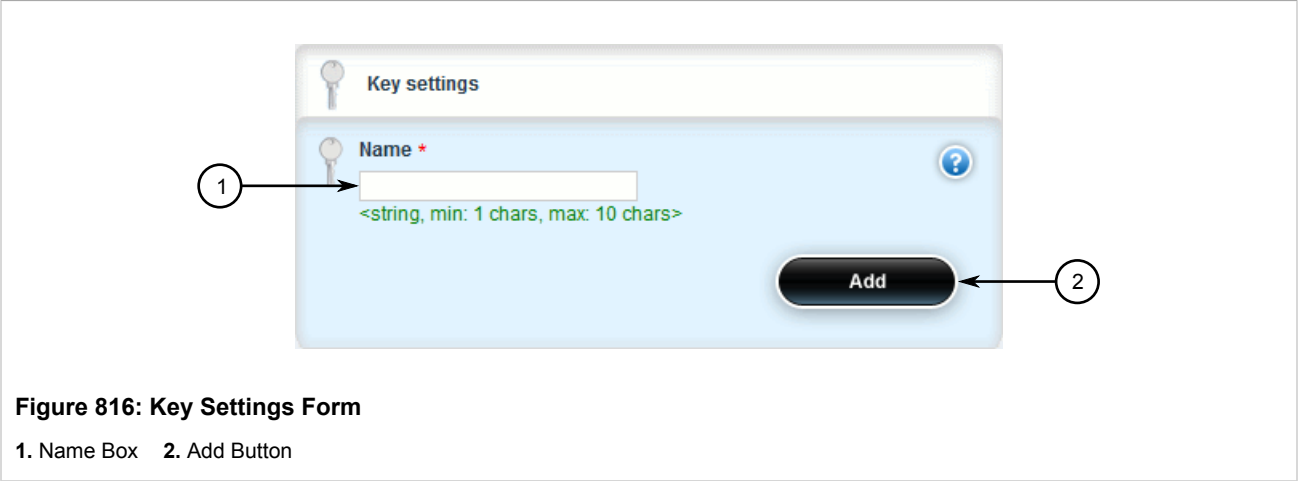
## Section 5.31.3

## Adding a GRE Tunnel

To add a GRE tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **tunnel » gre** and click **<Add gre>** in the menu. The **Key Settings** form appears.

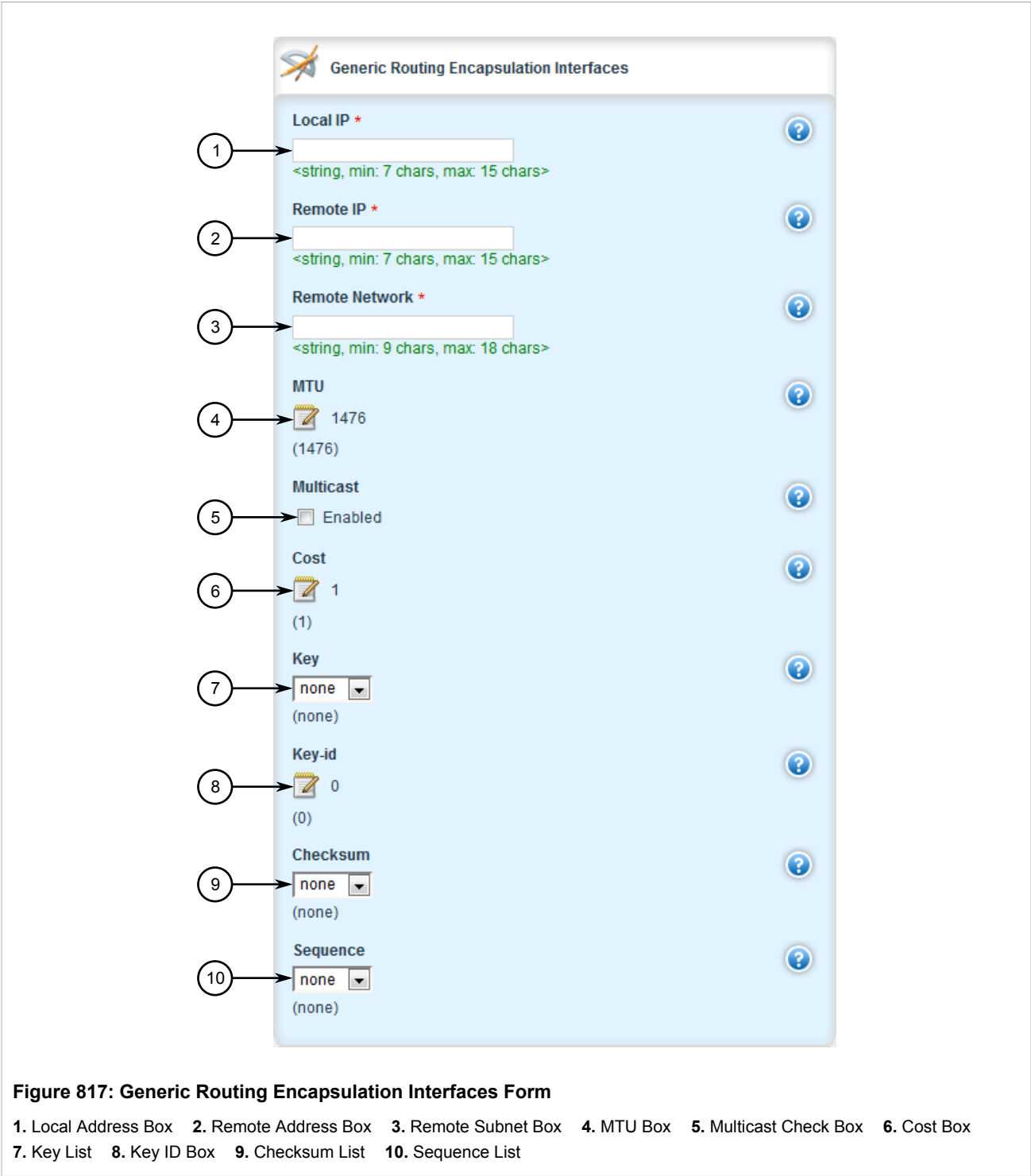




3. Configure the following parameter(s) as required:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 10 characters long The GRE tunnel network interface name - the interface name must start with a lowercase letter, but may contain any combination of lowercase letters, numbers and dashes up to a maximum of 10 characters. The prefix 'gre-' will be added to this interface name.

4. Click **Add**. The **Generic Routing Encapsulation Interfaces** form appears.



5. Configure the following parameter(s) as required:

Parameter	Description
Local IP	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the local end of the tunnel.

Parameter	Description
Remote IP	<b>Synopsis:</b> A string 7 to 15 characters long The IP address of the remote end of the tunnel.
Remote Network	<b>Synopsis:</b> A string 9 to 18 characters long The target network of the remote end of the tunnel (xxx.xxx.xxx.xxx/xx).
MTU	<b>Default:</b> 1476 The MTU of the GRE interface.
Multicast	<b>Synopsis:</b> typeless Enables multicast traffic on the tunnel interface.
Cost	<b>Synopsis:</b> An integer between 1 and 255 <b>Default:</b> 1 The routing cost associated with networking routing that directs traffic through the tunnel.
key	<b>Synopsis:</b> { none, input, output, both } <b>Default:</b> none The key for tunneled packets
key-id	<b>Synopsis:</b> An integer between 0 and 4294967295 <b>Default:</b> 0 The key ID for tunneled packets
checksum	<b>Synopsis:</b> { none, input, output, both } <b>Default:</b> none The checksum for tunneled packets
sequence	<b>Synopsis:</b> { none, input, output, both } <b>Default:</b> none The sequence number for tunneled packets

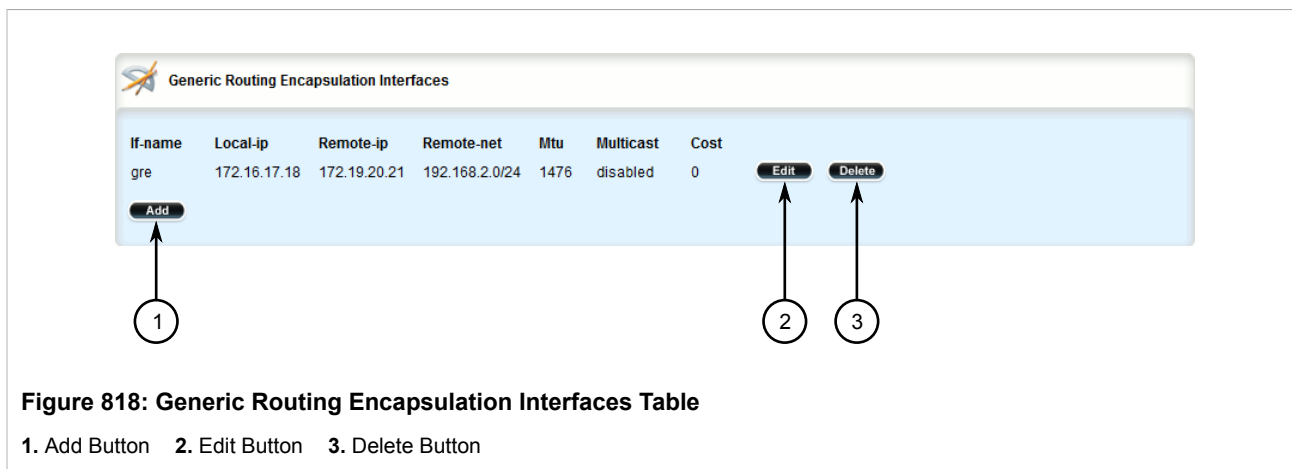
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.31.4

## Deleting a GRE Tunnel

To delete a GRE tunnel, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **tunnel » gre**. The **Generic Routing Encapsulation Interfaces** table appears.

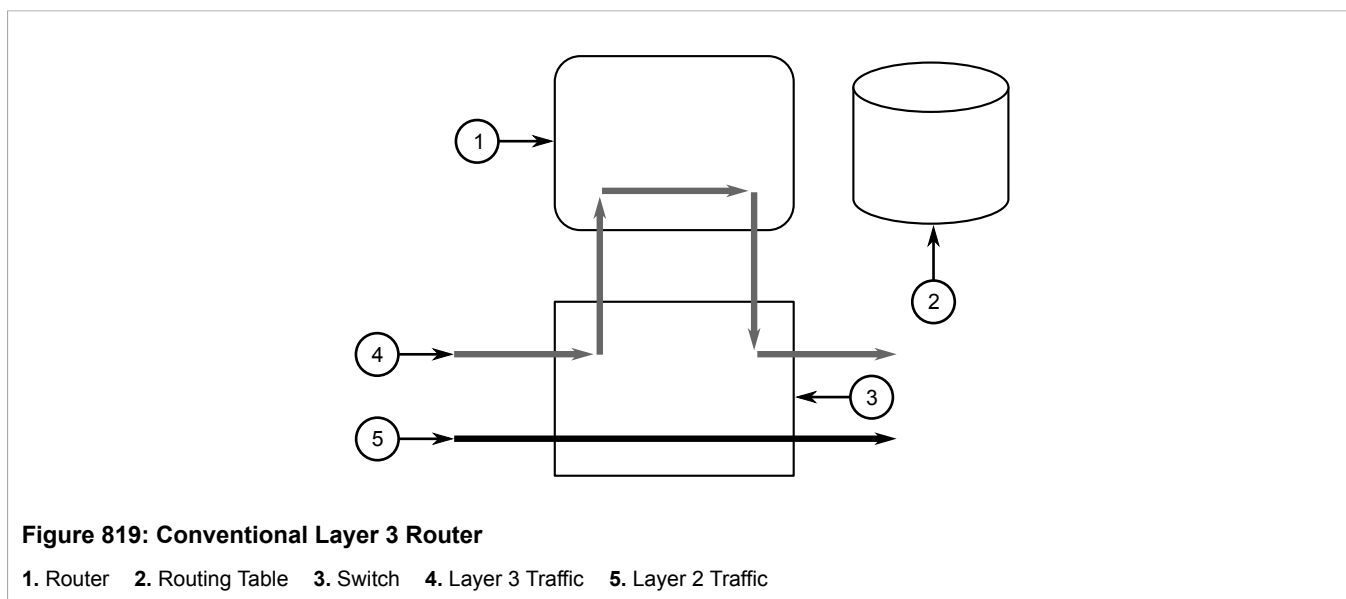


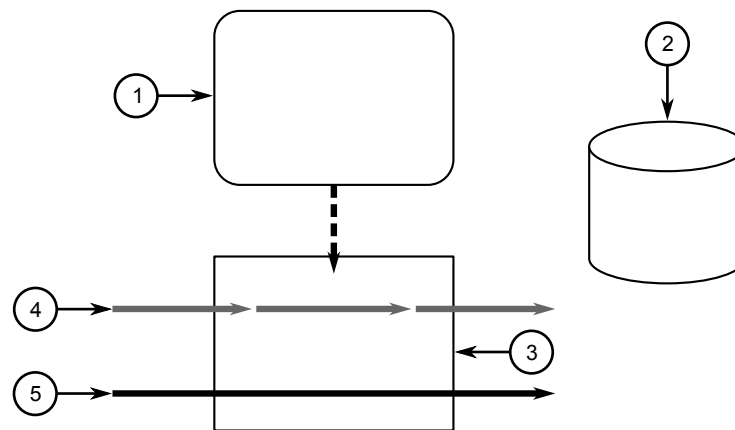
3. Click **Delete** next to the chosen tunnel.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.32

## Managing Layer 3 Switching

A switch is an inter-network device that makes frame forwarding decisions in hardware. A Layer 3 switch, sometimes called a multilayer switch, is one which makes hardware-based decisions for IP packets as well as Layer 2 frames. Traditionally, routers are used to make routing decisions using software. A Layer 3 switch will make the same decisions in hardware, which means that packet forwarding will be much faster than in a conventional router.





**Figure 820: Layer 3 Switch**

1. Router 2. Forwarding Table 3. Switch 4. Layer 3 Traffic 5. Layer 2 Traffic

The following sections describe how to configure and manage Layer 3 switching:

- [Section 5.32.1, “Layer 3 Switching Concepts”](#)
- [Section 5.32.2, “Configuring Layer 3 Switching”](#)
- [Section 5.32.3, “Managing Static ARP Table Entries”](#)
- [Section 5.32.4, “Viewing a Static and Dynamic ARP Table Summary”](#)
- [Section 5.32.5, “Viewing Routing Rules”](#)
- [Section 5.32.6, “Flushing Dynamic Hardware Routing Rules”](#)

#### Section 5.32.1

## Layer 3 Switching Concepts

The following sections describe Layer 3 Switching concepts and rules:

- [Section 5.32.1.1, “Layer 3 Switch Forwarding Table”](#)
- [Section 5.32.1.2, “Static Layer 3 Switching Rules”](#)
- [Section 5.32.1.3, “Dynamic Learning of Layer 3 Switching Rules”](#)
- [Section 5.32.1.4, “Layer 3 Switch ARP Table”](#)
- [Section 5.32.1.5, “Multicast Cross-VLAN Layer 2 Switching”](#)
- [Section 5.32.1.6, “Size of the Layer 3 Switch Forwarding Table”](#)
- [Section 5.32.1.7, “Interaction with the Firewall”](#)

#### Section 5.32.1.1

## Layer 3 Switch Forwarding Table

To route a packet with a specific destination IP address, a router needs the following information:

- **Egress interface (subnet):** this information is stored in the router's Routing Table.



**NOTE**

*In a Layer 2 switched network segment, a VLAN constitutes an IP subnet.*

- **Next-hop gateway Media Access Control (MAC) address:** this information is stored in the router's ARP Table.



**NOTE**

*If the next hop is the destination subnet itself, then the destination host MAC address is required.*

A Layer 3 Switch uses the routing information listed above and translates it into Layer 3 switching rules. These rules are known as the *Layer 3 Switch Forwarding Information Base (FIB)* or the *Layer 3 Switch Forwarding Table*. A Layer 3 switching rule is actually a set of parameters identifying a traffic flow to be switched and determining how to perform the switching.

Layer 3 switching Application-Specific Integrated Circuits (ASICs) store Layer 3 switching rules in a Ternary Content Addressable Memory (TCAM) table. Layer 3 switching rules can be statically configured or dynamically learned (also known as *auto-learned*).

Section 5.32.1.2

## Static Layer 3 Switching Rules

When creating a static route through switch management, hardware acceleration can be explicitly configured. If hardware acceleration is selected, an appropriate Layer 3 switching rule is installed in the ASIC's TCAM and never ages out.



**NOTE**

*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.*

Section 5.32.1.3

## Dynamic Learning of Layer 3 Switching Rules

For static routes without hardware acceleration or for dynamic routes, Layer 3 switching rules can be dynamically learned based on software-based router and firewall decisions. For example, the Layer 3 switch can automatically decide to offload some flows from the router into the Layer 3 Forwarding Table.

After a certain amount of traffic for the same flow is successfully routed, the Layer 3 switching ASIC begins switching the rest of the packets belonging to the same flow. A flow is unidirectional traffic between two hosts. For example, traffic flowing between ports from one host to another is considered a flow. Traffic flowing in the opposite direction between the same ports is considered a different flow.



**NOTE**

*For 8G or 88G SM, the maximum number of Layer 3 switching rules is 1000 or 3000 respectively.*

Different auto-learning methods may be used:

- **Flow-oriented learning** is when the switch uses the following information to identify a traffic flow:
  - Source IP address

- Destination IP address
- Protocol
- Source TCP/UDP port
- Destination TCP/UDP port

This learning method is more granular and requires more ASIC resources, but it provides more flexibility in firewall configuration as the rule takes the protocol and TCP/UDP port into consideration to make forwarding decisions.

- **Host-oriented learning** is when the switch uses the following information to identify a traffic flow:
  - Source IP address
  - Destination IP address

This learning method provides less flexibility in firewall configuration, as the user can allow or disallow traffic between two hosts.

For unicast traffic, each flow constitutes one rule. For multicast routing, one multicast route may constitute several rules.

The Layer 3 switch continuously monitors activity (this is, the presence of traffic) for dynamically learned rules. Because of this, dynamically learned rules may be removed after a configurable time due to inactivity.

#### Section 5.32.1.4

### Layer 3 Switch ARP Table

A router needs to know the destination host or next-hop gateway MAC address for it to forward a packet on the other subnet. Therefore, software maintains an Address Resolution Protocol (ARP) table that maps IP addresses to MAC addresses. The same information is also needed by the Layer 3 switching ASIC when it switches IP packets between subnets.

The destination or gateway MAC address is usually obtained through ARP. However, ARP entries can also be statically configured in the Layer 3 Switch so that they do not time out. When configuring a static ARP entry, if no value is entered for the MAC Address parameter, the address is automatically resolved through ARP and then saved statically. This is preserved across reboots of the device.

For a static Layer 3 switching rule, the destination MAC address for the rule is always resolved, and is also saved statically.

#### Section 5.32.1.5

### Multicast Cross-VLAN Layer 2 Switching

Some RUGGEDCOM Layer 3 Switch models do not have full multicast Layer 3 switching capability and only support multicast cross-VLAN Layer 2 switching. Multicast cross-VLAN Layer 2 switching differs from the normal multicast Layer 3 switching in the following ways:

- Packet modification is not done. Specifically, the source MAC address and Time-To-Live (TTL) values in forwarded packets do not change.
- Separate TCAM table entries are required for each VLAN in the multicast switching rule. For example, a multicast stream ingressing VLAN 1 and egressing VLAN 2 and VLAN 3 requires three TCAM table entries.
- Supported bandwidth depends on the rule. Multicast traffic potentially has multiple egress VLANs, and the total utilized ASIC bandwidth is the ingress bandwidth multiplied by the number of ingress and egress VLANs. For

example, a 256 Mbps multicast stream ingressing VLAN 1 and egressing VLANs 2 and 3 requires 768 Mbps (256 Mbps × 3) of ASIC bandwidth.

- If a multicast packet should be forwarded to multiple egress VLANs, it egresses those VLANs sequentially rather than concurrently. This means the packet will experience different latency for each egress VLAN.

## Section 5.32.1.6

## Size of the Layer 3 Switch Forwarding Table

The routing table in a software router is limited only by the amount of available memory; its size can be virtually unlimited. However, the size of the TCAM in Layer 3 switching ASICs is significantly limited and may not be sufficient to accommodate all Layer 3 switching rules. If the TCAM is full and a new static rule is created, the new rule replaces some dynamically learned rule. If all of the rules in the TCAM are static, then the new static rule is rejected.

## Section 5.32.1.7

## Interaction with the Firewall

If security is a concern and you use a firewall in a Layer 3 Switch, it is important to understand how the Layer 3 switch interacts with the firewall.

A software router always works in agreement with a firewall so that firewall rules are always applied. However, in a Layer 3 Switch, if a switching rule is set in the switching ASIC (for example, due to a statically configured route), the ASIC switches all the traffic matching the rule before the firewall inspects the traffic.

Layer 3 switch ASICs are somewhat limited in how switching rules can be defined. These limitations do not allow configuring arbitrary firewall rules directly in the Layer 3 switch hardware. For sophisticated firewall rules, the firewall has to be implemented in software and the Layer 3 Switch must not switch traffic that is subject to firewall processing.

Whenever a change is made to the firewall configuration, some of the dynamically learned Layer 3 switching rules might conflict with the new firewall configuration. To resolve potential conflicts, dynamically learned Layer 3 switching rules are flushed upon any changes to the firewall configuration. The dynamically learned Layer 3 switching rules then have to be re-learned while the new firewall rules are applied.

For statically configured Layer 3 switching rules, take care to avoid conflicts between Layer 3 switching and the firewall. It should be understood that static Layer 3 switching rules always take precedence. Therefore, you must thoroughly examine the switch configuration for potential conflicts with the firewall. For more information about firewalls, refer to [Section 5.16, "Managing Firewalls"](#)

## Section 5.32.2

## Configuring Layer 3 Switching

To configure Layer 3 switching, do the following:

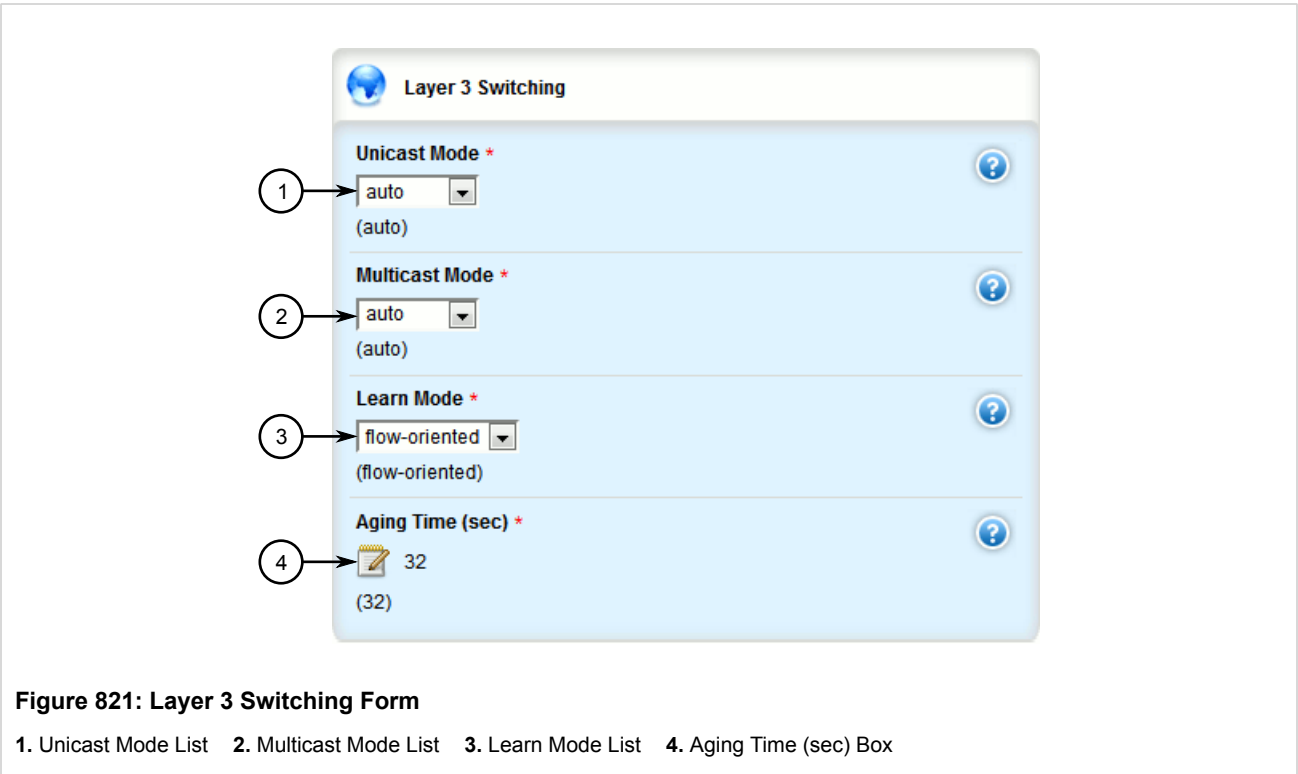
**NOTE**

*When hardware acceleration is used, and learning mode is set to flow-oriented, fragmented IP packets cannot be forwarded. To overcome this limitation, if it is known there will be a significant amount of fragmented packets, set learning mode to host-oriented.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.



2. Navigate to **switch » layer3-switching**. The **Layer 3 Switching** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Unicast Mode	<b>Synopsis:</b> { disabled, auto, static } <b>Default:</b> auto  <itemizedlist><listitem>Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing.</listitem> <listitem>Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering.</listitem> <listitem>Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.</listitem></itemizedlist>
Multicast Mode	<b>Synopsis:</b> { disabled, auto, static } <b>Default:</b> auto  <itemizedlist><listitem>Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing.</listitem> <listitem>Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering.</listitem> <listitem>Auto: Both statically configured and dynamically learned Layer 3 switching

Parameter	Description
	rules will be used. In this mode, maximum routing hardware acceleration is utilized.
Learn Mode	<p><b>Synopsis:</b> { flow-oriented, host-oriented }</p> <p><b>Default:</b> flow-oriented</p> <p>Defines how dynamically learned traffic flows are identified:</p> <ul style="list-style-type: none"> <li>Flow-oriented: Traffic flows are identified by a 5-tuple signature: Src IP address + Dst IP address + Protocol + Src TCP/UDP port + Dst TCP/UDP port. This mode should be used, if fine-granularity firewall filtering is configured in the device (i.e. some flows between two hosts should be forwarded, while other flows between the same two hosts should be filtered). However, this mode utilizes more Layer 3 switching ASIC resources and is not recommended if fine-granularity firewall filtering is not required.</li> <li>Host-oriented: Traffic flows are identified by a 2-tuple signature: Src IP address + Dst IP address. All traffic between two IP hosts is hardware-accelerated regardless of the protocol and TCP/UDP ports. This mode potentially controls multiple flows with a single rule and hence is more efficient in utilizing Layer3 switching ASIC resources.</li> </ul>
Aging Time (sec)	<p><b>Synopsis:</b> An integer between 16 and 600</p> <p><b>Default:</b> 32</p> <p>This parameter configures the time a dynamically learned rule for a traffic flow, which has become inactive, is held before being removed from the Layer 3 switch forwarding table.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.32.3

## Managing Static ARP Table Entries

The following sections describe how to manage static ARP table entries:

- [Section 5.32.3.1, “Viewing a List of ARP Table Entries”](#)
- [Section 5.32.3.2, “Adding a Static ARP Table Entry”](#)
- [Section 5.32.3.3, “Deleting a Static ARP Table Entry”](#)

### Section 5.32.3.1

## Viewing a List of ARP Table Entries

To view a list of static ARP table entries, navigate to **switch » layer3-switching » arp-table**. If table entries have been configured, the **ARP Table Configuration** table appears.

ARP Table Configuration			
IP Address	MAC	VLAN ID	Status
172.30.137.31	00:00:00:00:00:00	1	unresolved

**Figure 822: ARP Table Configuration Table**

If no ARP table entries have been configured, add static ARP table entries as needed. For more information about adding static ARP table entries, refer to [Section 5.32.3.2, “Adding a Static ARP Table Entry”](#).

### Section 5.32.3.2

## Adding a Static ARP Table Entry

To add a static ARP table entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » layer3-switching » arp-table** and click **<Add arp-table>**. The **Key Setting** form appears.

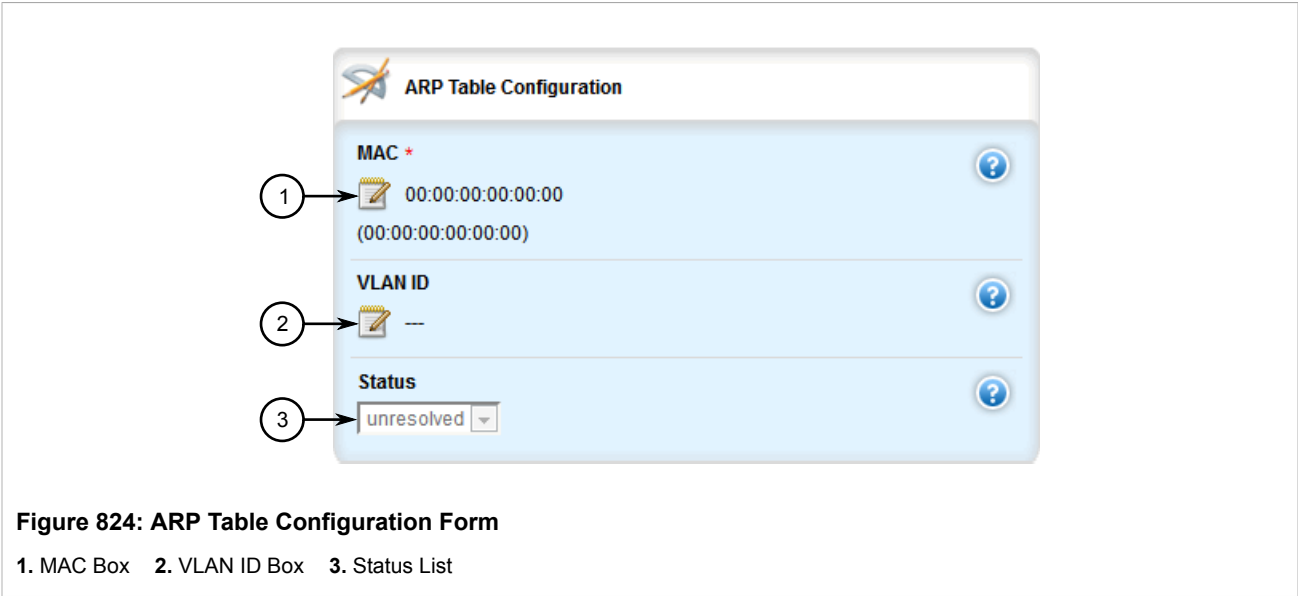
**Figure 823: Key Settings Form**

1. IP Address Box    2. Add Button

3. Configure the following parameters as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string The IP address of the network device the entry describes.

4. Click **Add**. The **ARP Table Configuration** form appears.



5. Configure the following parameters as required:



**NOTE**  
*Letters in MAC addresses must be lowercase.*

Parameter	Description
MAC	<b>Synopsis:</b> A string <b>Default:</b> 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 The VLAN Identifier of the VLAN upon which the MAC address operates.
status	<b>Synopsis:</b> { resolved, unresolved } <b>Default:</b> unresolved Address Resolution Protocol (ARP) entry resolution status: <itemizedlist><listitem>Resolved: The MAC-IP address pair is resolved and operational.</listitem> <listitem>Unresolved: The device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically.</listitem></itemizedlist>

6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

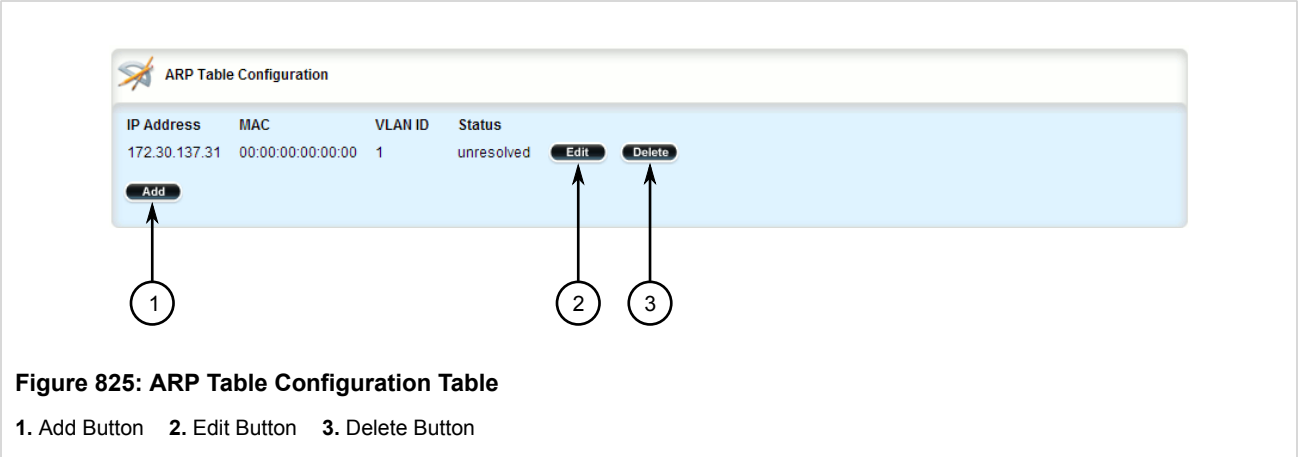
Section 5.32.3.3

### Deleting a Static ARP Table Entry

To delete a static ARP table entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to **switch » layer3-switching » arp-table**. The **ARP Table Configuration** table appears.

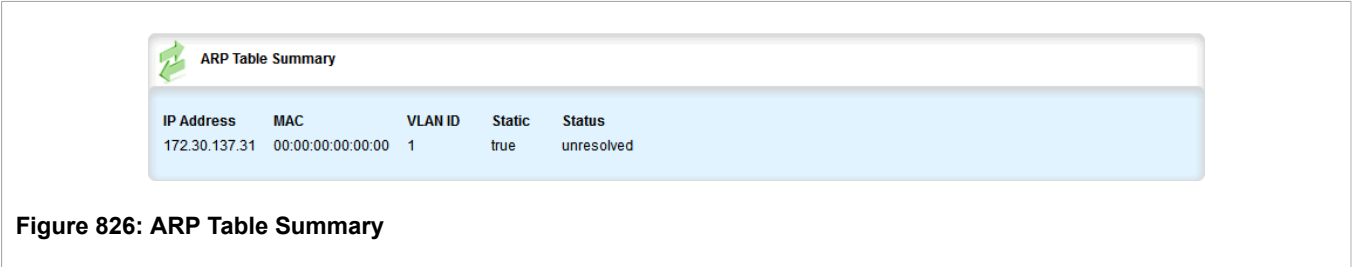


3. Click **Delete** button next to the chosen address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.32.4

Viewing a Static and Dynamic ARP Table Summary

To view a static and dynamic ARP table summary, navigate to **switch » layer3-switching » arp-table-summary**. If ARP table entries have been configured, the **ARP Table Summary** appears.



This table provides the following information:

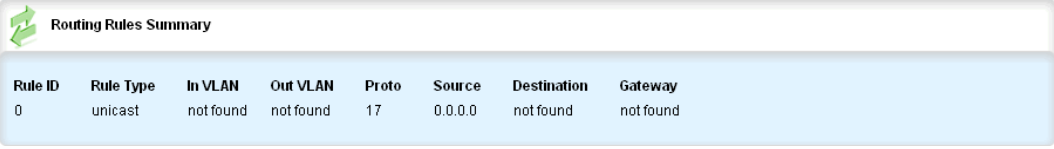
Parameter	Description
IP Address	<b>Synopsis:</b> A string The IP address of the network device the entry describes.
MAC	<b>Synopsis:</b> A string <b>Default:</b> 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
VLAN ID	The VLAN Identifier of the VLAN upon which the MAC address operates.
static	<b>Synopsis:</b> true or false <b>Default:</b> true

Parameter	Description
	Whether the entry is static or dynamic. Static entries are configured as a result of management activity. Dynamic entries are automatically learned by the device and can be unlearned.
status	<b>Synopsis:</b> { resolved, unresolved } <b>Default:</b> unresolved  The Address Resolution Protocol (ARP) entry resolution status: <itemizedlist><listitem>Resolved: MAC-IP address pair is resolved and operational.</listitem> <listitem>Unresolved: the device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically.</listitem></itemizedlist>

## Section 5.32.5

## Viewing Routing Rules

To view a list of routing rules, navigate to **switch » layer3-switching » routing-rules-summary**. If any static or dynamic ARP table entries are configured, the **Routing Rules Summary** table appears.



The image shows a screenshot of the 'Routing Rules Summary' table in a web interface. The table has a title bar with a green icon and the text 'Routing Rules Summary'. Below the title bar is a table with the following data:

Rule ID	Rule Type	In VLAN	Out VLAN	Proto	Source	Destination	Gateway
0	unicast	not found	not found	17	0.0.0.0	not found	not found

Figure 827: Routing Rules Summary Table

This table provides the following information:

Parameter	Description
Rule ID	<b>Synopsis:</b> An integer between 0 and 2999 Defines the order in which rules are matched on each ingress packet. The first matched rule is applied on the packet.
Rule Type	<b>Synopsis:</b> { multicast, unicast, invalid, hidden } Identifies the type of the rule: unicast,multicast,invalid.
In VLAN	Identifies the ingress VLAN. To match the rule, the packet's ingress VLAN must match the number.
Out VLAN(s)	Identifies the egress VLAN. The matched multicast packet is sent to the identified VLAN.
Protocol	The IP Encapsulated Protocol number. Unless zero is specified, the incoming packet's IP protocol must match this number.
source	<b>Synopsis:</b> { any } or a string Identifies the source IP address or subnet. To match the rule, the incoming packet's source IP address must belong to the subnet.
Source Port	<b>Synopsis:</b> An integer between 0 and 65535 The port associated with the source flow. A value of 0 means Not Applicable.
destination	<b>Synopsis:</b> { any } or a string Defines the destination IP address or subnet. To match the rule, the incoming packet's destination IP address must belong to the subnet.
Destination Port	<b>Synopsis:</b> An integer between 0 and 65535

Parameter	Description
	The port associated with the destination flow. A value of 0 means Not Applicable.
gateway	<b>Synopsis:</b> A string Defines the nexthop IP address. The matched unicast packet is sent to the identified gateway.
Pkts/sec	Displays the statistical throughput of all packets matching the rule, in packets per second.
static	<b>Synopsis:</b> true or false Whether the rule is static or dynamic. Static rules are configured as a result of management activity. Dynamic rules are automatically learned by the device and can be unlearned subject to aging time.
routing-action	<b>Synopsis:</b> { forward, exclude } The action applied to packets matching the rule: <itemizedlist><listitem>Forward: Perform a hardware acceleration.</listitem> <listitem>Exclude: Exclude from hardware acceleration and always pass matching packets to the CPU for software routing.</listitem></itemizedlist>
status	<b>Synopsis:</b> { active, resolving, pending, excluding } Whether the rule is currently operational or not: <itemizedlist><listitem>Active: The rule is fully operational and can be applied, so hardware acceleration is performed.</listitem> <listitem>Resolving: The rule is not operational yet due to some unresolved information, like the Address Resolution Protocol (ARP) or gateway's MAC address in the MAC Address Table. Hardware acceleration is not performed.</listitem> <listitem>Pending: there are not enough hardware resources to setup the rule and all its dependencies. Hardware acceleration is not performed.</listitem></itemizedlist>

## Section 5.32.6

## Flushing Dynamic Hardware Routing Rules

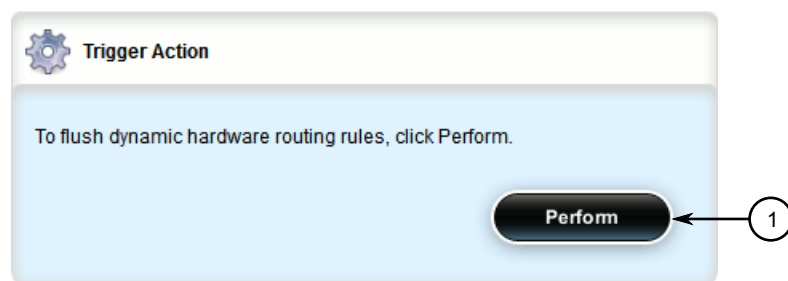
Flushing dynamic hardware routing rules removed dynamic rules from the Routing Rules Summary table.

**NOTE**

*Only dynamic rules can be flushed. Static rules, enabled by activating hardware acceleration, never age out. For more information about enabling hardware acceleration, refer to [Section 5.32.1, “Layer 3 Switching Concepts”](#).*

To flush dynamic hardware routing rules, do the following:

1. Navigate to **switch » layer3-switching** and click **flush-dynamic-rules**. The **Trigger Action** form appears.



**Figure 828: Trigger Action Form**

1. Perform Button

2. Click **Perform**.

Section 5.33

## 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.

The following sections describe how to configure and manage classes of service:

- [Section 5.33.1, "Configuring Classes of Service"](#)
- [Section 5.33.2, "Managing Priority-to-CoS Mapping"](#)
- [Section 5.33.3, "Managing DSCP-to-CoS Mapping"](#)

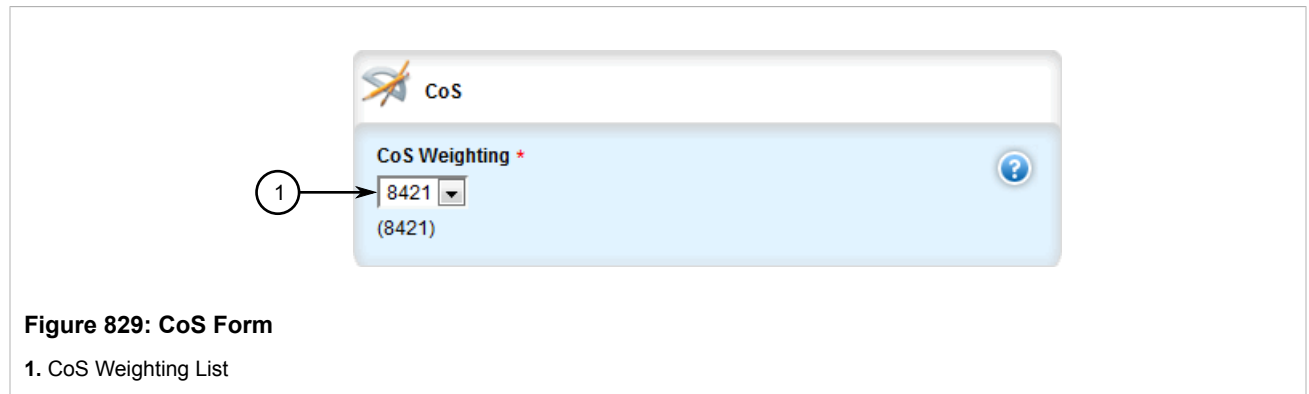


## Section 5.33.1

## Configuring Classes of Service

To configure Classes of Service, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » class-of-service**. The **CoS** form appears.



3. Configure the following parameters as required:

Parameter	Description
CoS Weighting	<b>Synopsis:</b> { 8421, strict } <b>Default:</b> 8421 During traffic bursts, frames queued in the switch pending transmission on a port may have different Class of Service (CoS) priorities. This parameter specifies the weighting algorithm for transmitting different priority CoS frames.

4. 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 5.33.2.2, “Adding a Priority-to-CoS Mapping Entry”](#) or [Section 5.33.3.2, “Adding a DSCP-to-CoS Mapping Entry”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

## Section 5.33.2

## 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.

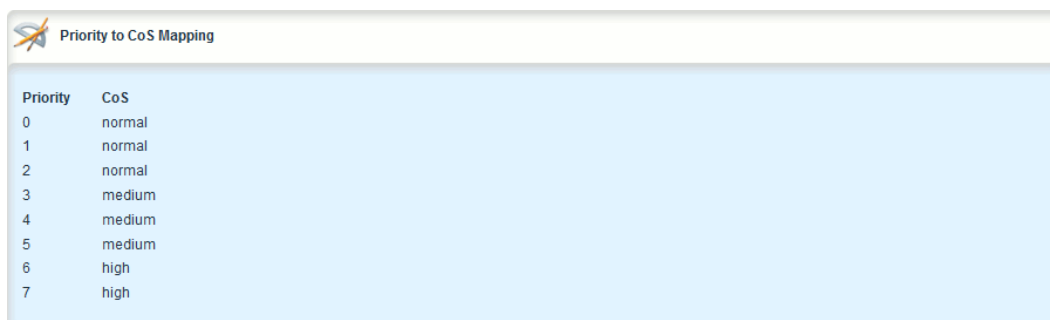
The following sections describe how to configure and manage priority-to-CoS mapping:

- [Section 5.33.2.1, “Viewing a List of Priority-to-CoS Mapping Entries”](#)
- [Section 5.33.2.2, “Adding a Priority-to-CoS Mapping Entry”](#)
- [Section 5.33.2.3, “Deleting a Priority-to-CoS Mapping Entry”](#)

### Section 5.33.2.1

## Viewing a List of Priority-to-CoS Mapping Entries

To view a list of priority-to-CoS mapping entries, navigate to **switch » class-of-service » priority-to-cos**. If priorities have been configured, the **Priority to CoS Mapping** table appears.



Priority	CoS
0	normal
1	normal
2	normal
3	medium
4	medium
5	medium
6	high
7	high

**Figure 830: Priority to CoS Mapping Table**

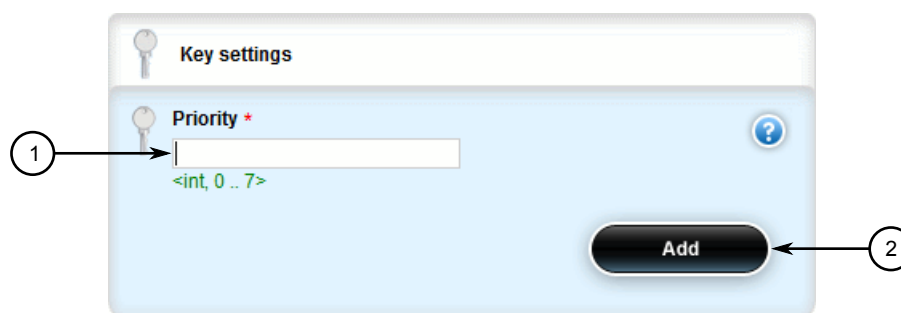
If no entries have been configured, add entries as needed. For more information, refer to [Section 5.33.2.2](#), “Adding a Priority-to-CoS Mapping Entry”.

### Section 5.33.2.2

## Adding a Priority-to-CoS Mapping Entry

To add a priority-to-CoS mapping entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » class-of-service » priority-to-cos** and click **<Add priority-to-cos>**. The **Key Settings** form appears.



The image shows the 'Key settings' form. It has a title bar with a key icon and the text 'Key settings'. Below the title bar is a section with a key icon, the label 'Priority \*', and a text input field. Below the input field is the text '<int, 0 .. 7>'. A circled number '1' with an arrow points to the input field. To the right of the input field is a blue question mark icon. At the bottom right of the form is a dark blue button with the text 'Add'. A circled number '2' with an arrow points to the 'Add' button.

**Figure 831: Key Settings Form**

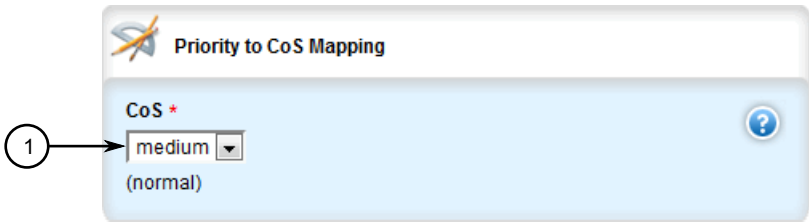
1. Priority Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Priority	<b>Synopsis:</b> An integer between 0 and 7

Parameter	Description
	The value of the IEEE 802.1p priority.

- Click **Add** to add the priority. The **Priority to CoS Mapping** form appears.



**Figure 832: Priority to CoS Mapping Form**

1. CoS List

- Configure the following parameter(s) as required:



**IMPORTANT!**

*Since RSTP BPDU's are sent through the critical CoS queue, take extra care when adding a priority with a CoS set to Critical.*

Parameter	Description
CoS	<p><b>Synopsis:</b> { normal, medium, high, crit }</p> <p><b>Default:</b> normal</p> <p>The Class of Service (CoS) assigned to received tagged frames with the specified IEEE 802.1p priority value.</p>

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.33.2.3

## 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.*

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » class-of-service » priority-to-cos**. The **Priority to CoS Mapping** table appears.

Priority	CoS	Edit	Delete
0	normal	Edit	Delete
1	normal	Edit	Delete
2	normal	Edit	Delete
3	medium	Edit	Delete
4	medium	Edit	Delete
5	medium	Edit	Delete
6	high	Edit	Delete
7	high	Edit	Delete

1. Add Button    2. Edit Button    3. Delete Button

**Figure 833: Priority to CoS Mapping Table**

1. Add Button    2. Edit Button    3. Delete Button

- Click **Delete** next to the chosen priority.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.33.3

## 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.

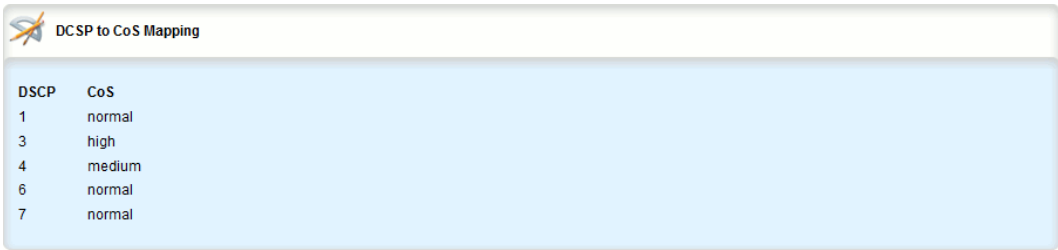
The following sections describe how to configure and manage DSCP-to-CoS mapping:

- [Section 5.33.3.1, “Viewing a List of DSCP-to-CoS Mapping Entries”](#)
- [Section 5.33.3.2, “Adding a DSCP-to-CoS Mapping Entry”](#)
- [Section 5.33.3.3, “Deleting a DSCP-to-CoS Mapping Entry”](#)

### Section 5.33.3.1

## Viewing a List of DSCP-to-CoS Mapping Entries

To view a list of DSCP-to-CoS mapping entries, navigate to **switch » class-of-service » dscp-to-cos**. If DSCPs have been configured, the **DSCP to CoS Mapping** table appears.



DSCP	CoS
1	normal
3	high
4	medium
6	normal
7	normal

Figure 834: DSCP to CoS Mapping Table

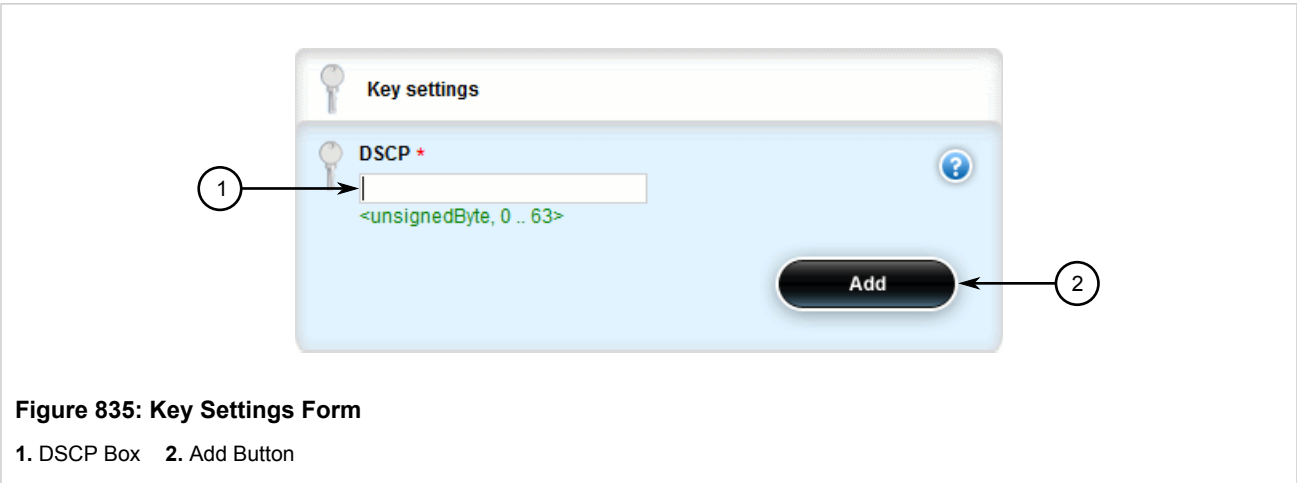
If no entries have been configured, add entries as needed. For more information, refer to [Section 5.33.3.2, “Adding a DSCP-to-CoS Mapping Entry”](#).

Section 5.33.3.2

Adding a DSCP-to-CoS Mapping Entry

To add a DSCP-to-CoS mapping entry, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *switch » class-of-service » dcsp-to-cos* and click **<Add dscp>**. The **Key Settings** form appears.



**Figure 835: Key Settings Form**

1. DSCP Box    2. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
DSCP	<b>Synopsis:</b> An integer between 0 and 63 The Differentiated Services Code Point (DSCP); a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header.

- 4. Click **Add** to add the DSCP. The **DSCP to CoS Mapping** form appears.

**Figure 836: DSCP to CoS Mapping Form**

1. CoS List

5. Configure the following parameter(s) as required:

Parameter	Description
CoS	<p><b>Synopsis:</b> { normal, medium, high, crit }</p> <p><b>Default:</b> normal</p> <p>The Class of Service (CoS) assigned to the received frames with the specified DSCP.</p>

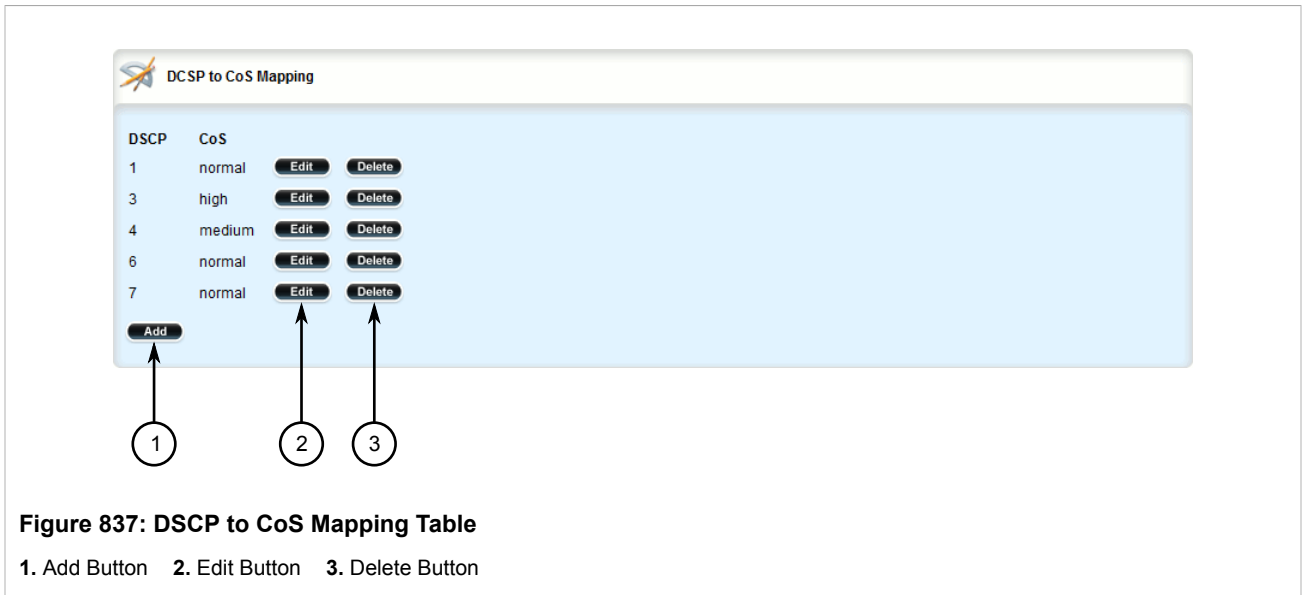
6. Configure the CoS parameters on select switched Ethernet ports and/or trunk interfaces as needed. For more information, refer to [Section 3.18.2, “Configuring a Switched Ethernet Port”](#) and/or [Section 3.22.2, “Adding an Ethernet Trunk Interface”](#).
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.33.3.3

## Deleting a DSCP-to-CoS Mapping Entry

To delete a DSCP-to-CoS mapping entry, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » class-of-service » dscp-to-cos**. The **DSCP to CoS Mapping** table appears.



3. Click **Delete** next to the chosen DSCP.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.34

## Managing MAC Addresses

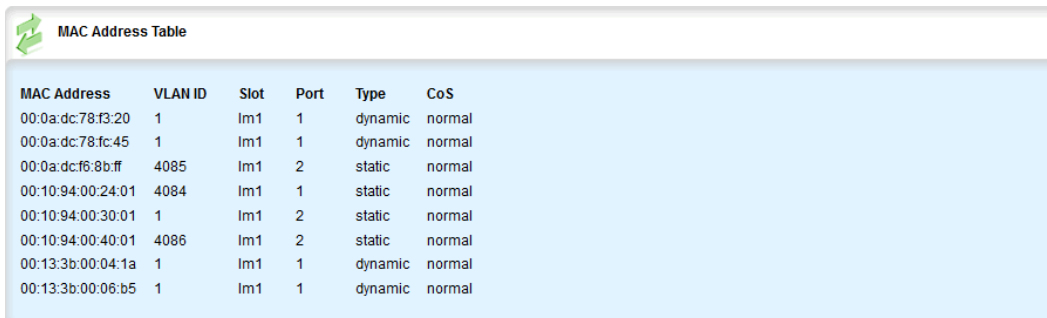
The following sections describe how to configure and manage MAC addresses:

- [Section 5.34.1, “Viewing a Dynamic List of MAC Addresses”](#)
- [Section 5.34.2, “Purging the Dynamic MAC Address List”](#)
- [Section 5.34.3, “Configuring MAC Address Learning Options”](#)
- [Section 5.34.4, “Managing Static MAC Addresses”](#)

#### Section 5.34.1

## Viewing a Dynamic List of MAC Addresses

To view a dynamic list of learned and statically configured MAC addresses, navigate to **switch » mac-tables » mac-table**. If MAC addresses have been learned, the **MAC Address Table** appears.

A screenshot of the 'MAC Address Table' from a network device's web interface. The table has a light blue header and a white body. It contains 8 rows of data. The columns are: MAC Address, VLAN ID, Slot, Port, Type, and CoS. The data rows show various MAC addresses, VLAN IDs (1, 4085, 4084, 4086), slots (Im1), ports (1, 2), types (dynamic, static), and CoS (normal).

MAC Address	VLAN ID	Slot	Port	Type	CoS
00:0a:dc:78:f3:20	1	Im1	1	dynamic	normal
00:0a:dc:78:fc:45	1	Im1	1	dynamic	normal
00:0a:dc:f6:8b:ff	4085	Im1	2	static	normal
00:10:94:00:24:01	4084	Im1	1	static	normal
00:10:94:00:30:01	1	Im1	2	static	normal
00:10:94:00:40:01	4086	Im1	2	static	normal
00:13:b0:00:04:1a	1	Im1	1	dynamic	normal
00:13:b0:00:06:b5	1	Im1	1	dynamic	normal

**Figure 838: MAC Address Table**

This table provides the following information:

Parameter	Description
MAC Address	<b>Synopsis:</b> A string The MAC address learned by the switch.
VLAN ID	The VLAN identifier of the VLAN upon which the MAC address operates.
Slot	<b>Synopsis:</b> { sm, Im1, Im2, Im3, Im4, Im5, Im6, swport, eth, serport, celport } The slot containing the module including the port.
Port	<b>Synopsis:</b> An integer between 1 and 16 The port on which the MAC address has been learned.
Type	<b>Synopsis:</b> { static, dynamic } How the MAC address has been learned by the switch: <ul style="list-style-type: none"><li>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.</li><li>DYNAMIC: The address has been automatically learned by the switch and can be automatically unlearned.</li></ul>
CoS	<b>Synopsis:</b> { N/A, normal, medium, high, crit } The Class Of Service (CoS) that is assigned to frames carrying this address as a source or destination address.

If a MAC address is not listed, do the following:

- Configure the MAC address learning options to dynamically detect the MAC addresses of other devices on the network. For more information, refer to [Section 5.34.3, “Configuring MAC Address Learning Options”](#).
- Configure the address on the device as a static MAC address. For more information, refer to [Section 5.34.4.2, “Adding a Static MAC Address”](#).

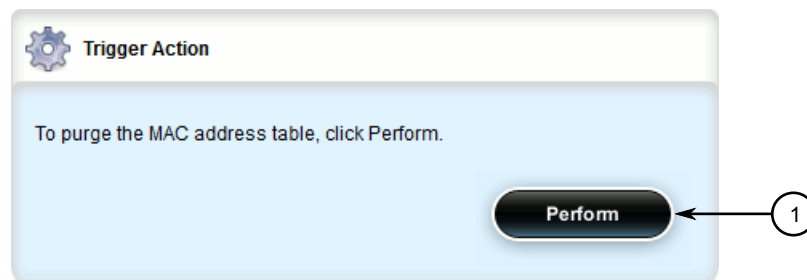
#### Section 5.34.2

## Purging the Dynamic MAC Address List

To purge the dynamic MAC address list of all entries, do the following:

1. Navigate to **switch » mac-tables** and click **purge-mac-table** in the menu. The **Trigger Action** form appears.

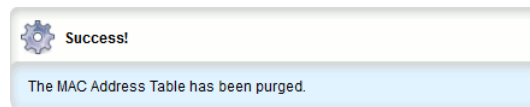




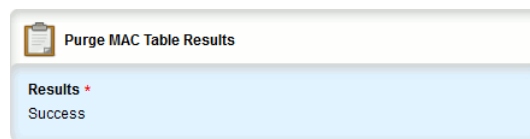
**Figure 839: Trigger Action Form**

1. Perform Button

2. Click the **Perform** button. Once the table is purged, the **Success!** and **Purge MAC Table Results** forms appear.



**Figure 840: Success! Form**



**Figure 841: Purge MAC Table Results Form**

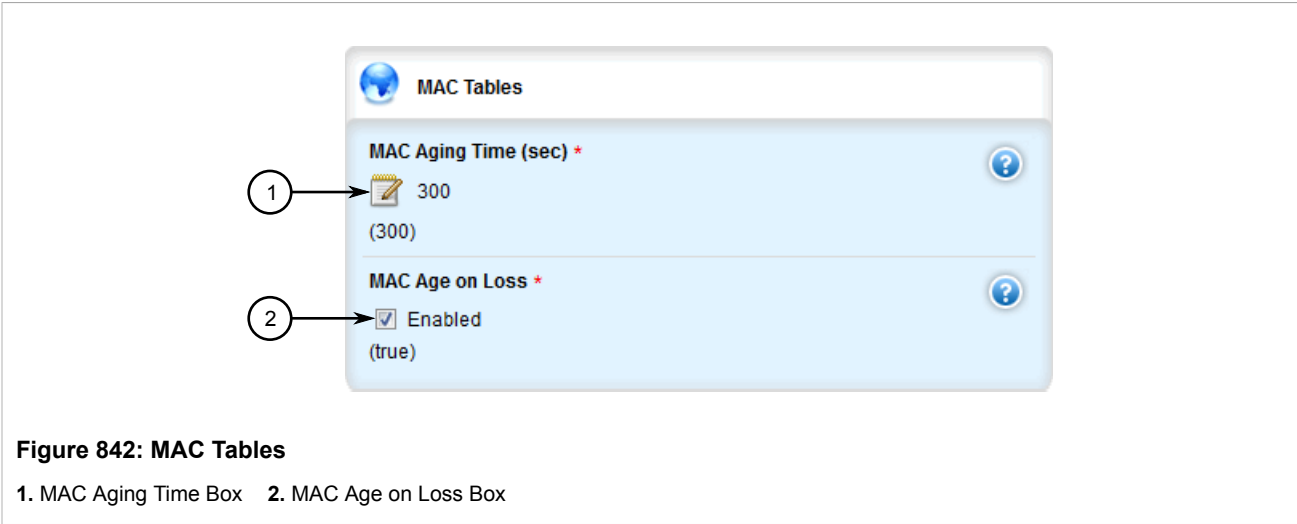
### Section 5.34.3

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mac-tables**. The **MAC Tables** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
MAC Aging Time (sec)	<b>Synopsis:</b> An integer between 15 and 800 <b>Default:</b> 300 The time a learned MAC address is held before being aged out.
MAC Age on Loss	<b>Synopsis:</b> true or false <b>Default:</b> 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.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.34.4

# Managing Static MAC Addresses

Static MAC addresses must be configured when the device is 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.

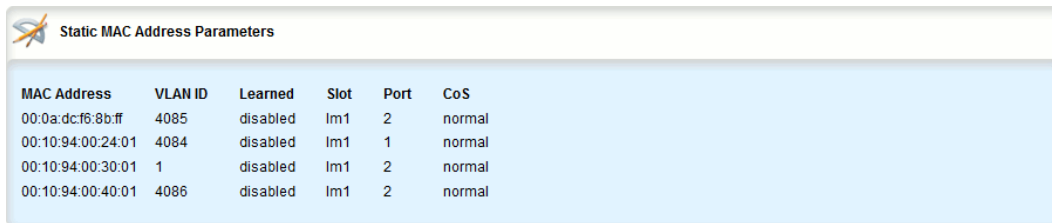
The following sections describe how to configure and manage static MAC addresses:

- [Section 5.34.4.1, “Viewing a List of Static MAC Addresses”](#)
- [Section 5.34.4.2, “Adding a Static MAC Address”](#)
- [Section 5.34.4.3, “Deleting a Static MAC Address”](#)

## Section 5.34.4.1

## Viewing a List of Static MAC Addresses

To view a list of static MAC addresses configured on the device, navigate to **switch » mac-tables » static-mac-table**. If static MAC addresses have been configured, the **Static MAC Address Parameters** table appears.



MAC Address	VLAN ID	Learned	Slot	Port	CoS
00:0a:dcf6:8b:ff	4085	disabled	1m1	2	normal
00:10:94:00:24:01	4084	disabled	1m1	1	normal
00:10:94:00:30:01	1	disabled	1m1	2	normal
00:10:94:00:40:01	4086	disabled	1m1	2	normal

**Figure 843: Static MAC Address Parameters Table**

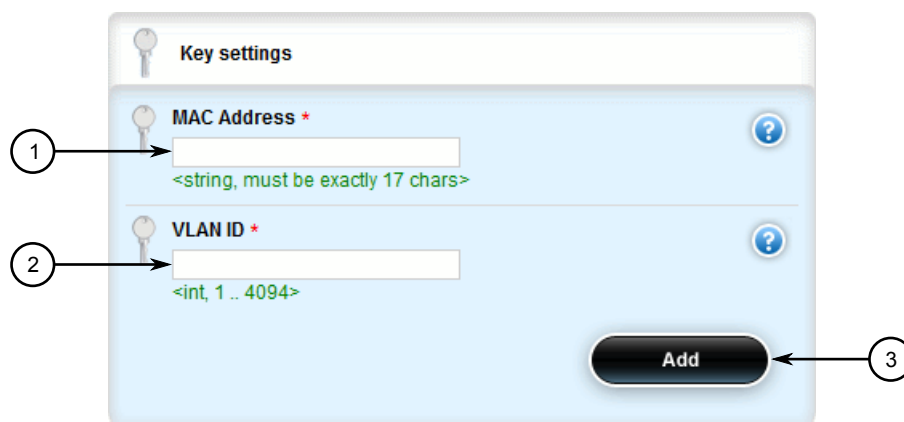
If no static MAC addresses have been configured, add addresses as needed. For more information, refer to [Section 5.34.4.2, “Adding a Static MAC Address”](#).

## Section 5.34.4.2

## Adding a Static MAC Address

To add a static MAC address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » mac-tables » static-mac-table** and click **<Add static-mac>**. The **Key Settings** form appears.



The Key Settings form contains two input fields and an Add button. The first field is labeled 'MAC Address \*' with a red asterisk and a blue question mark icon. Below it is a text input box and a green hint text '<string, must be exactly 17 chars>'. The second field is labeled 'VLAN ID \*' with a red asterisk and a blue question mark icon. Below it is a text input box and a green hint text '<int, 1 .. 4094>'. At the bottom right is a black 'Add' button. Three numbered circles with arrows point to these elements: circle 1 points to the MAC Address input box, circle 2 points to the VLAN ID input box, and circle 3 points to the Add button.

**Figure 844: Key Settings Form**

1. MAC Address Box   2. VLAN ID Box   3. Add Button

3. Configure the following parameter(s) as required:



**NOTE**  
*Letters in MAC addresses must be lowercase.*

Parameter	Description
MAC Address	<b>Synopsis:</b> A string A unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 The VLAN identifier of the VLAN upon which the MAC address operates.

4. Click **Add** to add the static MAC address. The **Static MAC Address Parameters** form appears.

The image shows the 'Static MAC Address Parameters' form. It has a title bar with a logo and the text 'Static MAC Address Parameters'. Below the title bar, there are four sections, each with a parameter name and a control element. The first section is 'Learned' with a checkbox labeled 'Enabled'. The second section is 'Slot' with a dropdown menu showing '--'. The third section is 'Port' with a dropdown menu showing '--'. The fourth section is 'CoS \*' with a dropdown menu showing 'normal' and '(normal)' below it. Each section has a blue circular help icon with a question mark to its right. Numbered callouts 1 through 4 point to the 'Enabled' checkbox, the 'Slot' dropdown, the 'Port' dropdown, and the 'CoS' dropdown respectively.

**Figure 845: Static MAC Address Parameters Form**

1. Learned Check Box   2. Slot List   3. Port List   4. CoS List

5. Configure the following parameter(s) as required:

Parameter	Description
learned	<b>Synopsis:</b> typeless If set, the system will auto-learn the port upon which the device with this address is located.
Slot	The name of the module location provided on the silkscreen across the top of the device.
Port	The selected ports on the module installed in the indicated slot.
CoS	<b>Synopsis:</b> { N/A, normal, medium, high, crit } <b>Default:</b> normal The priority of traffic for a specified address.

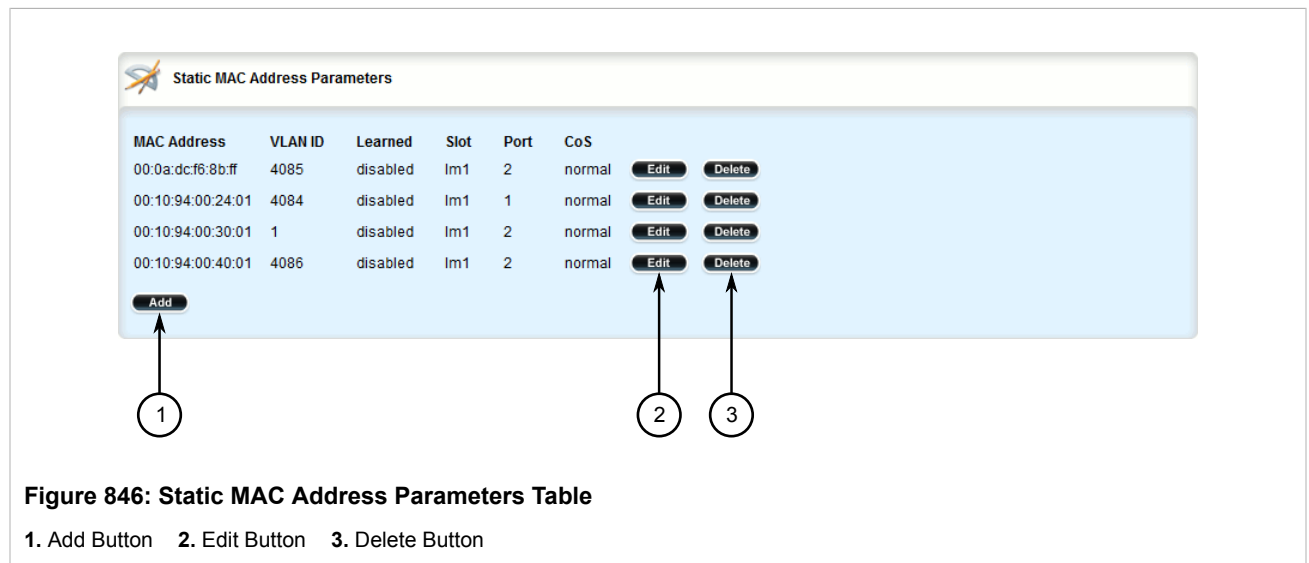
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.34.4.3

## Deleting a Static MAC Address

To delete a static MAC address, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » mac-tables » static-mac-table**. The **Static MAC Address Parameters** table appears.



- Click **Delete** next to the chosen static MAC address.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.35

## Managing Spanning Tree Protocol

The following sections describe how to configure and manage STP:

- [Section 5.35.1, “RSTP Operation”](#)
- [Section 5.35.2, “RSTP Applications”](#)
- [Section 5.35.3, “MSTP Operation”](#)
- [Section 5.35.4, “Configuring STP Globally”](#)
- [Section 5.35.5, “Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces”](#)
- [Section 5.35.6, “Managing Multiple Spanning Tree Instances Globally”](#)
- [Section 5.35.7, “Managing Multiple Spanning Tree Instances Per-Port”](#)

- [Section 5.35.8, “Viewing the Status of RSTP”](#)
- [Section 5.35.9, “Viewing RSTP Per-Port Statistics”](#)
- [Section 5.35.10, “Clearing Spanning Tree Protocol Statistics”](#)

#### Section 5.35.1

## 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.

The following sections further describe the operation of RSTP:

- [Section 5.35.1.1, “RSTP States and Roles”](#)
- [Section 5.35.1.2, “Edge Ports”](#)
- [Section 5.35.1.3, “Point-to-Point and Multipoint Links”](#)
- [Section 5.35.1.4, “Path and Port Costs”](#)
- [Section 5.35.1.5, “Bridge Diameter”](#)
- [Section 5.35.1.6, “eRSTP”](#)
- [Section 5.35.1.7, “Fast Root Failover”](#)

#### Section 5.35.1.1

### 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.

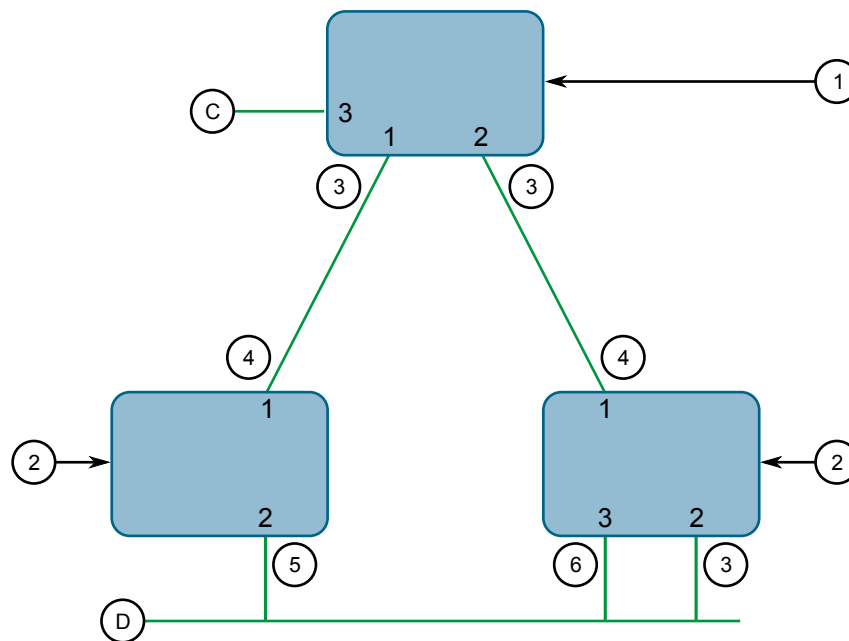
**IMPORTANT!**

*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 847: 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 5.35.1.2

## 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 5.35.1.3

## 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 5.35.1.4

## 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 5.35.1.5

## 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 5.35.1.6

## 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 5.35.1.7

### 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 5.35.2

## RSTP Applications

The following sections describe various applications of RSTP:

- [Section 5.35.2.1, “RSTP in Structured Wiring Configurations”](#)
- [Section 5.35.2.2, “RSTP in Ring Backbone Configurations”](#)
- [Section 5.35.2.3, “RSTP Port Redundancy”](#)

Section 5.35.2.1

### 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 848](#) would leave all the ports of bridges 555 through 888 connected to the network.

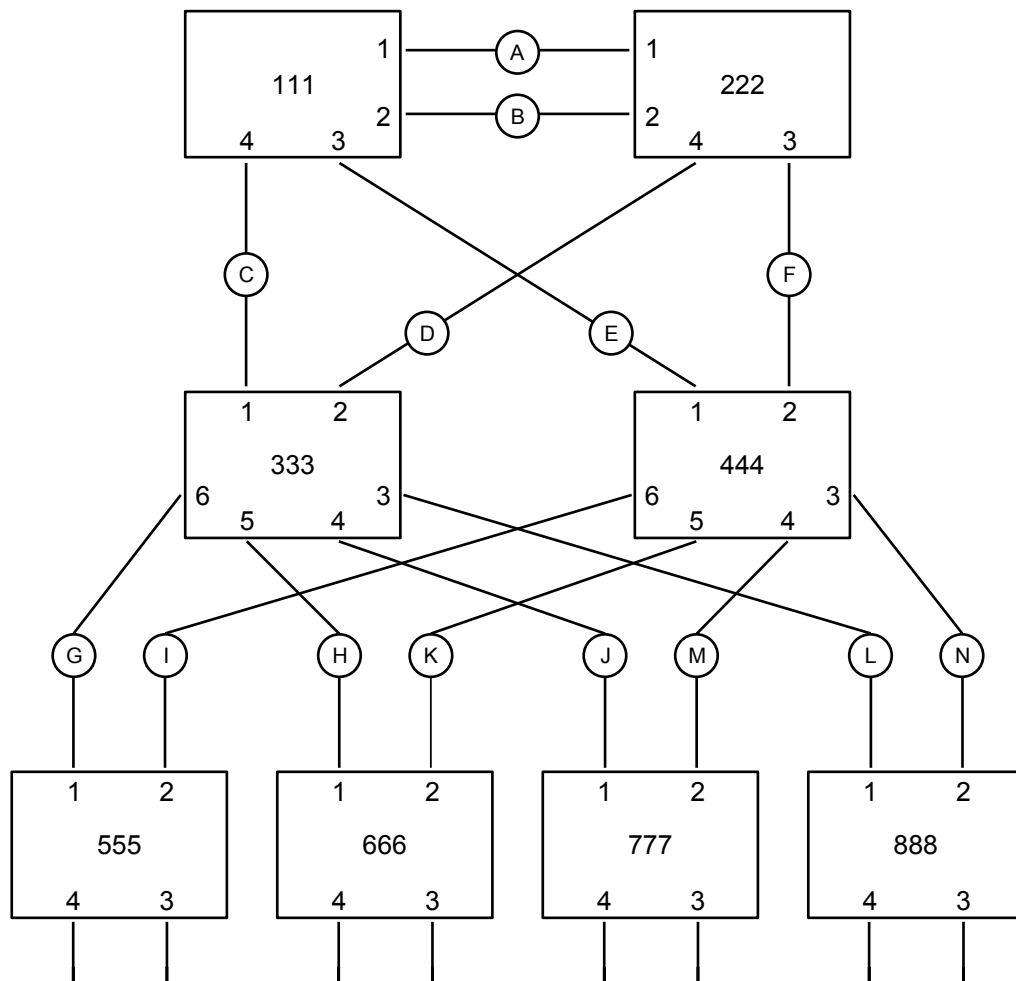


Figure 848: Example - Structured Wiring Configuration

To design a structured wiring configuration, do the following:

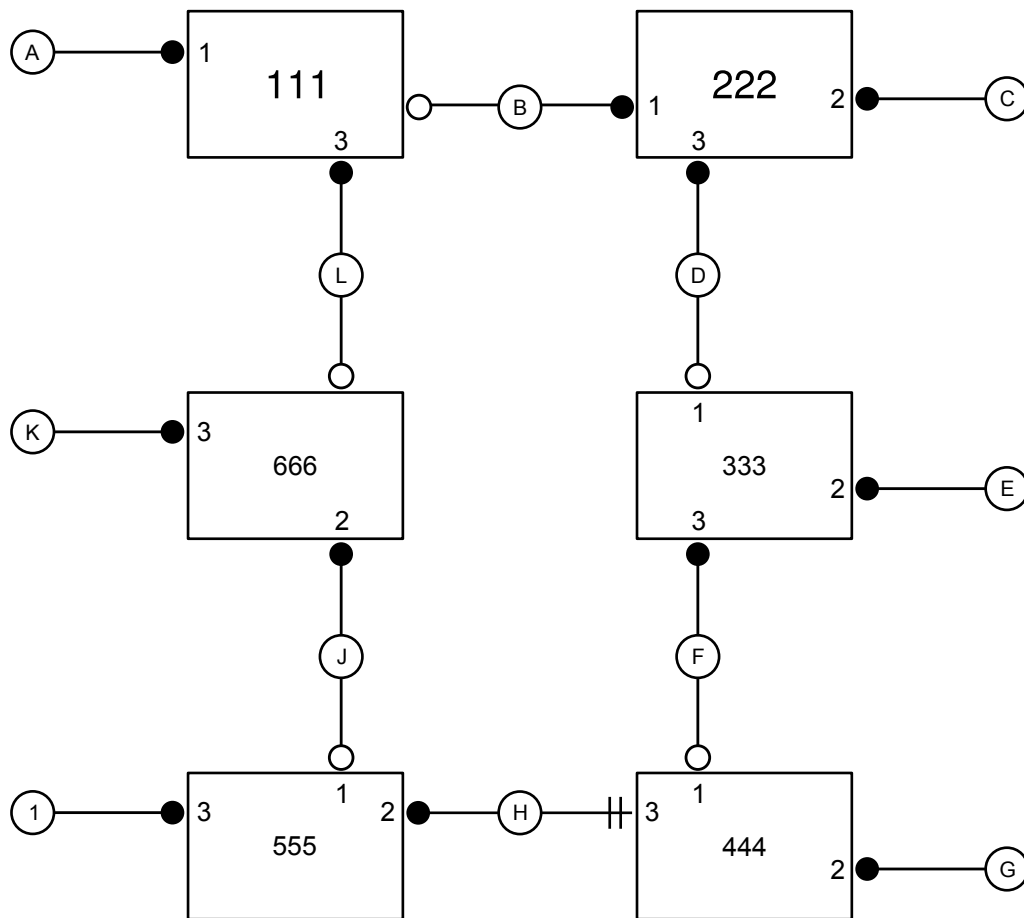
1. **Select the design parameters for the network.**  
What are the requirements for robustness and network failover/recovery times? Are there any special requirements for diverse routing to a central host computer? Are there any special port redundancy requirements?
2. **Identify required legacy support.**  
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 5.35.2.2

### 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 example, as indicated by the double bars through link H in [Figure 849](#). In the event of a failure on link D, bridge 444 will unblock link H. Bridge 333 will communicate with the network through link F.



**Figure 849: 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 [www.siemens.com/ruggedcom](http://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 5.35.2.3

## 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.

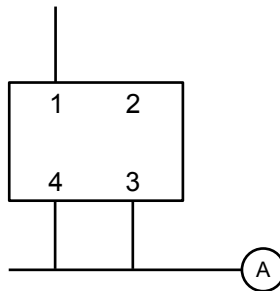


Figure 850: Example - Port Redundancy

### Section 5.35.3

## 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.

The following sections further describe the operation of MSTP:

- [Section 5.35.3.1, “MSTP Regions and Interoperability”](#)
- [Section 5.35.3.2, “MSTP Bridge and Port Roles”](#)
- [Section 5.35.3.3, “Benefits of MSTP”](#)
- [Section 5.35.3.4, “Implementing MSTP on a Bridged Network”](#)

#### Section 5.35.3.1

### MSTP Regions and Interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of inter-operating with bridges that support only RSTP or legacy STP, without requiring any special configuration.

An MST region may be defined as the set of interconnected bridges whose MST Region Identification is identical. The interface between MSTP bridges and non-MSTP bridges, or between MSTP bridges with different MST Region Identification information, becomes part of an MST Region boundary.

Bridges outside an MST region will see the entire region as though it were a single (R)STP bridge, with the internal detail of the MST region being hidden from the rest of the bridged network. In support of this, MSTP maintains separate *hop counters* for spanning tree information exchanged at the MST region boundary versus information propagated inside the region. For information received at the MST region boundary, the (R)STP Message Age is incremented only once. Inside the region, a separate Remaining Hop Count is maintained, one for each spanning tree instance. The external Message Age parameter is referred to the (R)STP Maximum Age Time, whereas the internal Remaining Hop Counts are compared to an MST region-wide Maximum Hops parameter.

#### » MSTI

An MSTI (Multiple Spanning Tree Instance) is one of sixteen independent spanning tree instances that may be defined in an MST region (not including the IST). An MSTI is created by mapping a set of VLANs to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN-to-MSTI mappings must be identical for all bridges in an MST region.

RUGGEDCOM ROX II supports 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of others. Data traffic originating from the same source and bound to the same destination, but on different VLANs on different MSTIs, may therefore travel a different path across the network.

#### » IST

An MST region always defines an IST (Internal Spanning Tree). The IST spans the entire MST region, and carries all data traffic that is not specifically allocated (by VLAN) to a specific MSTI. The IST is always computed and is defined to be MSTI zero.

The IST is also the extension inside the MST region of the CIST

#### » CST

The CST (Common Spanning Tree) spans the entire bridged network, including MST regions and any connected STP or RSTP bridges. An MST region is seen by the CST as an individual bridge, with a single cost associated with its traversal.



## » CIST

The CIST (Common and Internal Spanning Tree) is the union of the CST and the ISTs in all MST regions. The CIST therefore spans the entire bridged network, reaching into each MST region via the latter's IST to reach every bridge on the network.

### Section 5.35.3.2

## 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	<ul style="list-style-type: none"><li>• The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region.</li><li>• A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root.</li><li>• Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.</li></ul>
MSTI Port Roles	<p>For each MSTI on a bridge:</p> <ul style="list-style-type: none"><li>• The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root.</li><li>• A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root.</li><li>• Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root.</li></ul> <p>The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.</p>
Boundary Ports	<p>A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike.</p> <p>A Boundary Port may be:</p>

Role	Description
	<ul style="list-style-type: none"><li>• The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port).</li><li>• A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role.</li></ul> <p>A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.</p>

## Section 5.35.3.3

## 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 5.35.3.4

## 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 5.35.4, “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 5.35.6.3, “Adding a Multiple Spanning Tree Instance”](#).
3. Create static VLANs and map them to the MSTIs. For more information, refer to [Section 5.36.4.2, “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 5.35.7, “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 5.35.4, “Configuring STP Globally”](#)

Section 5.35.4

## Configuring STP Globally

To configure global settings for the Spanning Tree Protocol (STP), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » spanning-tree**. The **Spanning Tree**, **eRSTP** and **RSTP (Common) Instance** forms appear.

The image shows a 'Spanning Tree' configuration form with the following fields and callouts:

- 1** points to the **Enabled \*** checkbox, which is checked and labeled 'Enabled (true)'. A blue question mark icon is to its right.
- 2** points to the **STP Protocol Version \*** dropdown menu, which is set to 'rstp' and labeled '(rstp)'. A blue question mark icon is to its right.
- 3** points to the **Hello Time (sec) \*** input box, which contains the value '2' and is labeled '(2)'. A blue question mark icon is to its right.
- 4** points to the **Max Age (sec) \*** input box, which contains the value '20' and is labeled '(20)'. A blue question mark icon is to its right.
- 5** points to the **Transmission Hold Count \*** input box, which contains the value '0' and is labeled '(0)'. A blue question mark icon is to its right.
- 6** points to the **Forwarding Delay (sec) \*** input box, which contains the value '15' and is labeled '(15)'. A blue question mark icon is to its right.
- 7** points to the **Maximum Hops \*** input box, which contains the value '20' and is labeled '(20)'. A blue question mark icon is to its right.
- 8** points to the **MST Region Name** input box, which is empty and labeled '---'. A blue question mark icon is to its right.
- 9** points to the **MST Revision Level \*** input box, which contains the value '0' and is labeled '(0)'. A blue question mark icon is to its right.

**Figure 851: Spanning Tree Form**

1. Enabled Check Box   2. STP Protocol Version List   3. Hello Time Box   4. Max Age Box   5. Transmission Hold Count Box  
6. Forwarding Delay Box   7. Maximum Hops Box   8. MST Region Name Box   9. MST Revision Level Box

The image shows the 'eRSTP' configuration form. It contains several fields with numbered callouts: 1 points to the 'Max Network Diameter Multiplier' dropdown (value 4); 2 points to the 'BPDU Guard Mode' dropdown (value specify); 3 points to the 'BPDU Timeout' field (value ---); 4 points to the 'Fast Root Failover' dropdown (value on); 5 points to the 'IEEE802.1w Interoperability' checkbox (checked); 6 points to the 'Cost Style' dropdown (value stp). Each field has a help icon (question mark) to its right.

Figure 852: eRSTP Form

1. Max Network Diameter Multiplier List    2. BPDU Guard Mode List    3. Fast Root Failover List    4. IEEE802.1w Interoperability Check Box    5. Cost Style List

The image shows the 'RSTP (Common) Instance' configuration form. It contains one field with a numbered callout: 1 points to the 'Bridge Priority' dropdown (value 32768). A help icon (question mark) is to the right of the field.

Figure 853: RSTP (Common) Instance Form

1. Bridge Priority List

3. On the **Spanning Tree** form, configure the following parameters as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true

Parameter	Description
	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.
STP Protocol Version	<p><b>Synopsis:</b> { stp, rstp, mstp }</p> <p><b>Default:</b> rstp</p> <p>The version (either only STP or Rapid STP or Multiple STP) of the Spanning Tree Protocol (STP) to support.</p>
Hello Time (sec)	<p><b>Synopsis:</b> An integer between 1 and 10</p> <p><b>Default:</b> 2</p> <p>The time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic. (Relationship : <math>\text{maxAgeTime} \geq 2 * (\text{helloTime} + 1.0 \text{ seconds})</math>)</p>
Max Age (sec)	<p><b>Synopsis:</b> An integer between 6 and 40</p> <p><b>Default:</b> 20</p> <p>The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANS) are part of the network. (Relationship : <math>\text{maxAgeTime} \geq 2 * (\text{helloTime} + 1.0 \text{ seconds})</math>)</p>
Transmission Hold Count	<p><b>Synopsis:</b> An integer between 0 and 100</p> <p><b>Default:</b> 0</p> <p>The maximum number of configuration messages on each port that may be sent in a special event, such as recovering from a failure or bringing up a new link. After the maximum number of messages is reached, Rapid Spanning Tree Protocol (RSTP) will be limited to one message per second. Larger values allow the network to recover from failed links more quickly. If RSTP is being used in a ring architecture, the transmit count should be larger than the number of switches in the ring. If a number is not defined, the value is considered unlimited.</p>
Forwarding Delay (sec)	<p><b>Synopsis:</b> An integer between 4 and 30</p> <p><b>Default:</b> 15</p> <p>The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.</p>
Maximum Hops	<p><b>Synopsis:</b> An integer between 6 and 40</p> <p><b>Default:</b> 20</p> <p>The maximum possible bridge diameter inside a Multiple Spanning Tree (MST) region. MST BPDUs propagating inside an MST region carry a time-to-live parameter decremented 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.</p>
MST Region Name	<p><b>Synopsis:</b> A string 1 to 32 characters long</p> <p>The name of the MST region. All devices in the same MST region must have the same region name configured</p>
MST Revision Level	<p><b>Synopsis:</b> An integer between 0 and 65535</p> <p><b>Default:</b> 0</p> <p>The revision level for the MST configuration. Typically, all devices in the same MST region are configured with the same revision</p>

Parameter	Description
	level. However, different revision levels can be used to create sub-regions under the same region name.

4. On the **eRSTP** form, configure the following parameters as required:

Parameter	Description
Max Network Diameter Multiplier	<b>Synopsis:</b> { 1, 4 } <b>Default:</b> 4 The Max Network Diameter as a multiplier of the MaxAgeTime value.
BPDU Guard Mode	<b>Synopsis:</b> { specify, noshutdown, untilreset } <b>Default:</b> noshutdown The Rapid Spanning Tree Protocol (RSTP) standard does not address network security. RSTP must process every received Bridge Protocol Data Unit (BPDU) and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. BPDU Guard is a feature that protects the network from BPDUs received by a port where RSTP-capable devices are not expected to be attached. If a BPDU is received by a port for which the 'Edge' parameter is set to 'TRUE' or RSTP is disabled, the port will be shut down for the time period specified by this parameter. <itemizedlist><listitem>NO SHUTDOWN: BPDU Guard is disabled.</listitem> <listitem>UNTIL RESET: The port will remain shut down until the port reset command is issued by the user.</listitem> <listitem>SPECIFY: A timeout period is specified for the port using the BPDU Timeout parameter.</listitem></itemizedlist>
BPDU Timeout	<b>Synopsis:</b> An integer between 1 and 86400 The time for which a port is shutdown. Only applicable when BPDU Guard Mode is set to <emphasis>specify</emphasis>.
Fast Root Failover	<b>Synopsis:</b> { on, off, on-with-standard-root } <b>Default:</b> on The Fast Root Failover algorithm. Options include: <itemizedlist><listitem>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.</listitem> <listitem>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.</listitem> <listitem>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.</listitem></itemizedlist>
IEEE802.1w Interoperability	<b>Synopsis:</b> true or false <b>Default:</b> true Enables/disables IEEE 802.1w Interoperability
Cost Style	<b>Synopsis:</b> { stp, rstp } <b>Default:</b> stp The style of link costs to employ. STP uses 16-bit path costs based upon 1x10E9/link speed (4 for 1Gbps, 19 for 100 Mbps and 100 for 10 Mbps) whereas RSTP uses 32-bit costs based upon 2x10E13/link speed (20,000 for 1Gbps, 200,000 for 100 Mbps and 2,000,000 for 10 Mbps). Note that RSTP link costs are used only when the bridge version support is set to allow RSTP and the port does not migrate to the Spanning Tree Protocol (STP).

- On the **RSTP (Common) Instance** form, configure the following parameters as required:

Parameter	Description
Bridge Priority	<b>Synopsis:</b> { 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } <b>Default:</b> 32768 The priority assigned to the RSTP/Common Bridge Instance.

- If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to [Section 5.35.6.3, “Adding a Multiple Spanning Tree Instance”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.35.5

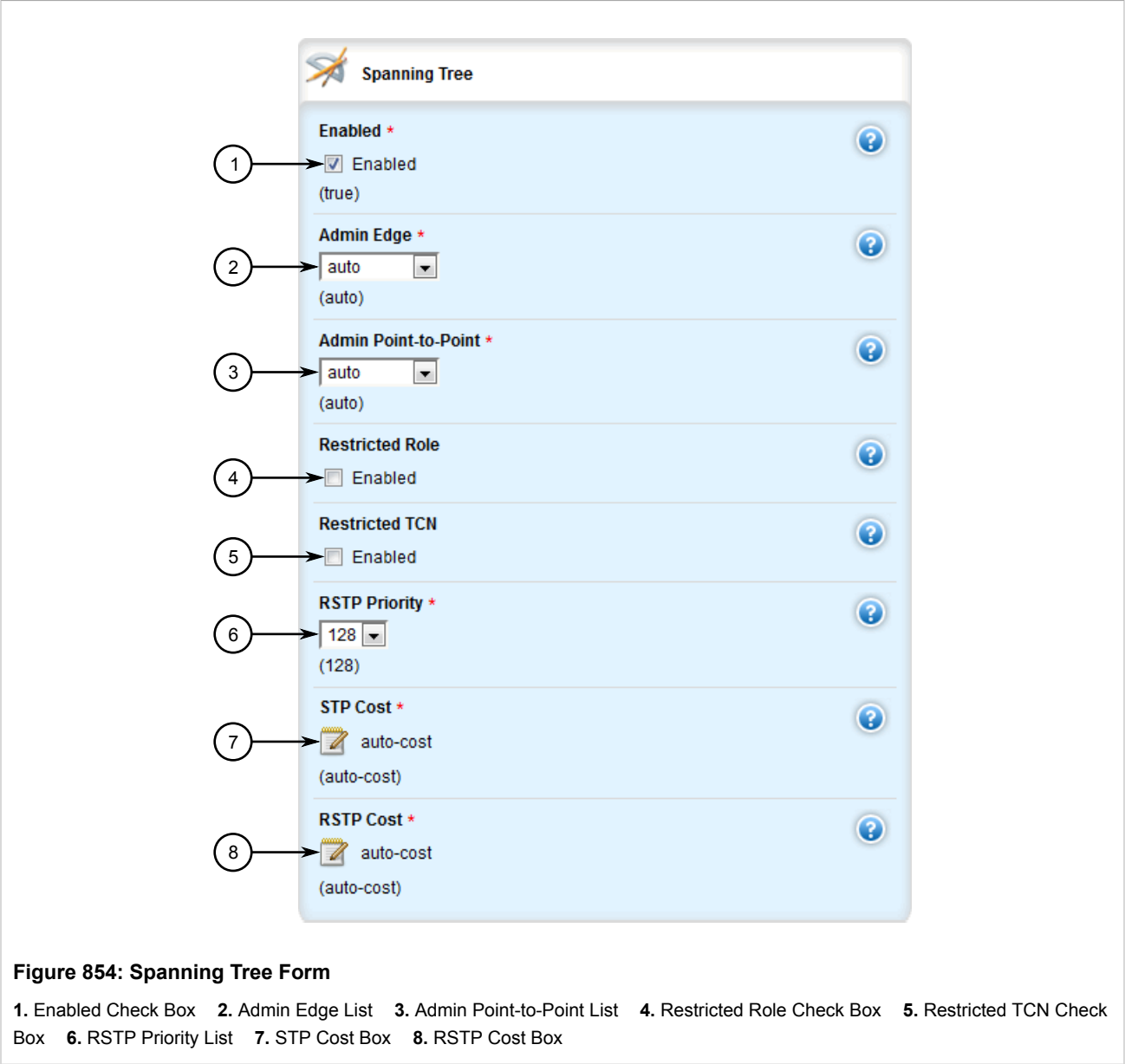
## Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces

To configure the Spanning Tree Protocol (STP) for a switched Ethernet port, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to:
  - **For switched Ethernet ports:**  
*interface » switch » {interface} » spanning-tree*, where *{interface}* is the name given to the switched Ethernet port.
  - **For Ethernet trunk interfaces:**  
*interface » trunks » {id} » spanning-tree*, where *{id}* is the ID given to the interface.

The **Spanning Tree** form appears.





3. Configure the following parameters as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables/disables STP/RSTP on the interface.
Admin Edge	<b>Synopsis:</b> { forceTrue, forceFalse, auto } <b>Default:</b> 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

Parameter	Description
	another port in the spanning tree will result in a detectable loop. The <b>Edgeness</b> of the port will be switched off and the standard RSTP rules will apply (until the next link outage).
Admin Point-to-Point	<p><b>Synopsis:</b> { forceTrue, forceFalse, auto }</p> <p><b>Default:</b> auto</p> <p>RSTP uses a peer-to-peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating in full-duplex mode. The point-to-point parameter allows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges).</p>
Restricted Role	<p><b>Synopsis:</b> typeless</p> <p>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.</p>
Restricted TCN	<p><b>Synopsis:</b> typeless</p> <p>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.</p>
RSTP Priority	<p><b>Synopsis:</b> { 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 }</p> <p><b>Default:</b> 128</p> <p>The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.</p>
STP Cost	<p><b>Synopsis:</b> { auto-cost } or an integer between 0 and 65535</p> <p><b>Default:</b> auto-cost</p> <p>The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP 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.</p>
RSTP Cost	<p><b>Synopsis:</b> { auto-cost } or an integer between 0 and 2147483647</p> <p><b>Default:</b> auto-cost</p> <p>The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP 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.</p>

4. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to [Section 5.35.6.3, “Adding a Multiple Spanning Tree Instance”](#).
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

#### Section 5.35.6

## 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 5.35.3, “MSTP Operation”](#).


The following sections describe how to configure and manage Multiple Spanning Tree Instances:

- [Section 5.35.6.1, “Viewing Statistics for Multiple Spanning Tree Instances”](#)
- [Section 5.35.6.2, “Viewing a List of Multiple Spanning Tree Instances”](#)
- [Section 5.35.6.3, “Adding a Multiple Spanning Tree Instance”](#)
- [Section 5.35.6.4, “Deleting a Multiple Spanning Tree Instance”](#)

#### Section 5.35.6.1

### Viewing Statistics for Multiple Spanning Tree Instances

To view statistics related to Multiple Spanning Tree Instances (MSTIs), navigate to **switch » spanning-tree » msti-status**. The **MSTI Status** table appears.



MSTI Status

MSTP Instance ID	Status	Root Priority	Root MAC	Bridge Priority	Bridge MAC	Root Port Slot	Root Port Port
1	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
2	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
3	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
4	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
5	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
6	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
7	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
8	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
9	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
10	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
11	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
12	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
13	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
14	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
15	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1
16	none	0	00:00:00:00:00:00	0	00:00:00:00:00:00	---	-1

**Figure 855: MSTI Status Table**

This table provides the following information:

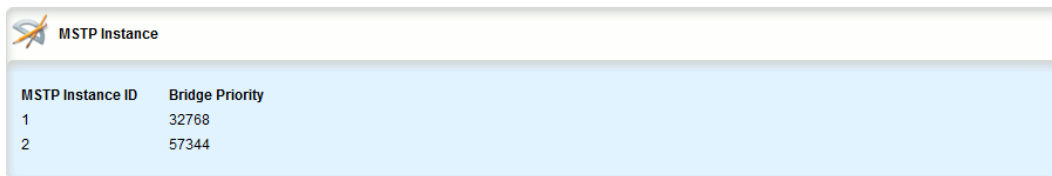
Parameter	Description
MSTP Instance ID	<b>Synopsis:</b> An integer between 1 and 16 The bridge identifier of this bridge.
status	<b>Synopsis:</b> { none, designatedBridge, notDesignatedForAnyLAN, rootBridge } The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports.
Root Priority	The bridge identifier of the root bridge.
Root MAC	<b>Synopsis:</b> A string The bridge identifier of the root bridge.
Bridge Priority	The bridge identifier of this bridge.
Bridge MAC	<b>Synopsis:</b> A string The bridge identifier of this bridge.
Root Port Slot	<b>Synopsis:</b> { ---, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, trnk } If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network.
Root Port Port	If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network.
Root Path Cost	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.

Parameter	Description
Total Topology Changes	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.

## Section 5.35.6.2

## Viewing a List of Multiple Spanning Tree Instances

To view a list of Multiple Spanning Tree Instances (MSTIs), navigate to **switch » spanning-tree » mstp-instance**. If MSTIs have been configured, the **MSTP Instance** table appears.



MSTP Instance	
MSTP Instance ID	Bridge Priority
1	32768
2	57344

Figure 856: MSTP Instance Table

If no MSTIs have been configured, add instances as needed. For more information, refer to [Section 5.35.6.3, “Adding a Multiple Spanning Tree Instance”](#).

## Section 5.35.6.3

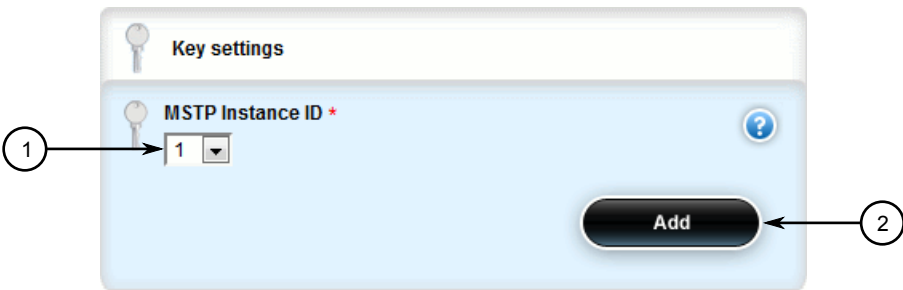
## Adding a Multiple Spanning Tree Instance

To add a Multiple Spanning Tree Instance (MSTI), do the following:

**NOTE**

*RUGGEDCOM ROX II supports up to 16 MSTIs.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » spanning-tree » mstp-instance** and click **<Add mstp-instance>** in the menu. The **Key Settings** form appears.



**Figure 857: Key Settings Form**

1. MSTP Instance ID List    2. Add Button

3. Configure the following parameter(s) as required:

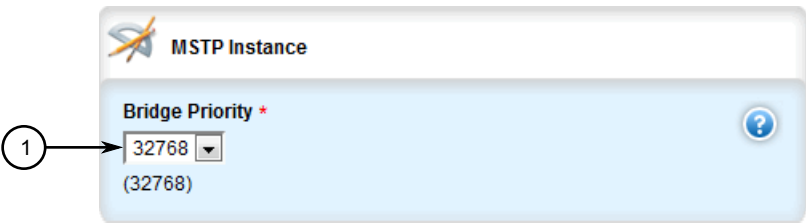
Parameter	Description
MSTP Instance ID	The Multiple Spanning Tree Protocol (MSTP) instance ID.

4. Click **Add** to create the instance. The **MSTP Instance** form appears.



**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.*



**Figure 858: MSTP Instance Form**

1. Bridge Priority List

5. Configure the following parameter(s) as required:

Parameter	Description
Bridge Priority	<p><b>Synopsis:</b> { 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 }</p> <p><b>Default:</b> 32768</p> <p>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</p>

Parameter	Description
	bridge is active. In this way, careful selection of bridge priorities can establish the path of traffic flows in normal and abnormal conditions.

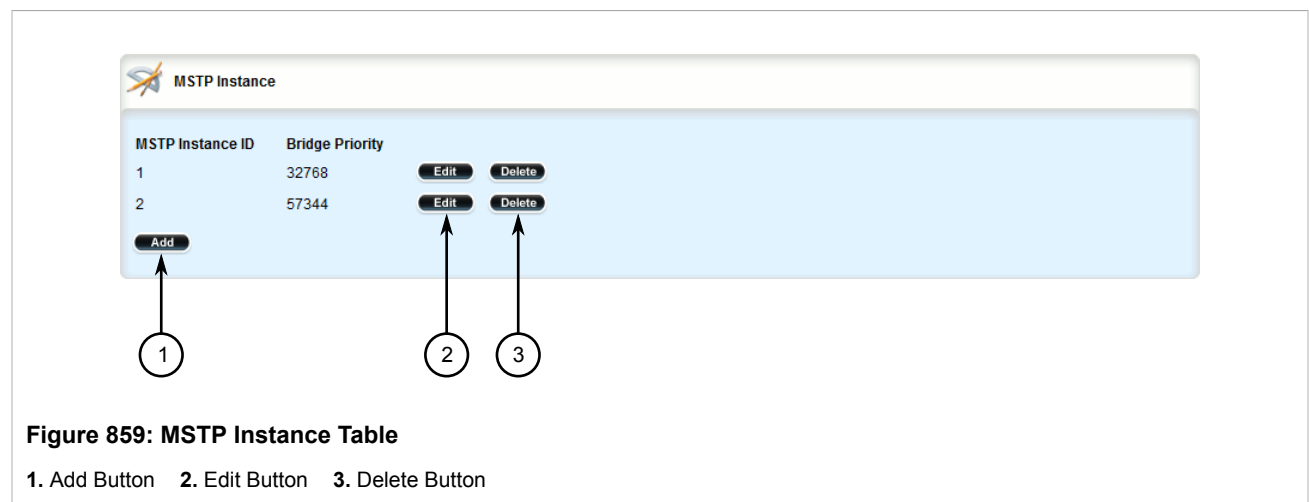
- Map one or more static VLANs and map them to the MSTI. For more information, refer to [Section 5.36.4.2, “Adding a Static VLAN”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.35.6.4

## Deleting a Multiple Spanning Tree Instance

To delete a Multiple Spanning Tree Instance (MSTI), do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **switch » spanning-tree » mstp-instance**. The **MSTP Instance** table appears.



- Click **Delete** next to the chosen instance.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.35.7

## Managing Multiple Spanning Tree Instances Per-Port

The following sections describe how to configure and manage Multiple Spanning Tree Instances (MSTIs) for individual switched Ethernet ports or Ethernet trunk interfaces:

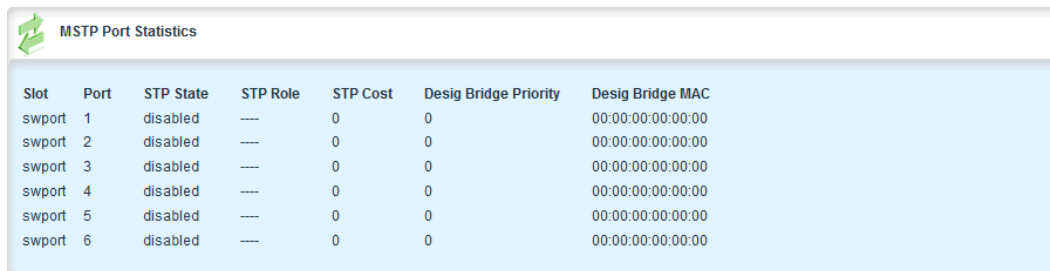
- [Section 5.35.7.1, “Viewing Per-Port Multiple Spanning Tree Instance Statistics”](#)
- [Section 5.35.7.2, “Viewing a List of Per-Port Multiple Spanning Tree Instances”](#)

- [Section 5.35.7.3, “Adding a Port-Specific Multiple Spanning Tree Instance”](#)
- [Section 5.35.7.4, “Deleting a Port-Specific Multiple Spanning Tree Instances”](#)

## Section 5.35.7.1

## Viewing Per-Port Multiple Spanning Tree Instance Statistics

To view Multiple Spanning Tree Instance (MSTI) statistics for individual switched Ethernet ports and/or Ethernet trunk interfaces, navigate to **switch » spanning-tree » port-msti-id » {id} » port-msti-stats**, where {id} is the ID for the MSTI. The **MSTP Port Statistics** table appears.:



The screenshot shows a web interface window titled "MSTP Port Statistics" with a green icon. It contains a table with the following data:

Slot	Port	STP State	STP Role	STP Cost	Desig Bridge Priority	Desig Bridge MAC
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

Figure 860: MSTP Port Statistics Table

This table provides the following information:

Parameter	Description
Slot	<b>Synopsis:</b> { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, trnk } The slot of the module that contains this port.
Port	<b>Synopsis:</b> An integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
STP State	<b>Synopsis:</b> { disabled, blocking, listening, learning, forwarding, linkDown, discarding } The status of this interface in the spanning tree: <ul style="list-style-type: none"><li>Disabled: The Spanning Tree Protocol (STP) is disabled on this port.</li><li>Link Down: STP is enabled on this port but the link is down.</li><li>Discarding: The link is not used in the STP topology but is standing by.</li><li>Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic.</li><li>Forwarding: The port is forwarding traffic.</li></ul>
STP Role	<b>Synopsis:</b> { ---, root, designated, alternate, backup, master } The role of this port in the spanning tree: <ul style="list-style-type: none"><li>Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to.</li><li>Root: The single port on the bridge, which provides connectivity towards the root bridge.</li><li>Backup: The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by.</li><li>Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by.</li><li>Master: Only exists in Multiple Spanning Tree Protocol (MSTP). The port is a Multiple Spanning Tree (MST) region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree (CST) root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).</li></ul>
STP Cost	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



Parameter	Description
	(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.
Desig Bridge Priority	The bridge identifier of this bridge.
Desig Bridge MAC	<b>Synopsis:</b> A string The bridge identifier of this bridge.

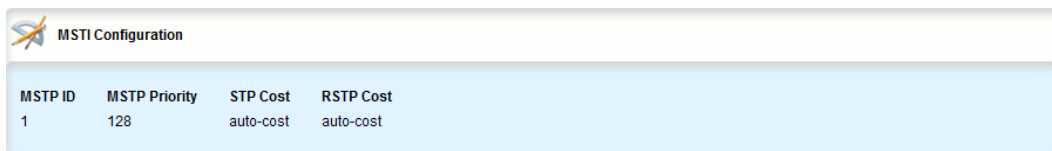
## Section 5.35.7.2

## Viewing a List of Per-Port Multiple Spanning Tree Instances

To view a list of the Multiple Spanning Tree Instances (MSTIs) for switched Ethernet ports or Ethernet trunk interfaces, navigate to:

- **For switched Ethernet ports:**  
*interface » switch » {interface} » spanning-tree » msti*, where {interface} is the switched Ethernet port.
- **For Ethernet trunk interfaces:**  
*interface » trunks » {id} » spanning-tree » msti*, where {id} is the ID given to the interface.

The **MSTI Configuration** table appears.



MSTP ID	MSTP Priority	STP Cost	RSTP Cost
1	128	auto-cost	auto-cost

**Figure 861: MSTI Configuration Table**

If no MSTIs have been configured, add them as needed. For more information, refer to [Section 5.35.7.3, “Adding a Port-Specific Multiple Spanning Tree Instance”](#).

## Section 5.35.7.3

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
  - **For switched Ethernet ports:**  
*interface » switch » {interface} » spanning-tree » msti*, where {interface} is the switched Ethernet port.
  - **For Ethernet trunk interfaces:**  
*interface » trunks » {id} » spanning-tree » msti*, where {id} is the ID given to the interface.

- Click **<Add msti>** in the menu. The **Key Settings** form appears.

**Figure 862: Key Settings Form**

1. MSTP ID List    2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
MSTP ID	MSTP Instance Identifier

- Click **Add** to create the instance. The **MSTI Configuration** form appears.

**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.*

**Figure 863: MSTI Configuration Form**

1. MSTP Priority List    2. STP Cost List    3. RSTP Cost List

- Configure the following parameter(s) as required:

Parameter	Description
MSTP Priority	<b>Synopsis:</b> { 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } <b>Default:</b> 128  The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
STP Cost	<b>Synopsis:</b> { auto-cost } or an integer between 0 and 65535 <b>Default:</b> auto-cost  The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP 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	<b>Synopsis:</b> { auto-cost } or an integer between 0 and 2147483647 <b>Default:</b> auto-cost  The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP 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.

7. Map one or more static VLANs and map them to the MSTI. For more information, refer to [Section 5.36.4.2, "Adding a Static VLAN"](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

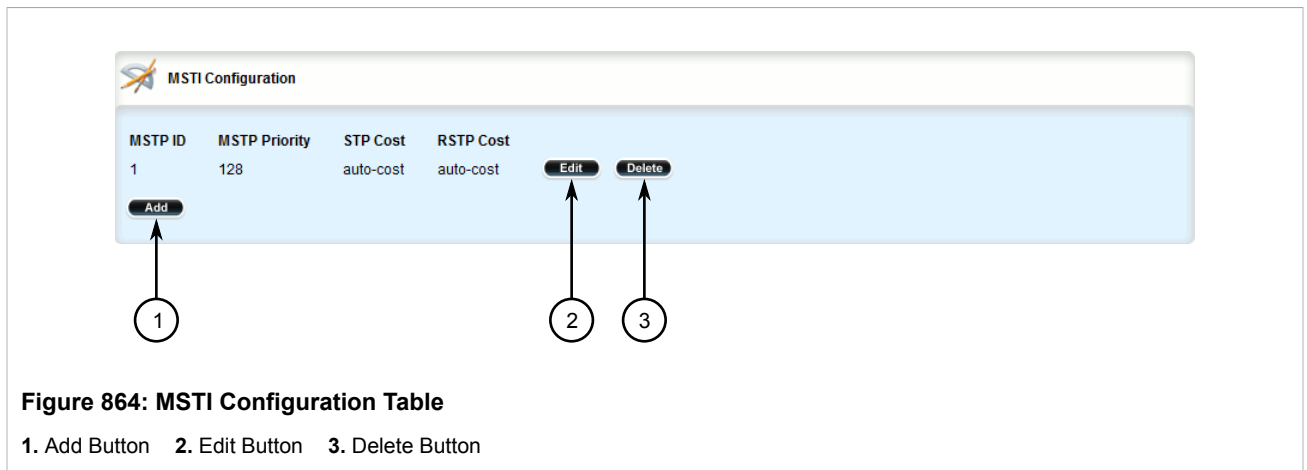
## Section 5.35.7.4

## 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
  - **For switched Ethernet ports:**  
*interface » switch » {interface} » spanning-tree » msti*, where *{interface}* is the switched Ethernet port.
  - **For Ethernet trunk interfaces:**  
*interface » trunks » {id} » spanning-tree » msti*, where *{id}* is the ID given to the interface.

The **MSTI Configuration** table appears.




3. Click **Delete** next to the chosen instance.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.35.8

## Viewing the Status of RSTP

To view the status of the RSTP network, navigate to **switch » spanning-tree**. The **RSTP Status** form appears.

 **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	1m1	?
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 Topology Changes	5	 ?

Figure 865: RSTP Status Form

This form provides the following information:

Parameter	Description
Status	<b>Synopsis:</b> { none, designatedBridge, notDesignatedForAnyLAN, rootBridge }  The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports.
Bridge Priority	The bridge identifier of this bridge.
Bridge MAC	<b>Synopsis:</b> A string The bridge identifier of this bridge.

Parameter	Description
Root Priority	The ports to which the multicast group traffic is forwarded.
Root MAC	<b>Synopsis:</b> A string The ports to which the multicast group traffic is forwarded.
Regional Root Priority	The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to.
Regional Root MAC	<b>Synopsis:</b> A string The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to.
Root Port Slot	<b>Synopsis:</b> { ---, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, trnk } If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network.
Root Port Port	If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network.
Root Path Cost	The total cost of the path to the root bridge, composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge.
Regional Root Path Cost	For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is the cost of the path to the Internal Spanning Tree (IST) root (i.e. regional root) bridge
Configured Hello Time	The configured hello time from the Bridge RSTP Parameters menu.
Learned Hello Time	The actual hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Forward Delay	The configured forward delay time from the Bridge RSTP Parameters menu.
Learned Forward Delay	The actual forward delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Max Age	The configured maximum age time from the Bridge RSTP Parameters menu.
Learned Max Age	The actual maximum age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Total Topology Changes	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.

## Section 5.35.9

## Viewing RSTP Per-Port Statistics

To view Rapid Spanning Tree Protocol (RSTP) statistics for each port, navigate to **switch » spanning-tree » port-rstp-stats**. The **RSTP Port Statistics** form appears.

Slot	Port	STP State	STP Role	STP Cost	Desig Bridge Priority	Desig Bridge MAC	Oper Edge
lm1	1	forwarding	root	19	32768	00:0a:dc:78:fc:40	false
lm1	2	linkDown	---	0	0	00:00:00:00:00:00	false

**Figure 866: RSTP Port Statistics Form**

1. Slot 2. Port 3. STP State 4. STP Role 5. STP Cost 6. Desig Bridge Priority 7. Desig Bridge MAC 8. Oper Edge

This table provides the following information:

Parameter	Description
Slot	<b>Synopsis:</b> { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, trnk } The slot of the module that contains this port.
Port	<b>Synopsis:</b> An integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
STP State	<b>Synopsis:</b> { disabled, blocking, listening, learning, forwarding, linkDown, discarding } Describes the status of this interface in the spanning tree: <itemizedlist><listitem>Disabled: Spanning Tree Protocol (STP) is disabled on this port.</listitem> <listitem>Link Down: STP is enabled on this port but the link is down.</listitem> <listitem>Discarding: The link is not used in the STP topology but is standing by.</listitem> <listitem>Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic.</listitem> <listitem>Forwarding : The port is forwarding traffic.</listitem></itemizedlist>
STP Role	<b>Synopsis:</b> { ---, root, designated, alternate, backup, master } The role of this port in the spanning tree: <itemizedlist><listitem>Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to.</listitem> <listitem>Root: The single port on the bridge, which provides connectivity towards the root bridge.</listitem> <listitem>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.</listitem> <listitem>Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by.</listitem> <listitem>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).</listitem></itemizedlist>
STP Cost	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.
Desig Bridge Priority	<b>Synopsis:</b> An integer between 0 and 65535

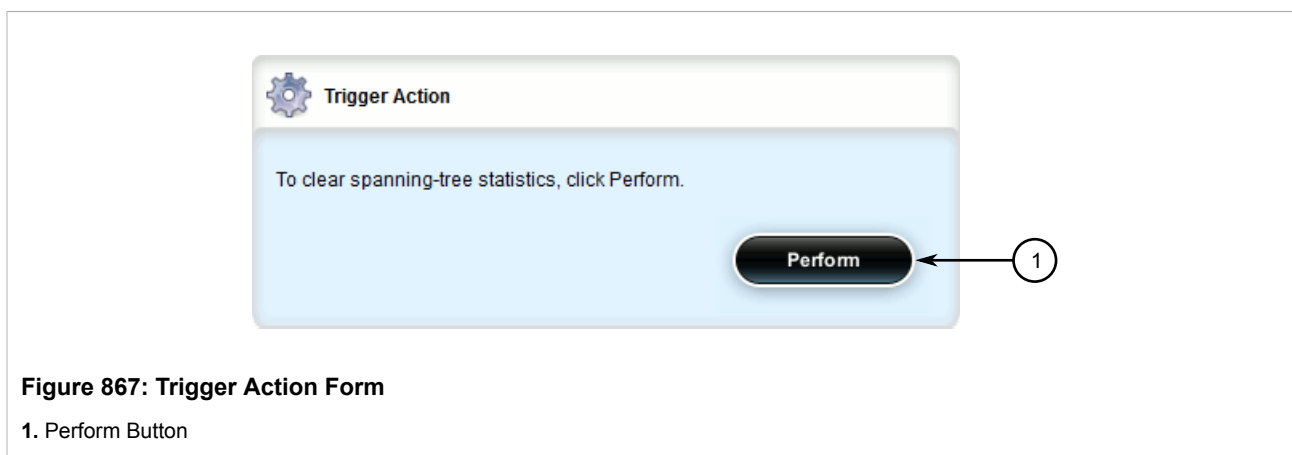
Parameter	Description
	Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.
Desig Bridge MAC	<b>Synopsis:</b> A string Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.
Oper Edge	<b>Synopsis:</b> true or false Whether or not the port is operating as an edge port.
RX RSTs	The number of Rapid Spanning Tree Protocol (RSTP) configuration messages received on this port.
TX RSTs	The number of Rapid Spanning Tree Protocol (RSTP) configuration messages transmitted on this port.
RX Confgs	The number of Spanning Tree Protocol (STP) configuration messages received on this port.
TX Confgs	The number of Spanning Tree Protocol (STP) configuration messages transmitted on this port.
RX TCNs	The number of configuration change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems.
TX TCNs	The number of configuration messages transmitted from this port.

#### Section 5.35.10

## Clearing Spanning Tree Protocol Statistics

To clear all Spanning Tree Protocol statistics, do the following:

1. Navigate to **switch » spanning-tree** and click **clear-stp-stats** in the menu. The **Trigger Action** form appears.



2. Click **Perform**.



Section 5.36

## 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 5.36.4, “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 5.36.1.7, “GARP VLAN Registration Protocol \(GVRP\)”](#)

The following sections describe how to configure and manage VLANs:

- [Section 5.36.1, “VLAN Concepts”](#)
- [Section 5.36.2, “Configuring the Internal VLAN Range”](#)
- [Section 5.36.3, “Managing VLANs for Switched Ethernet Ports”](#)
- [Section 5.36.4, “Managing Static VLANs”](#)
- [Section 5.36.5, “Managing Forbidden Ports”](#)
- [Section 5.36.6, “Managing VLANs for Virtual Switches”](#)
- [Section 5.36.7, “Managing VLANs for Routable-Only Ethernet Ports”](#)

Section 5.36.1

### VLAN Concepts

The following sections describe some of the concepts important to the implementation of VLANs in RUGGEDCOM ROX II:

- [Section 5.36.1.1, “Tagged vs. Untagged Frames”](#)
- [Section 5.36.1.2, “Native VLAN”](#)
- [Section 5.36.1.3, “Edge and Trunk Port Types”](#)
- [Section 5.36.1.4, “Ingress and Egress Rules”](#)
- [Section 5.36.1.5, “Forbidden Ports List”](#)
- [Section 5.36.1.6, “VLAN-Aware Mode of Operation”](#)
- [Section 5.36.1.7, “GARP VLAN Registration Protocol \(GVRP\)”](#)
- [Section 5.36.1.8, “PVLAN Edge”](#)
- [Section 5.36.1.9, “VLAN Advantages”](#)

## Section 5.36.1.1

## 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 5.36.1.2

## 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 5.36.1.3

## 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 VLANs. 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 5.36.1.5, "Forbidden Ports List"](#).*

Port Type	VLANs Supported	PVID Format	Usage
Edge	1 (Native) Configured	Untagged	<i>VLAN Unaware Networks:</i> All frames are sent and received without the need for VLAN tags.
		Tagged	<i>VLAN Aware Networks:</i> VLAN traffic domains are enforced on a single VLAN.
Trunk	All Configured	Tagged or Untagged	<i>switch-to-Switch Connections:</i> VLANs must be manually created and administered, or can be dynamically learned through GVRP. <i>Multiple-VLAN End Devices:</i> Implement connections to end devices that support multiple VLANs at the same time.

## Section 5.36.1.4

## Ingress and Egress Rules

Ingress and egress rules determine how traffic is received and transmitted by the switch.

Ingress rules are applied as follows to all frame when they are received by the switch:

Frame Received <sup>b</sup>	Untagged	Priority Tagged (VID = 0)	Tagged (Valid VID)
VLAN ID associated with the frame	PVID	PVID	VID in the Tag
Frame dropped due to its tagged/untagged format	No	No	No
Frame dropped if the frame associated with the VLAN is not configured (or learned) in the switch			Yes
Frame dropped if the ingress port is not a member of the VLAN the frame is associated with			No

<sup>b</sup> Does not depend on the ingress port's VLAN configuration parameters.

Egress rules are applied as follows to all frames when they are transmitted by the switch.

Egress Port Type	On Egress Port's Native VLAN	On Other VLAN	
		Port Is a Member Of the VLAN	Port Is Not a Member Of the VLAN
Edge	According to the egress port's PVID Format parameter	Dropped	
Trunk		Tagged	Dropped

## Section 5.36.1.5

## 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 5.36.5, "Managing Forbidden Ports"](#).

## Section 5.36.1.6

## 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 5.36.1.7

## GARP VLAN Registration Protocol (GVRP)

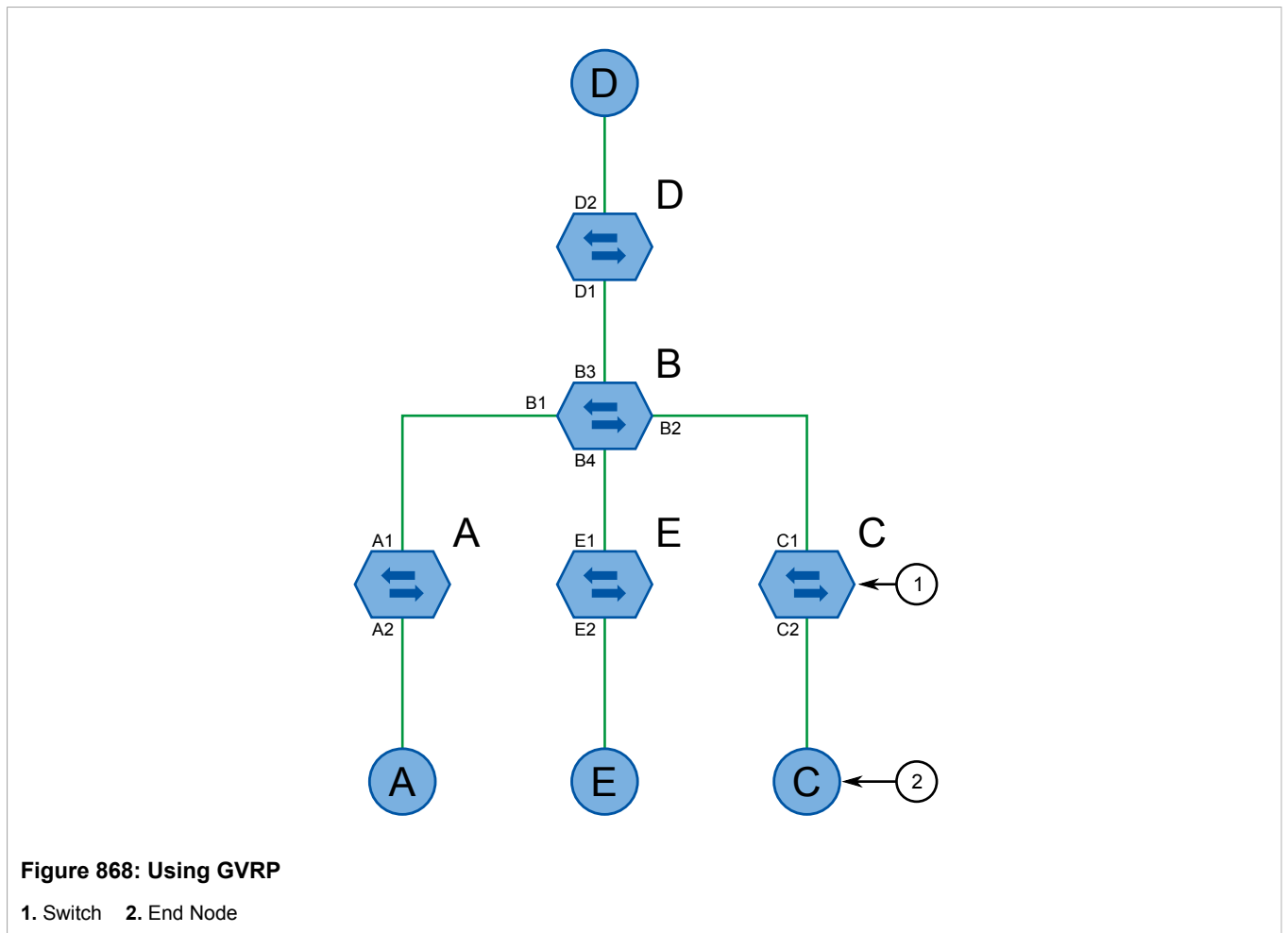
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere 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:



- 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 5.36.1.8

## PVLAN Edge

Protected VLAN (PVLAN) Edge refers to a feature of the switch that isolates multiple VLAN Edge ports from each other on a single device. All VLAN Edge ports in a switch that are configured as *protected* in this way are prohibited from sending frames to one another, but are still permitted to send frames to other, non-protected ports within the same VLAN. This protection extends to all traffic on the VLAN, including unicast, multicast and broadcast traffic.

**NOTE**

*This feature is strictly local to the switch. PVLAN Edge ports are not prevented from communicating with ports outside of the switch, whether protected (remotely) or not.*

Ports belonging to a specific PVID and a VLAN type of PVLAN Edge are part of one PVLAN Edge group. A PVLAN Edge group should include a minimum of two ports. There can be multiple PVLAN Edge groups on a switch.

It is not possible to combine a Gbit port with a 10/100 Mbit port as part of the same PVLAN Edge group.

Possible combinations of a PVLAN Edge group are listed below:

- A PVLAN Edge group with 10/100 Mbit ports from any line modules, with the exception of 2-port 100Base-FX line modules
- A PVLAN Edge group with Gbit ports from any line modules
- A PVLAN Edge group with 10/10 Mbit ports from 2-port 100Base-FX and Gbit ports from any line modules

## Section 5.36.1.9

## VLAN Advantages

The following are a few of the advantages offered by VLANs.

## » Traffic Domain Isolation

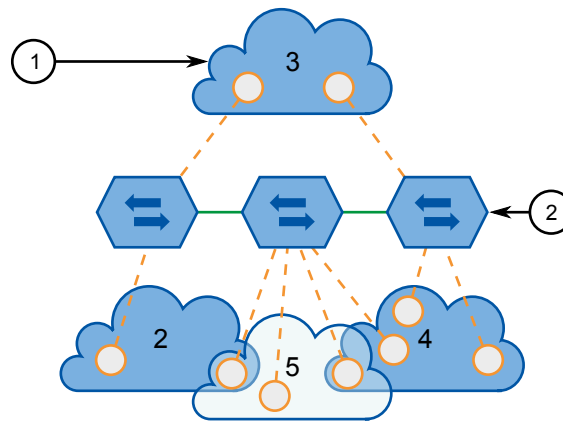
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

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 869: Multiple Overlapping VLANs**

1. VLAN 2. Switch

## » Administrative Convenience

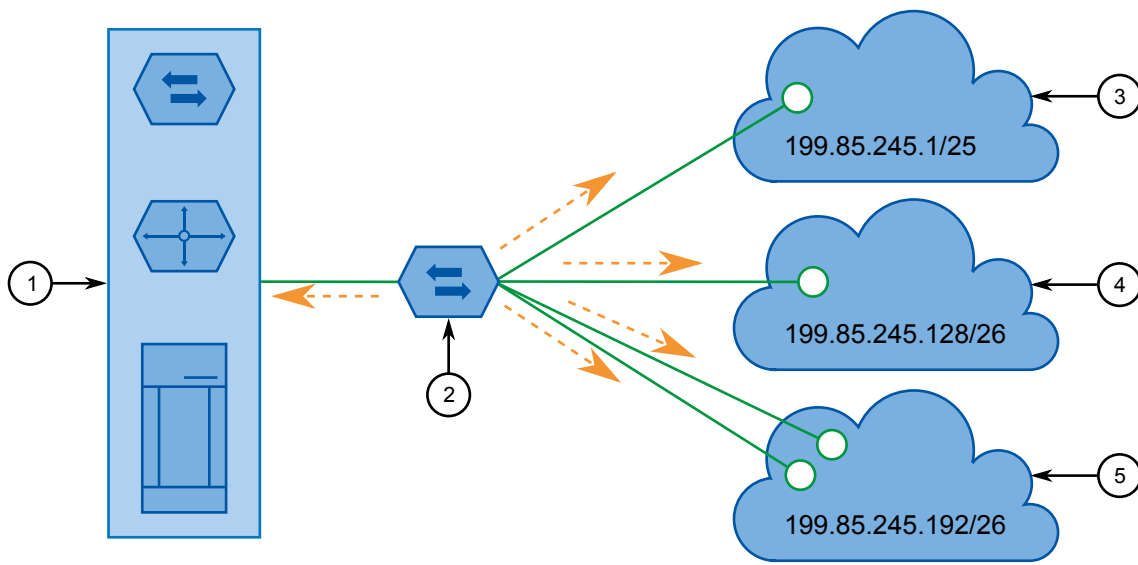
VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

## » 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 870: Inter-VLAN Communications**

1. Server, Router or Layer 3 Switch   2. Switch   3. VLAN 2   4. VLAN 3   5. VLAN 4

## Section 5.36.2

# 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 **End of Range** value repositions the matching serial VLAN. However, the matching serial VLAN is not affected when the **Start of Range** value is changed.*



### NOTE

*If no internal VLANs are available when a switched Ethernet or trunk port is configured, the range is automatically extended so a unique value can be assigned.*



### NOTE

*Routable Ethernet ports and trunks cannot be configured if internal VLANs are not enabled.*

To configure the internal VLAN range, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin » switch-config**. The **Internal VLAN Range** form appears.

**Internal VLAN Range**

1 → **Enabled \*** ☒ Enabled (false) ?

2 → **Start of Range \***  4094 (4094) ?

3 → **End of Range \***  4094 (4094) ?

**Figure 871: Internal VLAN Range Form**

1. Enabled Check Box   2. Start of Range Box   3. End of Range Box

3. Configure the following parameters:

Parameter	Description
enabled	<b>Synopsis:</b> true or false <b>Default:</b> false Enables/disables the Internal VLAN Range settings.
Start of Range	<b>Synopsis:</b> An integer between 2 and 4094 <b>Default:</b> 4094 <b>Prerequisite:</b> range-start must be less than or equal to range-end Defines the lower end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.
End of Range	<b>Synopsis:</b> An integer between 2 and 4094 <b>Default:</b> 4094 <b>Prerequisite:</b> range-end must be greater than or equal to range-start Defines the higher end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.36.3

# Managing VLANs for Switched Ethernet Ports

The following sections describe how to configure and manage VLANs specifically for switched Ethernet ports:

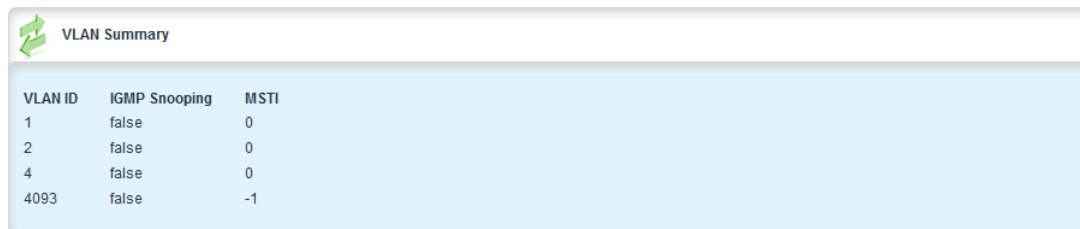


- [Section 5.36.3.1, “Viewing VLAN Assignments for Switched Ethernet Ports”](#)
- [Section 5.36.3.2, “Configuring VLANs for Switch Ethernet Ports”](#)

## Section 5.36.3.1

## Viewing VLAN Assignments for Switched Ethernet Ports

To determine which VLANs are assigned to each switched Ethernet port, navigate to **switch » vlans » vlan-summary**. The **VLAN Summary** table appears.



VLAN ID	IGMP Snooping	MSTI
1	false	0
2	false	0
4	false	0
4093	false	-1

**Figure 872: VLAN Summary Table**

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 3.18.2, “Configuring a Switched Ethernet Port”](#).

## Section 5.36.3.2

## Configuring VLANs for Switch 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » vlans » all-vlans » {id}**, where *{id}* is the ID of the VLAN. The **All VLANs Properties** form appears.

**Figure 873: All VLANs Properties Form**

1. IP Address Source List    2. ProxyARP Check Box    3. On-Demand Check Box

- Configure the following parameter(s) as required:

Parameter	Description
IP Address Source	<b>Synopsis:</b> { 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.
ProxyARP	<b>Synopsis:</b> typeless Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself.
on-demand	<b>Synopsis:</b> typeless Brings up this interface on demand only.
mtu	<b>Synopsis:</b> An integer between 68 and 1500 <b>Default:</b> 1500 The maximum transmission unit (the largest packet size allowed for this interface).

- Add Quality of Service (QoS) maps to the VLAN. For more information, refer to [Section 5.38.7.2, “Adding a QoS Map”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.36.4

## Managing Static VLANs

The following sections describe how to configure and manage static VLANs:

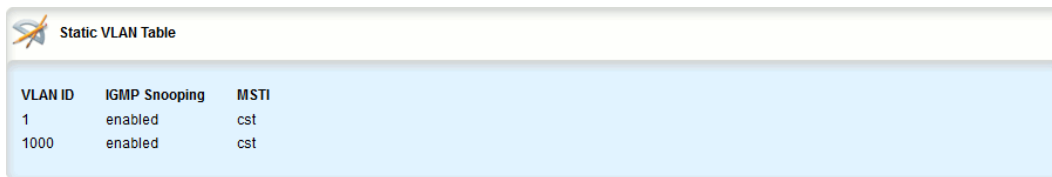
- [Section 5.36.4.1, “Viewing a List of Static VLANs”](#)

- [Section 5.36.4.2, “Adding a Static VLAN”](#)
- [Section 5.36.4.3, “Deleting a Static VLAN”](#)

#### Section 5.36.4.1

### Viewing a List of Static VLANs

To view a list of static VLANs, navigate to **switch » vlans » static-vlan**. If static VLANs have been configured, the **Static VLANs** table appears.



VLAN ID	IGMP Snooping	MSTI
1	enabled	cst
1000	enabled	cst

**Figure 874: Static VLANs Table**

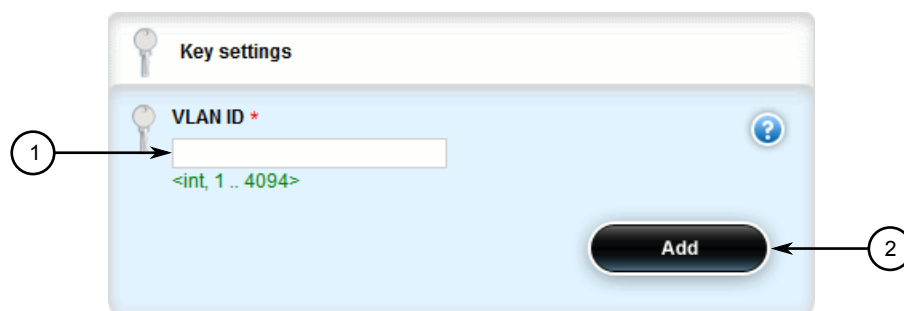
If no static VLANs have been configured, add static VLANs as needed. For more information, refer to [Section 5.36.4.2, “Adding a Static VLAN”](#).

#### Section 5.36.4.2

### Adding a Static VLAN

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » vlans » static-vlan** and click **<Add static-vlan>**. The **Key Settings** form appears.



The screenshot shows the 'Key settings' form for adding a static VLAN. It features a 'VLAN ID \*' input field with a range hint '<int, 1 ... 4094>' below it. A circled '1' points to this input field. To the right of the input field is a blue question mark icon. At the bottom right of the form is a black 'Add' button, which is pointed to by a circled '2'.

**Figure 875: Key Settings Form**

1. VLAN ID Box    2. Add Button

3. Configure the following parameter(s) as required:

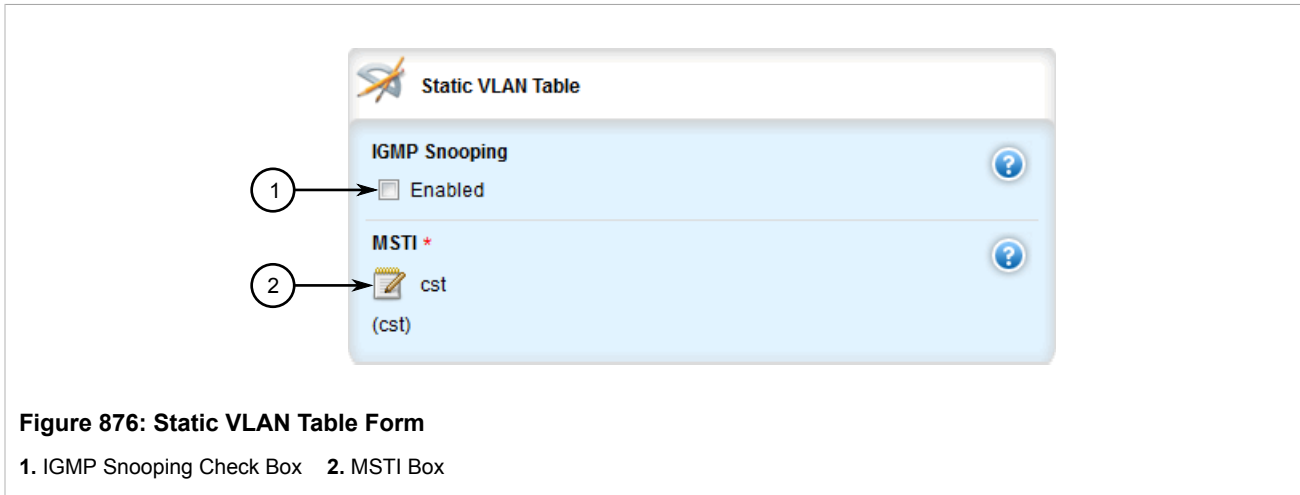


#### NOTE

The VLAN ID must be outside the internal VLAN range. For more information about configuring the internal VLAN range, refer to [Section 5.36.2, “Configuring the Internal VLAN Range”](#).

Parameter	Description
VLAN ID	<b>Synopsis:</b> An integer between 1 and 4094 <int, 1 \\. 15>;The VLAN identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.

4. Click **Add** to create the new static VLAN. The **Static VLAN Table** form appears.



5. Configure the following parameter(s) as required:



**NOTE**

*If **IGMP Snooping** is not enabled for the VLAN, both IGMP messages and multicast streams will be forwarded directly to all members of the VLAN. If any one member of the VLAN joins a multicast group, then all members of the VLAN will receive the multicast traffic.*

Parameter	Description
IGMP Snooping	<b>Synopsis:</b> typeless Enables or disables IGMP Snooping on the VLAN.
MSTI	<b>Synopsis:</b> { cst } or an integer between 1 and 16 <b>Default:</b> 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.

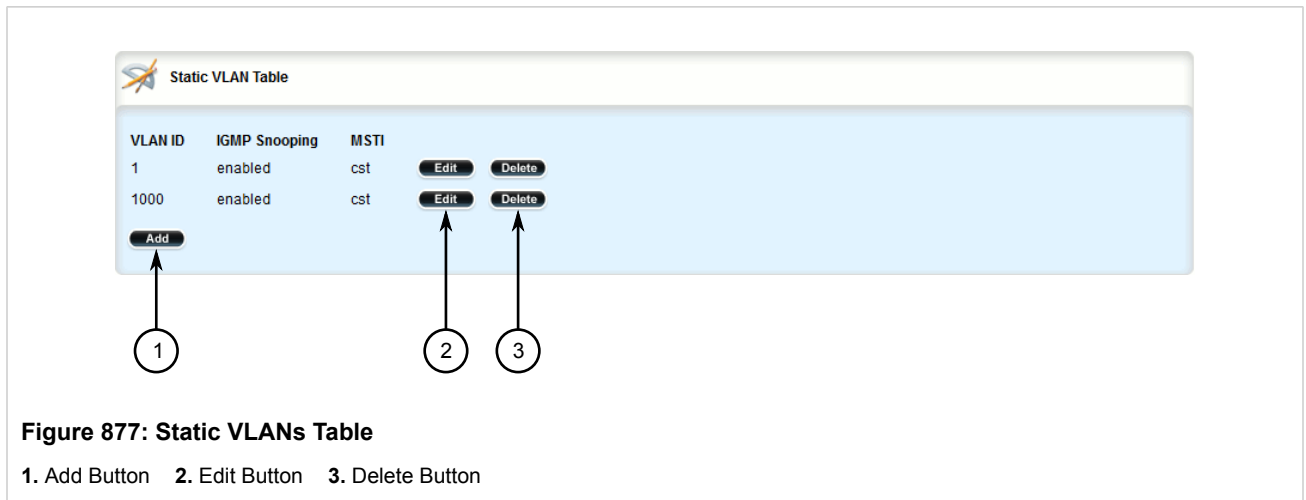
6. If needed, configure a forbidden ports list. For more information, refer to [Section 5.36.5.2, “Adding a Forbidden Port”](#).
7. Configure the VLAN. For more information, refer to [Section 5.36.3.2, “Configuring VLANs for Switch Ethernet Ports”](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

### Section 5.36.4.3

## Deleting a Static VLAN

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » vlans » static-vlan**. The **Static VLANs** table appears.



3. Click **Delete** next to the chosen static VLAN.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.36.5

## Managing Forbidden Ports

Static VLANs can be configured to exclude ports from membership in the VLAN using the forbidden ports list.

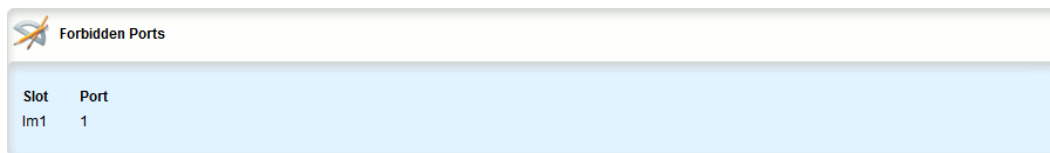
The following sections describe how to configure and manage a list of forbidden ports:

- [Section 5.36.5.1, “Viewing a List of Forbidden Ports”](#)
- [Section 5.36.5.2, “Adding a Forbidden Port”](#)
- [Section 5.36.5.3, “Deleting a Forbidden Port”](#)

### Section 5.36.5.1

## Viewing a List of Forbidden Ports

To view a list of forbidden ports, navigate to **switch » vlans » static-vlan » {name} » forbidden-ports**, where **{name}** is the name of the static VLAN. If ports have been forbidden, the **Forbidden Ports** table appears.



Slot	Port
Im1	1

**Figure 878: Forbidden Ports Table**

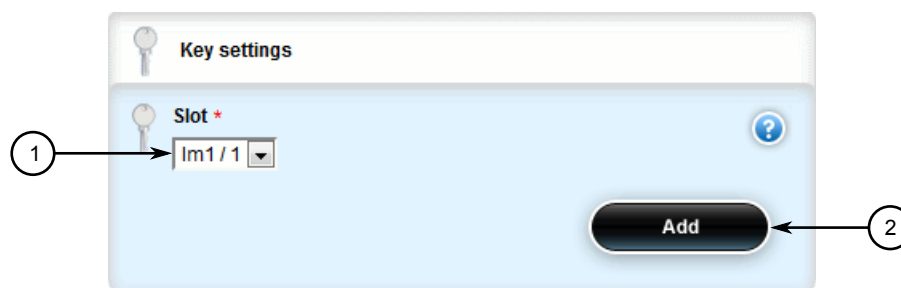
If no ports have been forbidden, add forbidden ports as needed. For more information, refer to [Section 5.36.5.2, “Adding a Forbidden Port”](#).

#### Section 5.36.5.2

### Adding a Forbidden Port

To add a forbidden port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » vlans » static-vlan » {name} » forbidden-ports**, where {name} is the name of the static VLAN.
3. Click **<Add forbidden-ports>**. The **Key Settings** form appears.



**Figure 879: Key Settings Form**

1. Slot Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Slot	The name of the module location provided on the silkscreen across the top of the device.
Port	The selected ports on the module installed in the indicated slot.

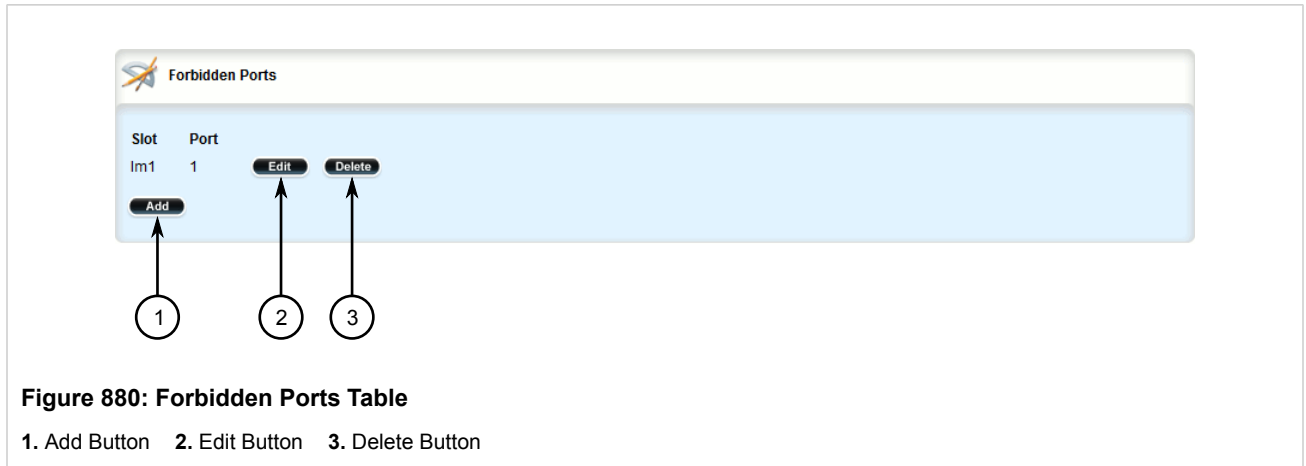
5. Click **Add** to add the forbidden port.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.36.5.3

## Deleting a Forbidden Port

To delete a forbidden port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » vlans » static-vlan » {name} » forbidden-ports**, where {name} is the name of the static VLAN. The **Forbidden Ports** table appears.



3. Click **Delete** next to the chosen port.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.36.6

## Managing VLANs for Virtual Switches

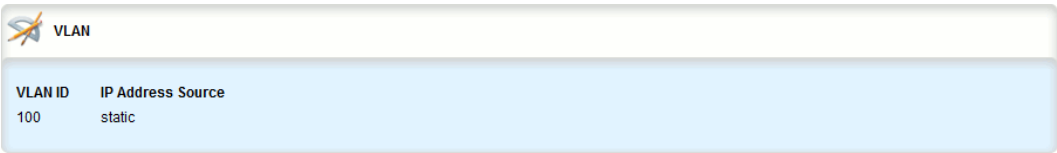
The following sections describe how to configure and manage VLANs for virtual switch interfaces:

- [Section 5.36.6.1, “Viewing a List of Virtual Switch VLANs”](#)
- [Section 5.36.6.2, “Adding a Virtual Switch VLAN”](#)
- [Section 5.36.6.3, “Deleting a Virtual Switch VLAN”](#)

### Section 5.36.6.1

## Viewing a List of Virtual Switch VLANs

To view a list of virtual switch VLANs, navigate to **interface » virtualswitch » {id} » vlan**, where {id} is the ID assigned to the virtual switch. If VLANs have been configured, the **VLAN** table appears.



VLAN ID	IP Address Source
100	static

Figure 881: VLAN Table

If no virtual switch VLANs have been configured, add VLANs as needed. For more information, refer to [Section 5.36.6.2, “Adding a Virtual Switch VLAN”](#).

Section 5.36.6.2

Adding a Virtual Switch VLAN

To add virtual switch VLAN, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *interface* » *virtualswitch* » *{id}* » *vlan*, where *{id}* is the ID assigned to the virtual switch.
3. Click **<Add vlan>**. The **Key Settings** form appears.

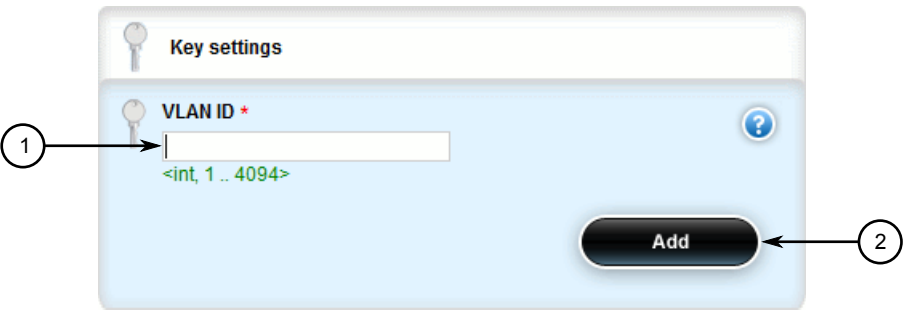


Figure 882: Key Settings Form

1. VLAN ID Box    2. Add Button

4. Configure the following parameter(s) as required:

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

5. Click **Add** to create the new VLAN. The **VLAN** form appears.



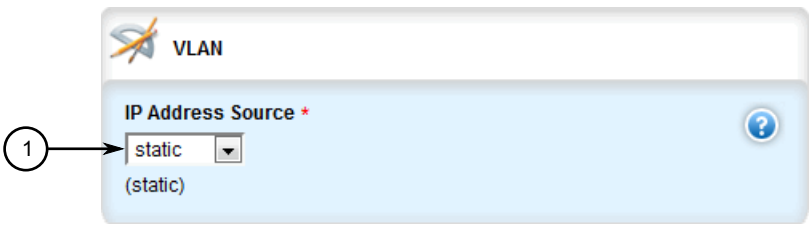


Figure 883: VLAN Form

1. IP Address Source Box

6. Configure the following parameter(s) as required:

Parameter	Description
IP Address Source	<b>Synopsis:</b> { static, dynamic } <b>Default:</b> static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.

7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 5.36.6.3

Deleting a Virtual Switch VLAN

To delete a virtual switch VLAN, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » virtualswitch » {id} » vlan**, where {id} is the ID assigned to the virtual switch. The **VLAN** table appears.

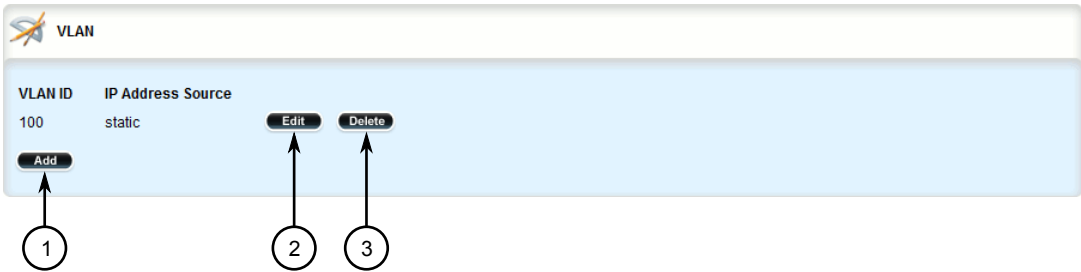


Figure 884: VLAN Table

1. Add Button    2. Edit Button    3. Delete Button

3. Click **Delete** next to the chosen VLAN.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.36.7

# Managing VLANs for Routable-Only Ethernet Ports


The following sections describe how to configure and manage VLANs for routable-only Ethernet ports:

- [Section 5.36.7.1, “Viewing a List of VLANs for Routable Ethernet Ports”](#)
- [Section 5.36.7.2, “Adding a VLAN to a Routable Ethernet Port”](#)
- [Section 5.36.7.3, “Deleting a VLAN for a Routable Ethernet Port”](#)

Section 5.36.7.1

## Viewing a List of VLANs for Routable Ethernet Ports

To view a list of VLANs configured for either a routable Ethernet port, navigate to **interface » {interface} » {interface-name} » vlan**, where *{interface}* is the type of interface and *{interface-name}* is the name of the interface. If VLANs have been configured, the **VLANs** table appears.



VLANs			
VLAN ID	IP Address Source	On-demand	
3	static	disabled	

Figure 885: VLANs Table

If no VLANs have been configured, add VLANs as needed. For more information about configuring VLANs for either a routable Ethernet port or virtual switch, refer to [Section 5.36.7.2, “Adding a VLAN to a Routable Ethernet Port”](#).

Section 5.36.7.2

## Adding a VLAN to a Routable Ethernet Port

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » eth » {interface-name} » vlan**, where *{interface-name}* is the name of the interface.
3. Click **<Add vlan>**. The **Key Settings** form appears.

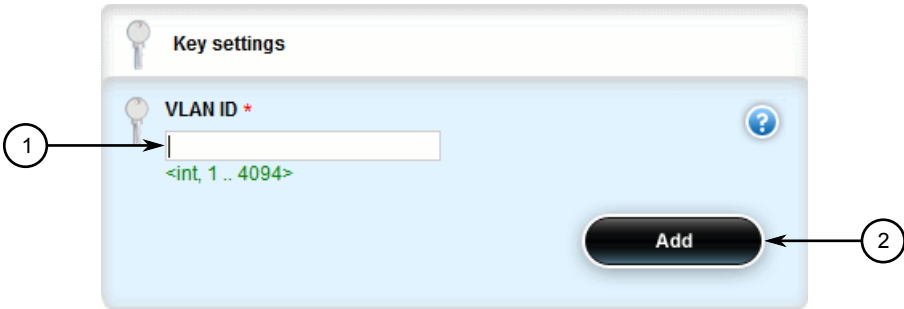


Figure 886: Key Settings Form

1. VLAN ID Box    2. Add Button

4. Configure the following parameter(s) as required:

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

5. Click **Add** to create the new VLAN. The **VLANs** form appears.

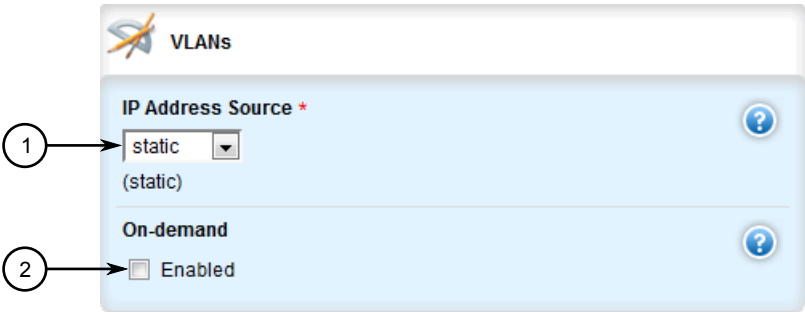


Figure 887: VLANs Form

1. IP Address Source Box    2. On-Demand Check Box

6. Configure the following parameter(s) as required:

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

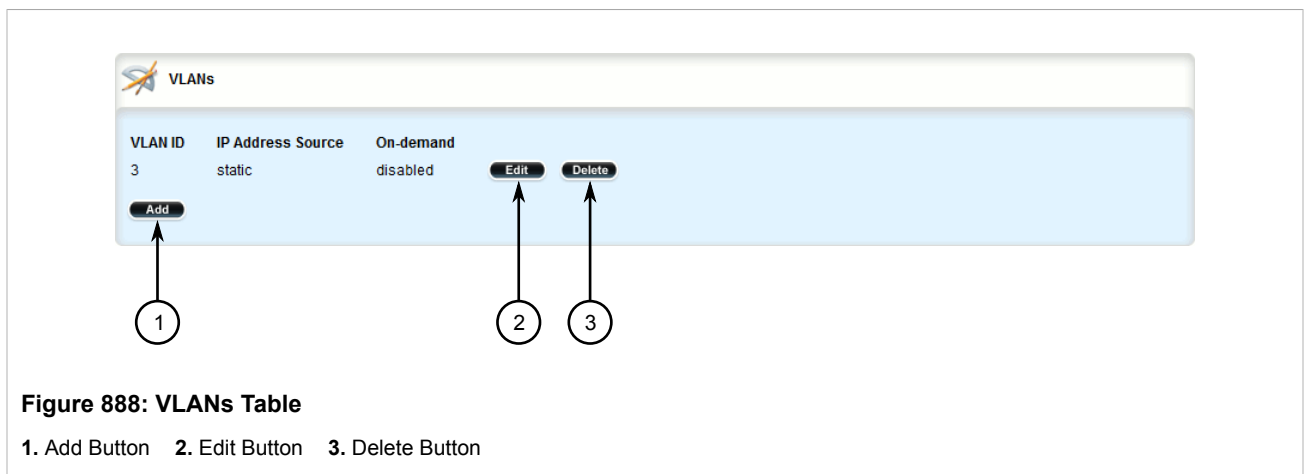
7. Add a QoS map for the VLAN. For more information, refer to [Section 5.38.7.2, “Adding a QoS Map”](#).
8. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
9. Click **Exit Transaction** or continue making changes.

### Section 5.36.7.3

## Deleting a VLAN for a Routable Ethernet Port

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **interface » eth » {name} » vlan**, where {name} is the name of the interface. The **VLANs** table appears.



3. Click **Delete** next to the chosen VLAN.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.37

## Managing Network Discovery and 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, which 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.*

The following sections describe how to configure and manage LLDP:

- [Section 5.37.1, “Configuring LLDP”](#)
- [Section 5.37.2, “Viewing Global Statistics and Advertised System Information”](#)
- [Section 5.37.3, “Viewing Statistics for LLDP Neighbors”](#)
- [Section 5.37.4, “Viewing Statistics for LLDP Ports”](#)

## Section 5.37.1

## Configuring LLDP

To configure the Link Layer Discovery Protocol (LLDP), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **switch » net-discovery » lldp**. The **LLDP** form appears.

LLDP

1

Enabled \*

☒ Enabled  
(true)

?

2

Transmission Interval (sec) \*

30

(30)

?

3

Transmission Hold \*

4

(4)

?

4

Reinitialization Delay (sec) \*

2

(2)

?

5

Transmission Delay (sec) \*

2

(2)

?

6

Notification Interval (sec) \*

5

(5)

?

**Figure 889: LLDP Form**

1. Enabled Check Box   2. Transmission Interval Box   3. Transmission Hold Box   4. Reinitialization Delay Box   5. Transmission Delay Box   6. Notification Interval Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> true Enables the Link Layer Discovery Protocol (LLDP). Note that LLDP is enabled on a port when LLDP is enabled globally and along with enabling per port setting in the Port LLDP Parameters menu.
Transmission Interval (sec)	<b>Synopsis:</b> An integer between 5 and 32768 <b>Default:</b> 30 The interval at which Link Layer Discovery Protocol (LLDP) frames are transmitted on behalf of this LLDP agent.
Transmission Hold	<b>Synopsis:</b> An integer between 2 and 10 <b>Default:</b> 4 The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in an LLDPDU. The actual

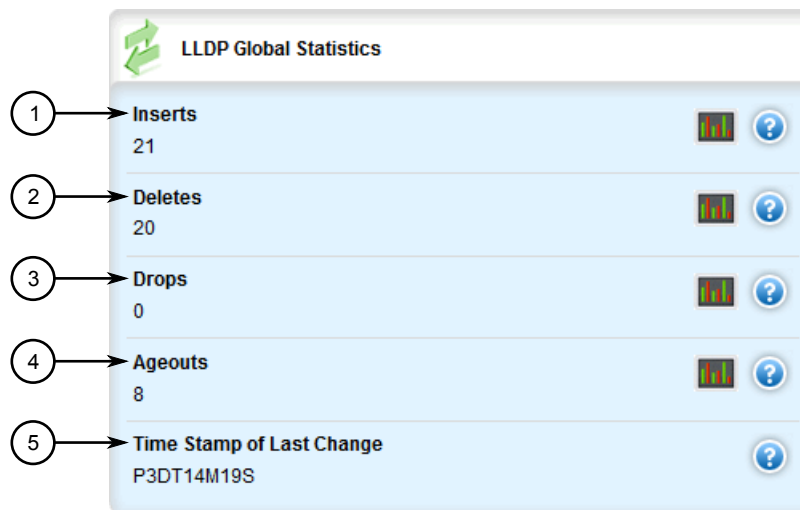
Parameter	Description
	TTL value can be expressed by the following formula: $TTL = \text{MIN}(65535, (\text{Tx Interval} * \text{Tx Hold}))$
Reinitialization Delay (sec)	<b>Synopsis:</b> An integer between 1 and 10 <b>Default:</b> 2 The delay in seconds from when the value of the Admin Status parameter of a particular port becomes 'Disabled' until re-initialization will be attempted.
Transmission Delay (sec)	<b>Synopsis:</b> An integer between 1 and 8192 <b>Default:</b> 2 The delay in seconds between successive LLDP frame transmissions initiated by the value or status changed. The recommended value is set by the following formula: 1 is less than or equal to txDelay less than or equal to $(0.25 * \text{Tx Interval})$
Notification Interval (sec)	<b>Synopsis:</b> An integer between 5 and 3600 <b>Default:</b> 5 Controls transmission of LLDP traps. The agent must not generate more than one trap in an indicated period.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.37.2

## Viewing Global Statistics and Advertised System Information

To view global statistics for LLDP and the system information that is advertised to neighbors, navigate to **switch » net-discovery » lldp**. The **LLDP Global Statistics** and **LLDP Local System** forms appear.



**Figure 890: LLDP Global Statistics Form**

1. Inserts   2. Deletes   3. Drops   4. Ageouts   5. Time Stamp of Last Change

The screenshot shows the 'LLDP Local System' configuration form. It has a title bar with a green icon and the text 'LLDP Local System'. Below the title bar are six sections, each with a blue header and a help icon (question mark in a circle). The sections are: 1. Local Chassis Subtype (with a dropdown menu showing 'macAddress'), 2. Local Chassis ID (with the value '00:0a:dc:ff:9a:00'), 3. Local Chassis Name (with the value 'R12.localdomain'), 4. Local Chassis Description (with the value 'RX5000-R-MNT-HI-HI-SM61-CM01-L3SEC-16TX01-XX-XX-XX-4FG50-X...'), 5. Local System Capabilities (with a list of checkboxes: stationOnly, docsisCableDevice, telephone, router (checked), wlanAccessPoint, bridge (checked), repeater, other), and 6. Local System Capabilities Enabled (with the same list of checkboxes as section 5). Numbered callouts 1 through 6 point to each of these sections respectively.

Figure 891: LLDP Local System Form

1. Local Chassis Subtype   2. Local Chassis ID   3. Local Chassis Name   4. Local Chassis Description   5. Local System Capabilities  
6. Local System Capabilities Enabled

The **LLDP Global Statistics** form displays the following information:

Parameter	Description
Inserts	<b>Synopsis:</b> An integer between 0 and 4294967295 The number of times an entry was inserted into the LLDP Neighbor Information Table.
Deletes	<b>Synopsis:</b> An integer between 0 and 4294967295 The number of times an entry was deleted from the LLDP Neighbor Information Table.
Drops	<b>Synopsis:</b> An integer between 0 and 4294967295



Parameter	Description
	The number of times an entry was deleted from the LLDP Neighbor Information Table because the information timeliness interval has expired.
Ageouts	<b>Synopsis:</b> An integer between 0 and 4294967295 The number of all TLVs discarded.
Time Stamp of Last Change	<b>Synopsis:</b> A string The duration of time between power-on and when this information was received.

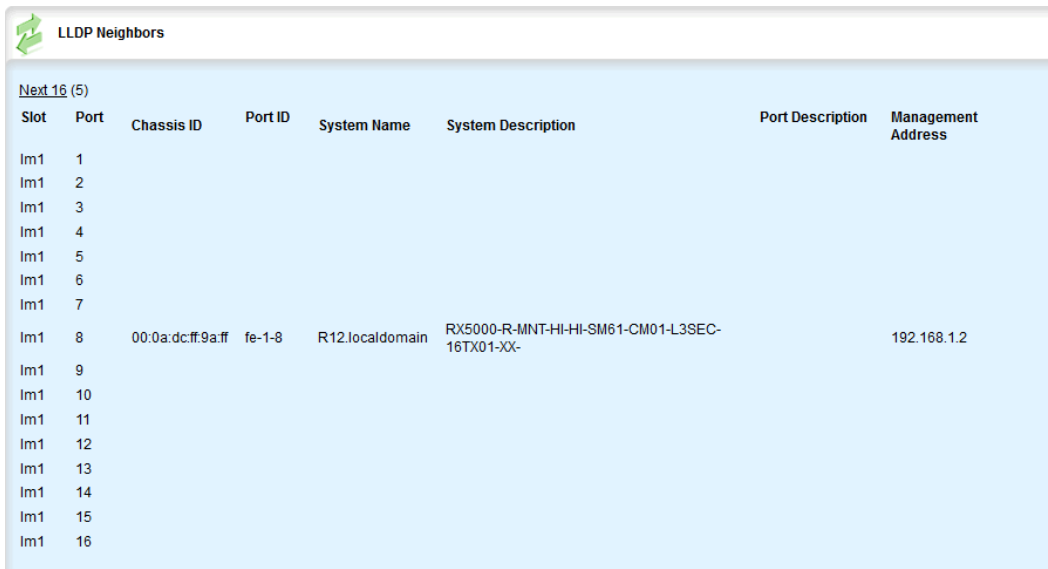
The **LLDP Local System** form displays the following information:

Parameter	Description
Local Chassis Subtype	<b>Synopsis:</b> { chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local } local-chassis-subtype
Local Chassis ID	<b>Synopsis:</b> A string local-chassis-id
Local Chassis Name	<b>Synopsis:</b> A string 1 to 255 characters long local-system-name
Local Chassis Description	<b>Synopsis:</b> A string 1 to 255 characters long local-system-desc
Local System Capabilities	local-system-caps
Local System Capabilities Enabled	local-system-caps-enabled

### Section 5.37.3

## Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, navigate to **switch » net-discovery » lldp » port-lldp-neighbors**. The **LLDP Neighbors** form appears.



The screenshot shows the 'LLDP Neighbors' page in a web interface. It features a table with columns for Slot, Port, Chassis ID, Port ID, System Name, System Description, Port Description, and Management Address. The table lists 16 entries for slot 'Im1', with ports 1 through 16. Port 8 is populated with data: Chassis ID '00:0a:dc:ff:9a:ff', Port ID 'fe-1-8', System Name 'R12.localdomain', System Description 'RX5000-R-MNT-HI-HI-SM61-CM01-L3SEC-16TX01-XX-', and Management Address '192.168.1.2'. A 'Next 16 (5)' link is visible at the top left of the table area.

Slot	Port	Chassis ID	Port ID	System Name	System Description	Port Description	Management Address
Im1	1						
Im1	2						
Im1	3						
Im1	4						
Im1	5						
Im1	6						
Im1	7						
Im1	8	00:0a:dc:ff:9a:ff	fe-1-8	R12.localdomain	RX5000-R-MNT-HI-HI-SM61-CM01-L3SEC-16TX01-XX-		192.168.1.2
Im1	9						
Im1	10						
Im1	11						
Im1	12						
Im1	13						
Im1	14						
Im1	15						
Im1	16						

**Figure 892: LLDP Neighbors Form**

This table displays the following information:

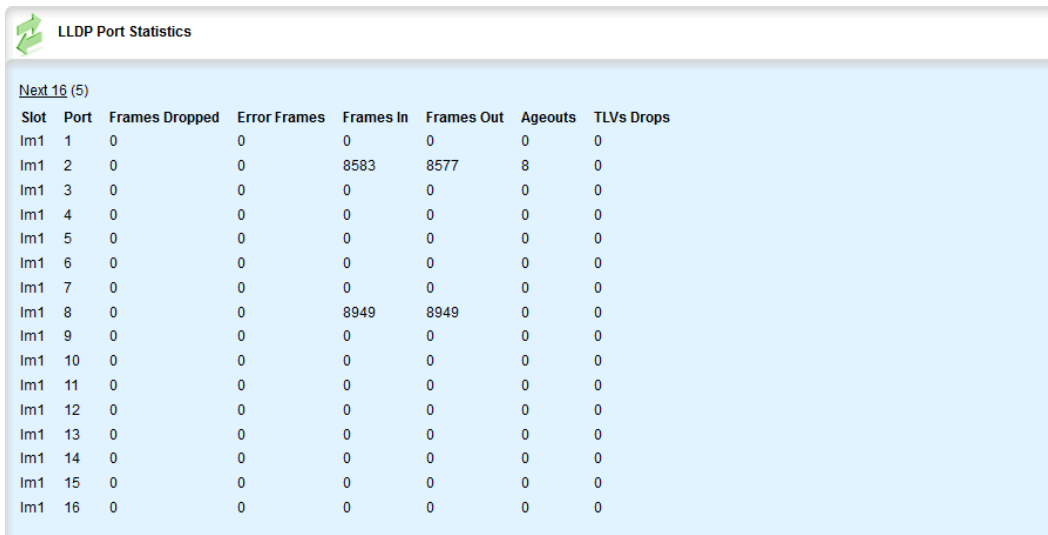
Parameter	Description
slot	<b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, cm, em, trnk } The slot of the module that contains this port.
Port	<b>Synopsis:</b> An integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
Chassis ID	<b>Synopsis:</b> A string The Chassis ID information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Port ID	<b>Synopsis:</b> A string The port ID (MAC) information received from a remote Link Layer Discovery Protocol (LLDP) agent.
System Name	<b>Synopsis:</b> A string 1 to 255 characters long The system name information received from a remote Link Layer Discovery Protocol (LLDP) agent
System Description	<b>Synopsis:</b> A string 1 to 255 characters long The system descriptor information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Port Description	<b>Synopsis:</b> A string 1 to 255 characters long The port description information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address	<b>Synopsis:</b> A string The management address received from a remote Link Layer Discovery Protocol (LLDP) agent.

Parameter	Description
Management Address Interface ID	The Management Address Interface ID received from a remote Link Layer Discovery Protocol (LLDP) agent.
System Capabilities	The system capabilities that are advertised for the remote device.
System Capabilities Enabled	Enables/disables the System Capabilities feature.
Chassis Subtype	<b>Synopsis:</b> { chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local } The chassis subtype information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Port Subtype	<b>Synopsis:</b> { interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, agentCircuitId, local } The port subtype information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address Subtype	<b>Synopsis:</b> { 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 management address subtype received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address Interface Subtype	<b>Synopsis:</b> { unknown, ifIndex, systemPortNumber } The management address interface subtype received from a remote Link Layer Discovery Protocol (LLDP) agent.
Time Stamp of Last Change	<b>Synopsis:</b> A string The duration of time between power-on and when this information was received.

## Section 5.37.4

## Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, navigate to **switch » net-discovery » lldp » port-lldp-stats**. The **LLDP Port Statistics** form appears.



The image shows a screenshot of the 'LLDP Port Statistics' form in a web interface. It features a green icon with a double arrow and the title 'LLDP Port Statistics'. Below the title is a link 'Next 16 (5)'. The main content is a table with 8 columns: Slot, Port, Frames Dropped, Error Frames, Frames In, Frames Out, Ageouts, and TLVs Drops. The table lists statistics for 16 ports (1-16) under slot 'lm1'. Ports 1, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, and 16 show zero values for all metrics. Ports 2 and 8 show non-zero values for Frames In and Frames Out.

Slot	Port	Frames Dropped	Error Frames	Frames In	Frames Out	Ageouts	TLVs Drops
lm1	1	0	0	0	0	0	0
lm1	2	0	0	8583	8577	8	0
lm1	3	0	0	0	0	0	0
lm1	4	0	0	0	0	0	0
lm1	5	0	0	0	0	0	0
lm1	6	0	0	0	0	0	0
lm1	7	0	0	0	0	0	0
lm1	8	0	0	8949	8949	0	0
lm1	9	0	0	0	0	0	0
lm1	10	0	0	0	0	0	0
lm1	11	0	0	0	0	0	0
lm1	12	0	0	0	0	0	0
lm1	13	0	0	0	0	0	0
lm1	14	0	0	0	0	0	0
lm1	15	0	0	0	0	0	0
lm1	16	0	0	0	0	0	0

**Figure 893: LLDP Port Statistics Form**

This table displays the following information:

Parameter	Description
slot	<b>Synopsis:</b> { ---, pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, cm, em, trnk } The slot of the module that contains this port.
Port	<b>Synopsis:</b> An integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
Frames Dropped	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol (LLDP) frames discarded.
Error Frames	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol Units (LLDPUs) received with detectable errors.
Frames In	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol Units (LLDPUs) received.
Frames Out	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol Units (LLDPUs) transmitted.
Ageouts	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of the times that a neighbor's information has been deleted from the Link Layer Discovery Protocol (LLDP) remote system MIB because the txinfoTTL timer has expired
TLVs Drops	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of all TLVs discarded
TLVs Unknown	<b>Synopsis:</b> An integer between 0 and 4294967295 A counter of all TLVs received on the port that are not recognized by the Link Layer Discovery Protocol (LLDP) local agent

## Section 5.38

# 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 5.16, “Managing Firewalls”](#).

RUGGEDCOM ROX II allows up to 4 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.

The following sections describe how to configure and manage traffic control settings:

- [Section 5.38.1, “Enabling and Configuring Traffic Control”](#)
- [Section 5.38.2, “Managing Traffic Control Interfaces”](#)
- [Section 5.38.3, “Managing Traffic Control Priorities”](#)
- [Section 5.38.4, “Managing Traffic Control Classes”](#)
- [Section 5.38.5, “Managing Traffic Control Devices”](#)
- [Section 5.38.6, “Managing Traffic Control Rules”](#)
- [Section 5.38.7, “Managing QoS Mapping for VLANs”](#)
- [Section 5.38.8, “Managing Egress Markers for QoS Maps”](#)
- [Section 5.38.9, “Viewing QoS Statistics”](#)

## Section 5.38.1

## 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**

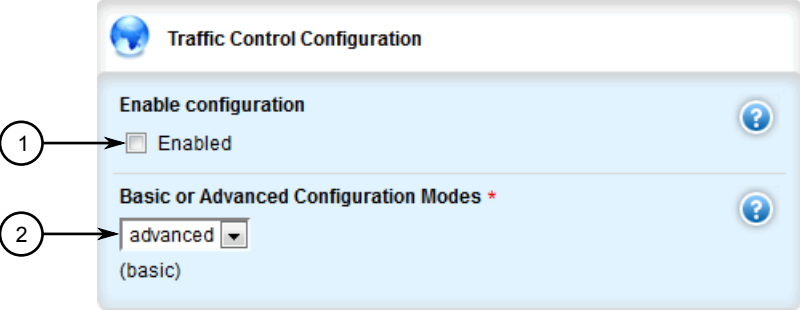
In advanced mode, each interface to be managed is assigned a total bandwidth for incoming and outgoing traffic. Classes are then defined for each interface, each with its own minimum assured bandwidth and a maximum permitted bandwidth. The combined minimum of the classes on an interface must be no more 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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control**. The **Traffic Control Configuration** form appears.



**Figure 894: Traffic Control Configuration Form**

1. Enable Configuration Box    2. Basic or Advanced Configuration Modes List

3. Configure the following parameter(s) as required:

Parameter	Description
Enable configuration	<b>Synopsis:</b> typeless Enables/disables traffic control (TC) for the current firewall configuration. The current firewall configuration is the one that is committed. When an active configuration is committed to the system, then an <b>enabled</b> TC configuration will be included. When a work configuration is committed, the <b>enabled</b> TC configuration will be included in the work configuration. <b>A TC configuration needs a firewall configuration to operate</b> .
Basic or Advanced Configuration Modes	<b>Synopsis:</b> { basic, advanced } <b>Default:</b> basic

Parameter	Description
	Choose to use either 'simple' or 'advanced' configuration modes. Click again on traffic-control after making a choice.

4. If basic mode is enabled, do the following:
  - a. Add traffic control interfaces. For more information, refer to [Section 5.38.2.2, “Adding a Traffic Control Interface”](#).
  - b. Add traffic control priorities. For more information, refer to [Section 5.38.3.2, “Adding a Traffic Control Priority”](#).
5. If advanced mode is enabled, do the following:
  - a. Add traffic control classes. For more information, refer to [Section 5.38.4.2, “Adding a Traffic Control Class”](#).
  - b. Add traffic control devices. For more information, refer to [Section 5.38.5.2, “Adding a Traffic Control Device”](#).
  - c. Add traffic control rules. For more information, refer to [Section 5.38.6.2, “Adding a Traffic Control Rule”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

## Section 5.38.2

## 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 5.38.1, “Enabling and Configuring Traffic Control”](#).*

The following sections describe how to configure and manage traffic control interfaces:

- [Section 5.38.2.1, “Viewing a List of Traffic Control Interfaces”](#)
- [Section 5.38.2.2, “Adding a Traffic Control Interface”](#)
- [Section 5.38.2.3, “Deleting a Traffic Control Interface”](#)

## Section 5.38.2.1

### Viewing a List of Traffic Control Interfaces

To view a list of traffic control interfaces, navigate to **qos » traffic-control » basic-configuration » tcinterfaces**. If interfaces have been configured, the **Basic Traffic Control Interfaces** table appears.

Basic Traffic Control Interfaces						
Interface	Type	Ingress Speed (numerical value only)	Unit for ingress speed	Egress Speed (numerical value only)	Unit for egress speed	Description
te1-3-1c24ppp	external	1500	kilobits	1500	kilobits	TC on T1 Link

**Figure 895: Basic Traffic Control Interfaces Table**

If no interfaces have been configured, add interfaces as needed. For more information, refer to [Section 5.38.2.2, “Adding a Traffic Control Interface”](#).

### Section 5.38.2.2

## Adding a Traffic Control Interface

To add a new traffic control interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control » basic-configuration » tcinterfaces**, and click **<Add tcinterfaces>**. The **Key Settings** form appears.

**Figure 896: Key Settings Form**

1. Interface Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
interface	<p><b>Synopsis:</b> A string 1 to 15 characters long</p> <p>An interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.</p>

4. Click **Add** to create the new traffic control interface. The **Interface to Apply Traffic Control** form appears.



Interface to Apply Traffic Control

1. Type \*  
none  
(none)

2. Ingress Speed (numerical value only)  
---

3. Egress Speed (numerical value only) \*  
<unsignedShort>

4. Unit for egress speed \*  
bps

5. Description  
---

Figure 897: Interface to Apply Traffic Control Form

1. Type List   2. Ingress Speed Box   3. Egress Speed Box   4. Unit for Egress Speed List   5. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Type	<b>Synopsis:</b> { internal, external, none } <b>Default:</b> 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.
Ingress Speed (numerical value only)	(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.
Unit for Ingress Speed	<b>Synopsis:</b> { none, kilobits, megabits } <b>Default:</b> none

Parameter	Description
	The unit for inbandwidth, per second.
Egress Speed (numerical value only)	The outgoing bandwidth for this interface. Specify only the number here. The unit (kilobits, megabits) is specified in the out-unit.
Unit for Egress Speed	<b>Synopsis:</b> { kilobits, megabits } <b>Default:</b> megabits The unit for outgoing bandwidth, per second.
Description	<b>Synopsis:</b> A string A description for this configuration item.

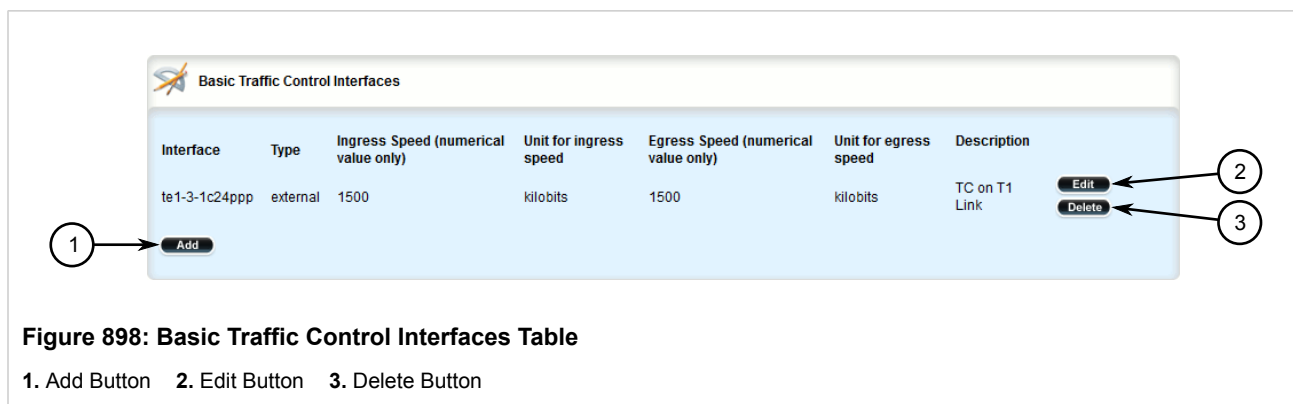
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.38.2.3

## Deleting a Traffic Control Interface

To delete a traffic control interface, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **qos » traffic-control » basic-configuration » tcinterfaces**. The **Basic Traffic Control Interfaces** table appears.



- Click **Delete** next to the chosen traffic control interface.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.38.3

## 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 5.38.1, “Enabling and Configuring Traffic Control”](#).

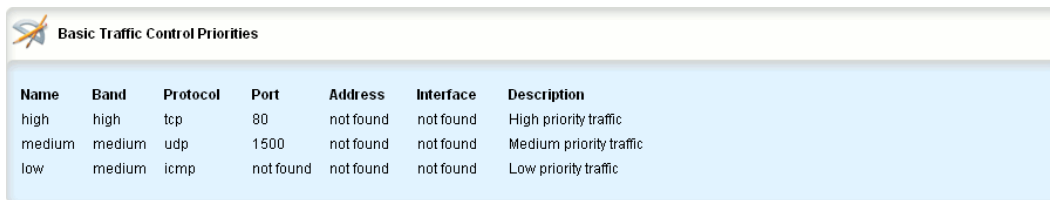
The following sections describe how to configure and manage traffic control priorities:

- [Section 5.38.3.1, “Viewing a List of Traffic Control Priorities”](#)
- [Section 5.38.3.2, “Adding a Traffic Control Priority”](#)
- [Section 5.38.3.3, “Deleting a Traffic Control Priority”](#)

## Section 5.38.3.1

## Viewing a List of Traffic Control Priorities

To view a list of traffic control priorities, navigate to **qos » traffic-control » basic-configuration » tcpriorities**. If priorities have been configured, the **Basic Traffic Control Priorities** table appears.



Name	Band	Protocol	Port	Address	Interface	Description
high	high	tcp	80	not found	not found	High priority traffic
medium	medium	udp	1500	not found	not found	Medium priority traffic
low	medium	icmp	not found	not found	not found	Low priority traffic

**Figure 899: Basic Traffic Control Priorities Table**

If no priorities have been configured, add priorities as needed. For more information, refer to [Section 5.38.3.2, “Adding a Traffic Control Priority”](#).

## Section 5.38.3.2

## Adding a Traffic Control Priority

To add a new traffic control priority, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control » basic-configuration » tcpriorities**, and click **<Add tcpriorities>**. The **Key Settings** form appears.

**Figure 900: Key Settings Form**

1. Name Box 2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string A distinct name for this configuration entry.

- Click **Add** to create the new traffic control priority. The **Basic Traffic Control Priorities** form appears.

**Figure 901: Basic Traffic Control Priorities Form**

1. Band List 2. Protocol Box 3. Port Box 4. Address Box 5. Interface Box 6. Description Box

- Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
band	<b>Synopsis:</b> { high, medium, low } <b>Default:</b> medium Priority (band) : high, medium, low... <b>High</b> band includes: Minimize Delay (md) (0x10), md + Minimize Monetary Cost (mmc) (0x12), md + Maximize Reliability (mr) (0x14), mmc+md+mr (0x16). <b>Medium</b> 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). <b>Low</b> band includes: mmc (0x02), mt (0x08), mmc+mt (0x0a), mr+mt (0x0c), mmc+mr+mt (0x0e).
protocol	<b>Synopsis:</b> { tcp, udp, icmp, all } or a string (choice) A targeted protocol.
port	<b>Synopsis:</b> A string (choice) Source port - can be specified <b>only if</b> protocol is TCP, UDP, DCCP, SCTP or UDPlite <b>Prerequisite:</b> A port number can be specified only when the protocol is either TCP, UDP, DCCP, SCTP or UDPlite
address	<b>Synopsis:</b> A string (choice) The source address. This can be specified <b>only if</b> the protocol, port and interface are not defined. <b>Prerequisite:</b> An address can be specified only if neither a protocol or port nor an interface are specified.
interface	<b>Synopsis:</b> A string 1 to 15 characters long (choice) The source interface. This can be specified <b>only if</b> the protocol, port and address are not defined. Lowercase alphanumerical as well as '.' and '-' characters are allowed. <b>Prerequisite:</b> An interface can be specified only if neither a protocol, port nor an address are specified.
description	<b>Synopsis:</b> A string (optional) A description for this configuration.

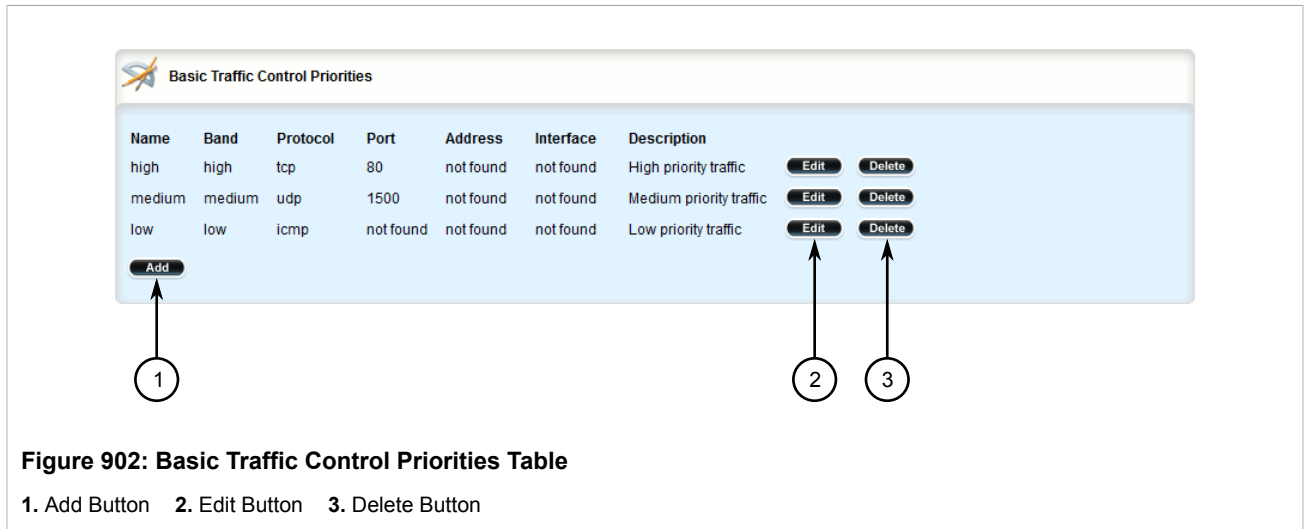
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

### Section 5.38.3.3

## Deleting a Traffic Control Priority

To delete a traffic control priority, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control » basic-configuration » tcpriorities**. The **Basic Traffic Control Priorities** table appears.



3. Click **Delete** next to the chosen traffic control priority.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.38.4

## Managing Traffic Control Classes

Traffic control classes define classes for traffic shaping. Optionally, they can also define parameters for Type of Service (ToS), which is an eight-bit field in the IPv4 header. Traffic control can inspect the ToS value of an incoming IP frame and classify traffic to provide preferential service in the outgoing queue. Traffic classification is done based on the ToS value and the ToS options defined for each traffic control class and traffic control rule. IP Traffic matching with the ToS options takes precedence over the mark rules.



#### NOTE

*One traffic control class must be added for each network interface.*



#### NOTE

*Type of Service (ToS) is defined by the Internet Engineering Task Force (IETF). For more information about ToS, refer to [RFC 1349](http://tools.ietf.org/html/rfc1349) [http://tools.ietf.org/html/rfc1349].*

The following sections describe how to configure and manage traffic control classes:

- [Section 5.38.4.1, “Viewing a List of Traffic Control Classes”](#)
- [Section 5.38.4.2, “Adding a Traffic Control Class”](#)
- [Section 5.38.4.3, “Deleting a Traffic Control Class”](#)

Section 5.38.4.1

Viewing a List of Traffic Control Classes

To view a list of traffic control classes, navigate to *qos » traffic-control » advanced-configuration » tcclasses*. If classes have been configured, the **Advanced Traffic Control Classes** table appears.

Advanced Traffic Control Classes							
Name	Interface	Mark	Min-bandwidth	Minbw-unit	Max-bandwidth	Maxbw-unit	Priority
TCP	te1-3-1c01 ppp	1	full/2	none	full	none	1

Figure 903: Advanced Traffic Control Classes Table

If no classes have been configured, add classes as needed. For more information, refer to [Section 5.38.4.2, “Adding a Traffic Control Class”](#).

Section 5.38.4.2

Adding a Traffic Control Class

- To add a new traffic control class, do the following:
1. Change the mode to **Edit Private** or **Edit Exclusive**.
  2. Navigate to *qos » traffic-control » advanced-configuration » tcclasses* and click **<Add tcclasses>**. The **Key Settings** form appears.

Figure 904: Key Settings Form

1. Name Box    2. Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string The name for this TC class entry.

4. Click **Add** to create the new class. The **Class Options** and **Advanced Traffic Control Classes** forms appear.

The screenshot shows the 'Class Options' form in the RUGGEDCOM ROX II web interface. The form has a light blue header with a pencil icon and the title 'Class Options'. Below the header, there are eight rows of configuration options, each with a blue question mark icon on the right. The options are: 'ToS Minimize Delay \*', 'ToS Maximize Throughput \*', 'ToS Maximize Reliability \*', 'ToS Minimize Cost \*', 'ToS Normal Service \*', 'Default \*', 'TCP Ack \*', and 'ToS Value'. Each of the first seven options has a checkbox labeled 'Enabled' and the text '(false)' below it. The 'ToS Value' option has a notepad icon and a dashed line '---' next to it. Eight numbered callouts (1-8) are placed to the left of the form, with arrows pointing to the checkboxes for the first seven options and the notepad icon for the eighth option.

**Figure 905: Class Options Form**

1. ToS Minimize Delay Check Box   2. ToS Maximize Throughput Check Box   3. ToS Maximize Reliability Check Box   4. ToS Minimize Cost Check Box   5. ToS Normal Service Check Box   6. Default Check Box   7. TCP Ack Check Box   8. ToS Value Box



The screenshot shows the 'Advanced Traffic Control Classes' configuration form. It contains several fields with callout numbers 1 through 8 pointing to them:

- 1. Interface \* (text input field, type: <string>)
- 2. Mark \* (text input field, type: <unsignedShort, 1 .. 255>)
- 3. Minimum Bandwidth (text input field with a pencil icon, value: ---)
- 4. Minimum Bandwidth Units \* (text input field with a pencil icon, value: none, (none))
- 5. Maximum Bandwidth (text input field with a pencil icon, value: ---)
- 6. Maximum Bandwidth Units \* (text input field with a pencil icon, value: none, (none))
- 7. Priority \* (text input field with a pencil icon, value: 0, (0))
- 8. Description (text input field with a pencil icon, value: ---)

Figure 906: Advanced Traffic Control Classes Form

1. Interface Box   2. Mark Box   3. Minimum Bandwidth Box   4. Minimum Bandwidth Unit list   5. Maximum Bandwidth Box  
6. Maximum Bandwidth Unit List   7. Priority Box   8. Description Box

5. On the **Class Options**, configure the following parameter(s) as required:

Parameter	Description
ToS Minimize Delay	<b>Synopsis:</b> true or false <b>Default:</b> false Value/mask encoding: 0x10/0x10
ToS Maximize Throughput	<b>Synopsis:</b> true or false <b>Default:</b> false Value/mask encoding: 0x08/0x08
ToS Maximize Reliability	<b>Synopsis:</b> true or false <b>Default:</b> false Value/mask encoding: 0x04/0x04
ToS Minimize Cost	<b>Synopsis:</b> true or false

Parameter	Description
	<b>Default:</b> false Value/mask encoding: 0x02/0x02
ToS Normal Service	<b>Synopsis:</b> true or false <b>Default:</b> false Value/mask encoding: 0x00/0x1e
default	<b>Synopsis:</b> true or false <b>Default:</b> false <emphasis role="bold">One default class</emphasis> per interface <emphasis role="bold">must</emphasis> be defined.
TCP ACK	<b>Synopsis:</b> true or false <b>Default:</b> false All TCP ACK packets into this class. This option should be specified only once per interface.
ToS Value	<b>Synopsis:</b> A string A custom classifier for the given value/mask. The values are hexadecimal, prefixed by '0x'. Ex.: 0x56[0x0F]

6. On the **Advanced Traffic Control Classes**, configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
interface	<b>Synopsis:</b> A string The interface to which this class applies. Each interface must be listed only once. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
mark	<b>Synopsis:</b> An integer between 1 and 255 A mark that identifies traffic belonging to this class. This is a unique integer between 1-255. Each class must have its own unique mark.
Minimum Bandwidth	<b>Synopsis:</b> 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: <orderedlist><listitem>'full/3' for a third of the bandwidth and</listitem> <listitem>'full*9/10' for nine tenths of the bandwidth.</listitem></orderedlist> In such a case, do not specify any minbw-unit.
Minimum Bandwidth Units	<b>Synopsis:</b> { none, kilobits, megabits } <b>Default:</b> none (per second) Only if the minimum bandwidth is a <emphasis role="bold">single numerical value</emphasis>

Parameter	Description
Maximum Bandwidth	<b>Synopsis:</b> 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: <code>&lt;orderedlist&gt;&lt;listitem&gt;'full/3'</code> for a third of the bandwidth and <code>&lt;/listitem&gt; &lt;listitem&gt;'full*9/10'</code> for nine tenths of the bandwidth. <code>&lt;/listitem&gt;&lt;/orderedlist&gt;</code> In such a case, do not specify any maxbw-unit.
Maximum Bandwidth Units	<b>Synopsis:</b> { none, kilobits, megabits } <b>Default:</b> none (per second) only if max-bandwidth is a <b>single numerical value</b>
priority	<b>Synopsis:</b> An integer between 0 and 7 <b>Default:</b> 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	<b>Synopsis:</b> A string A description for this configuration item.

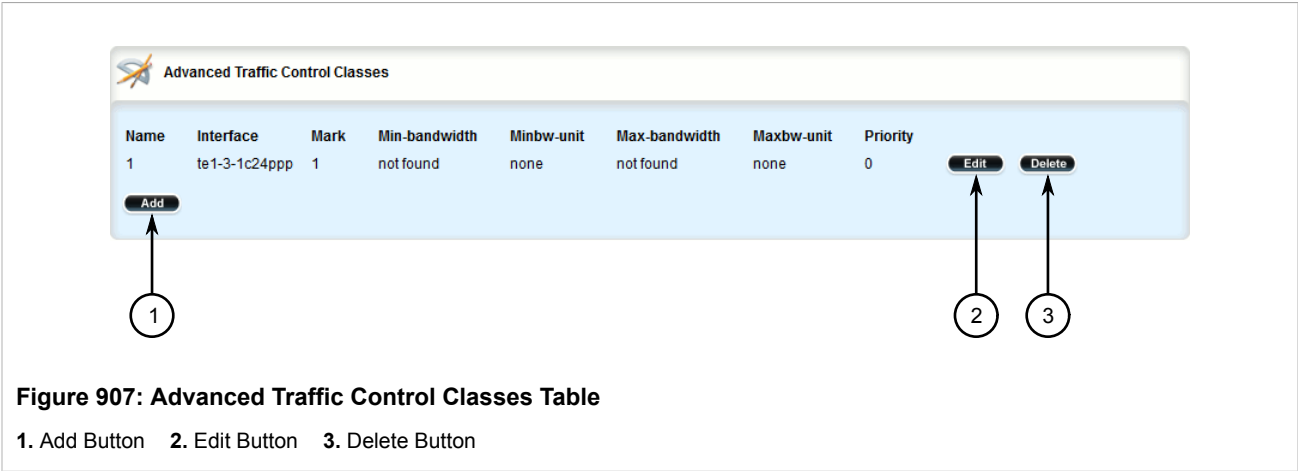
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.38.4.3

## Deleting a Traffic Control Class

To delete a traffic control class, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **qos » traffic-control » advanced-configuration » tcclasses**. The **Advanced Traffic Control Classes** table appears.




3. Click **Delete** next to the chosen class.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.38.5

# 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 5.38.1, “Enabling and Configuring Traffic Control”](#).*

The following sections describe how to configure and manage traffic control devices:

- [Section 5.38.5.1, “Viewing a List of Traffic Control Devices”](#)
- [Section 5.38.5.2, “Adding a Traffic Control Device”](#)
- [Section 5.38.5.3, “Deleting a Traffic Control Device”](#)

Section 5.38.5.1

## Viewing a List of Traffic Control Devices

To view a list of traffic control devices, navigate to **qos » traffic-control » advanced-configuration » tcdevices**. If devices have been configured, the **Advanced Traffic Control Interfaces** table appears.

Advanced Traffic Control Interfaces					
Interface	In Bandwidth	In Units	Out Bandwidth	Out Units	Description
te1-3-1c24ppp	1500	kilobits	1500	kilobits	not found

Figure 908: Advanced Traffic Control Interfaces Table

If no devices have been configured, add devices as needed. For more information, refer to [Section 5.38.5.2, “Adding a Traffic Control Device”](#).

Section 5.38.5.2

Adding a Traffic Control Device

To add a new traffic control device, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *qos » traffic-control » advanced-configuration » tcdevices*, and click **<Add tcdevices>**. The **Key Settings** form appears.

Key settings

Interface \*

1

<string>

2

Add

**Figure 909: Key Settings Form**

1. Interface Box    2. Add Button

- 3. Configure the following parameter(s) as required:

Parameter	Description
interface	<b>Synopsis:</b> A string 1 to 15 characters long An interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.

- 4. Click **Add** to create the new traffic control device. The **Advanced Traffic Control Interfaces** form appears.

**Figure 910: Advanced Traffic Control Interfaces Form**

1. In Band Width Box    2. In Unit List    3. Out Bandwidth Box    4. Out Unit List    5. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
In Bandwidth	<b>Default:</b> 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 Units	<b>Synopsis:</b> { none, kilobits, megabits } <b>Default:</b> none Unit for inbandwidth, per second.
Out Bandwidth	Maximum outgoing bandwidth... This is the maximum speed that can be handled. Additional packets will be dropped. This is the bandwidth that can be refred-to as 'full' when defining classes.
Out Units	<b>Synopsis:</b> { kilobits, megabits } <b>Default:</b> megabits Unit for outgoing bandwidth, per second.
description	<b>Synopsis:</b> A string

Parameter	Description
	A description for this configuration item.

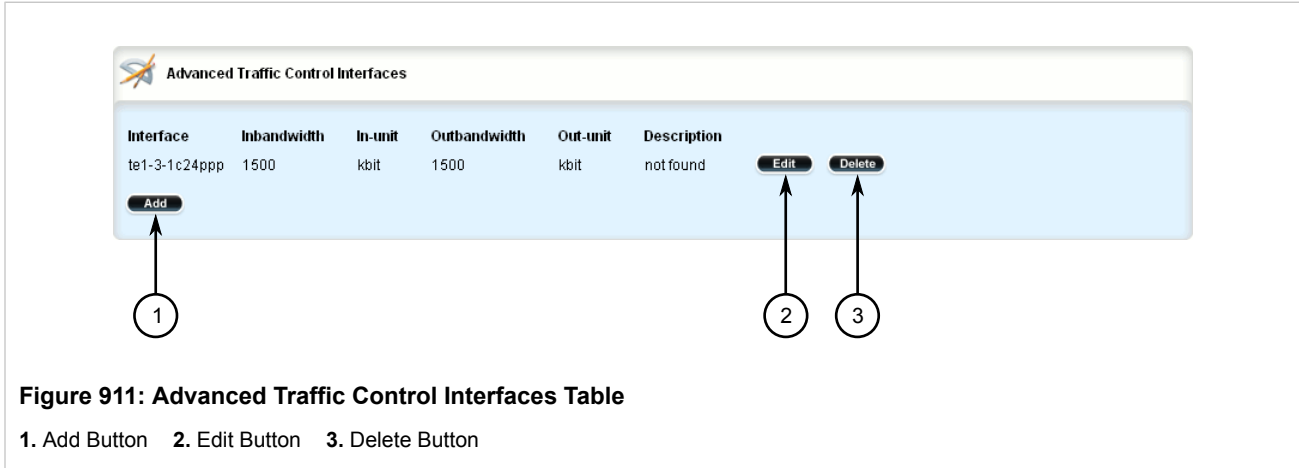
- 6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 7. Click **Exit Transaction** or continue making changes.

Section 5.38.5.3

Deleting a Traffic Control Device

To delete a traffic control device, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to **qos » traffic-control » advanced-configuration » tcdevices**. The **Advanced Traffic Control Interfaces** table appears.




- 3. Click **Delete** next to the chosen traffic control device.
- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

Section 5.38.6

Managing Traffic Control Rules

Traffic control rules define rules 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 5.38.1, “Enabling and Configuring Traffic Control”](#).*

The following sections describe how to configure and manage traffic control rules:

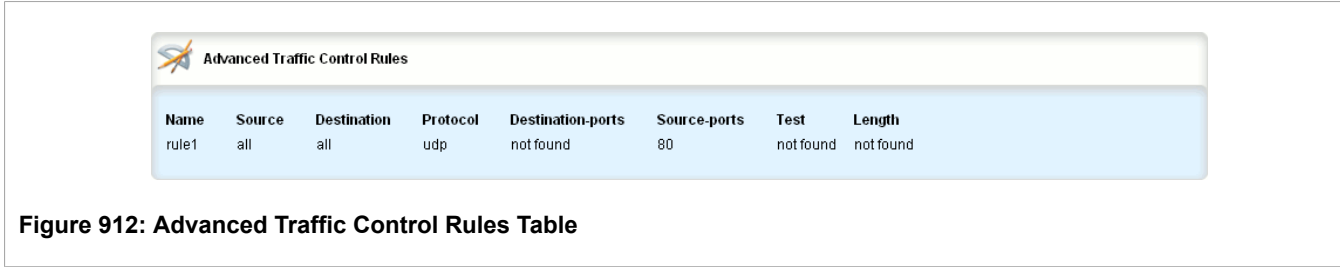
- [Section 5.38.6.1, “Viewing a List of Traffic Control Rules”](#)
- [Section 5.38.6.2, “Adding a Traffic Control Rule”](#)

- [Section 5.38.6.3, “Configuring QoS Marking”](#)
- [Section 5.38.6.4, “Deleting a Traffic Control Rule”](#)

Section 5.38.6.1

Viewing a List of Traffic Control Rules

To view a list of traffic control rules, navigate to **qos » traffic-control » advanced-configuration » tcrules**. If rules have been configured, the **Advanced Traffic Control Rules** table appears.



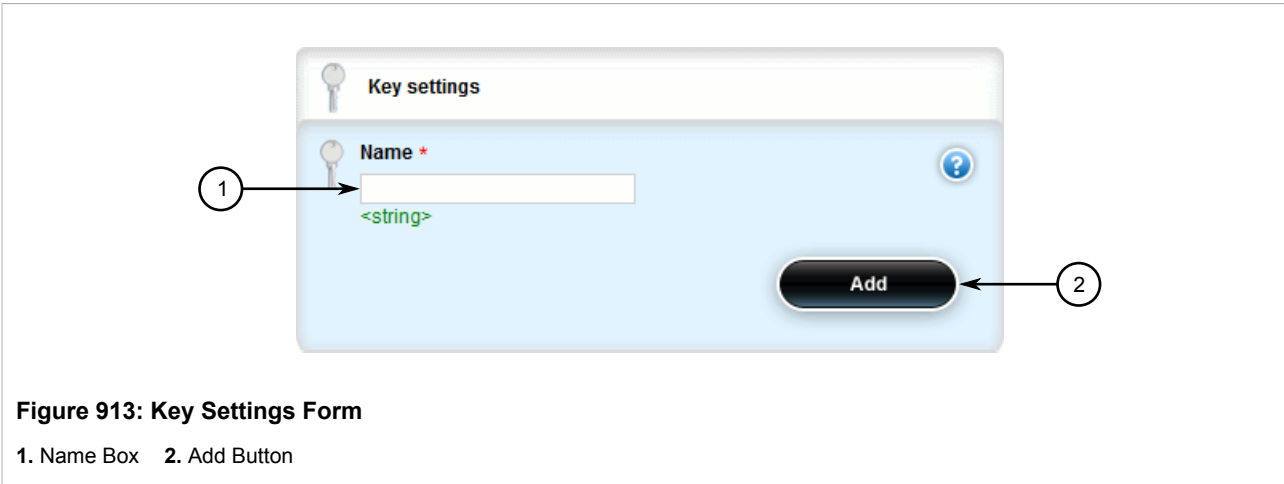
If no rules have been configured, add rules as needed. For more information, refer to [Section 5.38.6.2, “Adding a Traffic Control Rule”](#).

Section 5.38.6.2

Adding a Traffic Control Rule

To add a new traffic control rule, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control » advanced-configuration » tcrules**, and click **<Add tcrules>**. The **Key Settings** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
name	<b>Synopsis:</b> A string



Parameter	Description
	A distinct name for this rule.

4. Click **Add** to create the new traffic control rule. The **Advanced Traffic Control Rules** form appears.

The screenshot shows the 'Advanced Traffic Control Rules' form. It has a light blue background and a white header with the title and a logo. The form contains several fields, each with a blue question mark icon to its right. Numbered callouts point to the following fields: 1. Source (with a red asterisk), 2. Destination (with a red asterisk), 3. Protocol (with a red asterisk), 4. Destination Ports, 5. Source Ports, 6. Test, 7. Length, 8. Tos, and 9. Description. Each field has a small icon (a notepad with a pencil) next to it. The 'Source' and 'Destination' fields have a green '<string>' placeholder. The 'Protocol' field has a dropdown menu showing 'all' and '(all)'. The 'Destination Ports', 'Source Ports', 'Test', 'Length', 'Tos', and 'Description' fields have a '--' placeholder.

**Figure 914: Advanced Traffic Control Rules Form**

1. Source Box   2. Destination Box   3. Protocol Box   4. Destination Ports Box   5. Source Ports Box   6. Test Box   7. Length Box   8. TOS Box   9. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
iptype	<b>Synopsis:</b> { ipv4, ipv6, ipv4ipv6 } <b>Default:</b> ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.

Parameter	Description
source	<b>Synopsis:</b> A string IF name, comma-separated list of hosts or IPs, MAC addresses, or 'all'. When using MAC addresses, use '~' as prefix and '-' as separator. Ex.: ~00-1a-6b-4a-72-34,~00-1a-6b-4a-71-42
destination	<b>Synopsis:</b> A string IF name, comma-separated list of hosts or IPs, or 'all'.
protocol	<b>Synopsis:</b> { tcp, udp, icmp, all } or a string <b>Default:</b> all The protocol to match.
Destination Ports	<b>Synopsis:</b> A string (Optional) A comma-separated list of port names, port numbers or port ranges.
Source Ports	<b>Synopsis:</b> A string (Optional) A comma-separated list of port names, port numbers or port ranges.
test	<b>Synopsis:</b> 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: <b>&gt;!0&lt;/b&gt; Test if the connection mark is not zero: <b>&gt;!0:C&lt;/b&gt;</b></b>
length	<b>Synopsis:</b> 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 <b>&gt;64&lt;/b&gt; Greater or equal to 65 <b>&gt;=65&lt;/b&gt; Lesser or equal to 65 <b>&lt;=65&lt;/b&gt; In-between 64 and 768 <b>&gt;64:768&lt;/b&gt;</b></b></b></b>
tos	<b>Synopsis:</b> { 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	<b>Synopsis:</b> A string A description for this configuration item.

**NOTE**

*Only one QoS mark is allowed for each traffic control rule.*

- Configure the rules for a QoS mark. For more information, refer to [Section 5.38.6.3, “Configuring QoS Marking”](#).
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.38.6.3

## 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 assign the DSCP mark.

To configure the QoS mark for a traffic control rule, do the following:

### >> Configuring a Set Mark

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control » advanced-configuration » tcrules » {name} » mark-choice**, where {name} is the name of the traffic control rule.
3. In the menu, click **set**. The **Mark Choice Set** form appears.

The screenshot shows the 'Mark Choice Set' form in a web interface. It has a light blue header with a logo and the title 'Mark Choice Set'. Below the header are four sections, each with a label, a dropdown menu, and a help icon (a blue circle with a question mark). The sections are: 'Object \*' with a dropdown showing 'packet' and '(packet)'; 'Mark' with a dropdown showing '--'; 'Mask' with a dropdown showing '--'; and 'Chain Options \*' with a dropdown showing 'forward' and '(forward)'. Four numbered callouts (1, 2, 3, 4) point to the dropdown menus for Object, Mark, Mask, and Chain Options respectively.

**Figure 915: Mark Choice Set Form**

1. Object List   2. Mark   3. Mask   4. Chain Options List

4. Configure the following parameter(s) as required:

**NOTE**

The `chain-options` parameter specifies the chain in which the rule will be processed.

- **Pre-Routing - Mark the connection in the PREROUTING chain.**  
*This can be used with DNAT, SNAT and Masquerading rules in the firewall. An example of such a rule is Source.IP:192.168.2.101, Chain-option: preroute or default, but the actual Source.NAT address is 2.2.2.2.*
- **Post-Routing - Mark the connection in the POSTROUTING chain.**  
*This can be used with DNAT, SNAT and Masquerading rules in the firewall. An example of such rule is Destination.IP:192.168.3.101, Chain-option: preroute or default. In this case, the actual destination address is 192.168.3.101, but it will be translated to 192.168.3.33 by DNAT. Another example of a traffic control rule is Destination.IP:192.168.3.33, Chain-option: postrouting.*
- **Forward - Mark the connection in the FORWARD chain.**  
*This is the default chain option and it can be used for normal IP traffic without any address or port translation.*

Parameter	Description
object	<b>Synopsis:</b> { packet, connection } <b>Default:</b> packet Sets the mark on either a packet or a connection.
mark	<b>Synopsis:</b> A string A mark that corresponds to a class mark (decimal value).
mask	<b>Synopsis:</b> A string (optional) A mask to determine which mark bits will be set.
chain-options	<b>Synopsis:</b> { forward, postrouting, prerouting } <b>Default:</b> forward A chain where the set operation will take place.

## » Configuring a Modify Mark

1. In the menu, click **modify**. The **Mark Choice Modify** form appears.

**Figure 916: Mark Choice Modify Form**

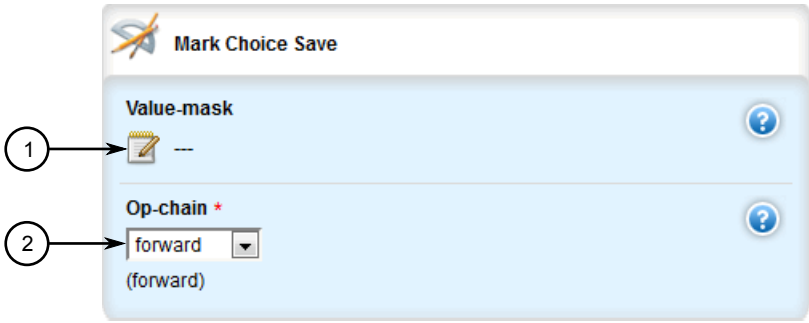
1. Logic Operation List    2. Mark Value Box    3. Modify Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
logic-op	<b>Synopsis:</b> { and, or } A logical operation to perform on the current mark: AND/OR.
mark-value	<b>Synopsis:</b> A string A mark to perform the operation with (decimal value).
modify-chain	<b>Synopsis:</b> { forward, postrouting, prerouting } <b>Default:</b> forward A chain in which the operation will take place.

>> **Configuring a Save Mark**

1. In the menu, click **save**. The **Mark Choice Save** form appears.



**Figure 917: Mark Choice Save Form**

1. Value Mask Box    2. Operation Chain List


2. Configure the following parameter(s) as required:

Parameter	Description
value-mask	<b>Synopsis:</b> A string Mask to process the mark with
op-chain	<b>Synopsis:</b> { forward, prerouting } <b>Default:</b> forward A chain in which the operation will take place.


>> **Configuring a Restore Mark**


1. In the menu, click **restore**. The **Mark Choice Restore** form appears.

Mark Choice Restore

Value-mask 

1 →

Op-chain \* 

2 → forward 

(forward)

**Figure 918: Mark Choice Restore Form**

1. Value Mask Box    2. Operation Chain List


2. Configure the following parameter(s) as required:


Parameter	Description
value-mask	<b>Synopsis:</b> A string A mask to process the mark with.
op-chain	<b>Synopsis:</b> { forward, prerouting } <b>Default:</b> forward A chain in which the operation will take place.

» **Configuring a Continue Mark**

1. In the menu, click **continue**. The **Mark Choice Continue** form appears.

Mark Choice Continue

Continue-chain \* 

1 → forward 

(forward)

**Figure 919: Mark Choice Continue Form**

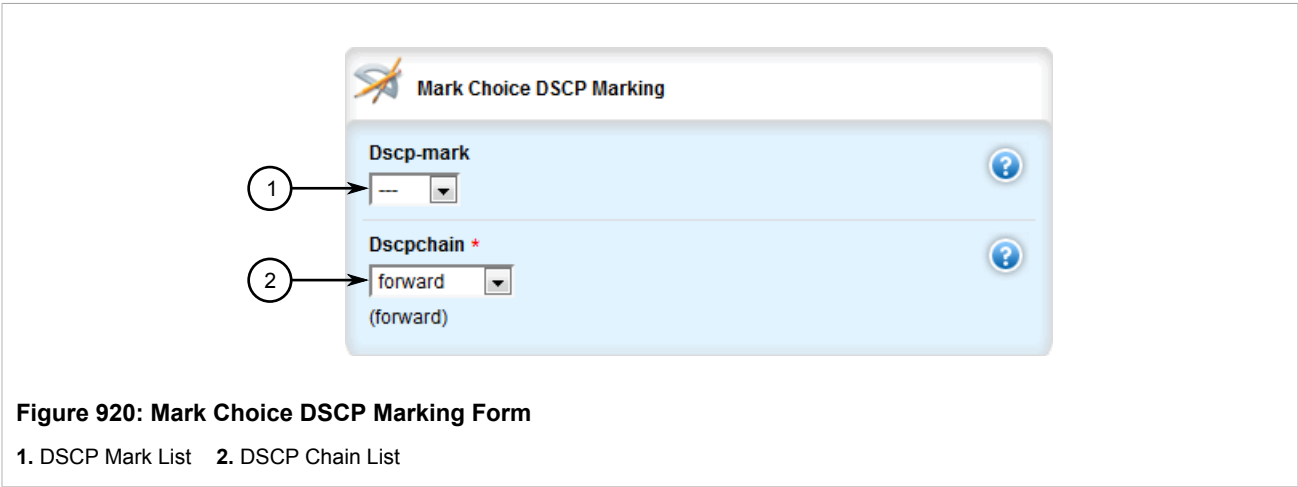
1. Continue Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
continue-chain	<b>Synopsis:</b> { forward, prerouting } <b>Default:</b> forward A chain in which the operation will take place.

>> **Configuring a DSCP Mark**

1. In the menu, click **dscpmarking**. The **Mark Choice DSCP Marking** form appears.



**Figure 920: Mark Choice DSCP Marking Form**

1. DSCP Mark List    2. DSCP Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
dscp-mark	<b>Synopsis:</b> { 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	<b>Synopsis:</b> { forward, postrouting, prerouting } <b>Default:</b> forward A chain where the DSCP marking will take place.

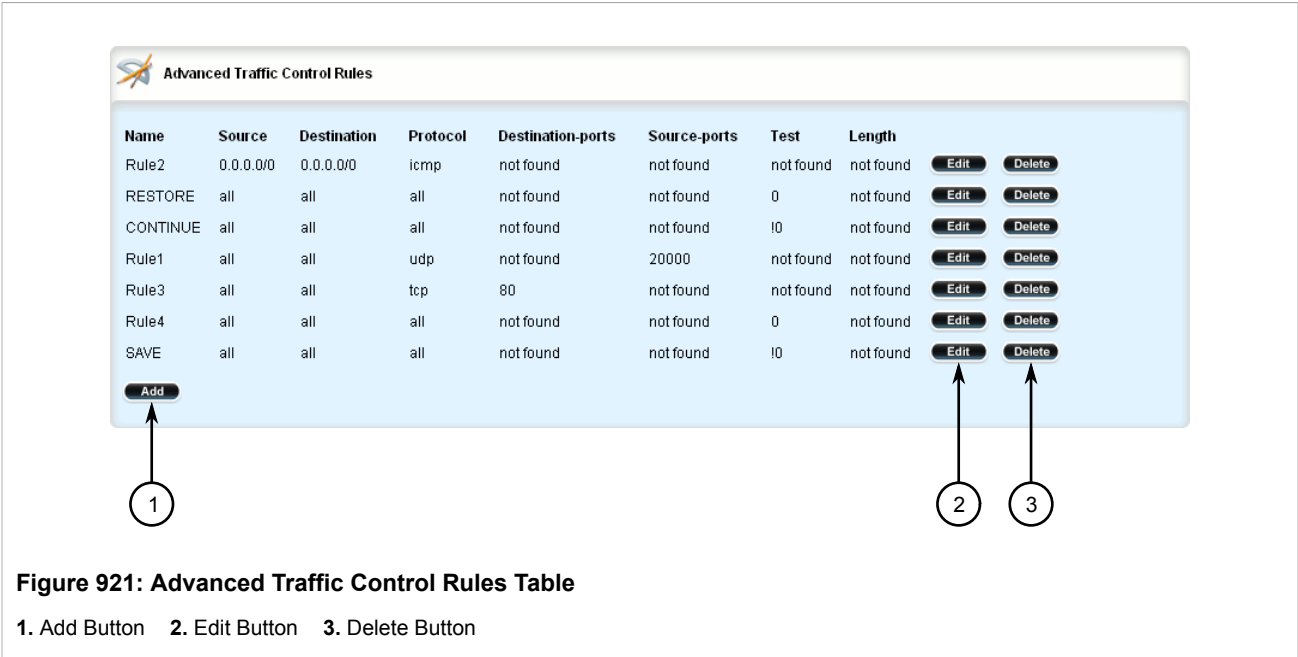
3. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
4. Click **Exit Transaction** or continue making changes.

Section 5.38.6.4

**Deleting aTraffic Control Rule**

To delete a traffic control rule, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **qos » traffic-control » advanced-configuration » tcrules**. The **Advanced Traffic Control Rules** table appears.



- Click **Delete** next to the chosen traffic control rule.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

Section 5.38.7

## Managing QoS Mapping for VLANs

Quality of Service (QoS) mapping is used to map QoS traffic. It assigns a traffic control mark to incoming IP traffic based on the priority value of a tagged frame. The incoming traffic is then classified and placed in the priority queues according to the traffic control rules specified for the marked rule. In addition, traffic control can assign the same priority or a different priority value when a frame needs to be egressed with a VLAN tag through a traffic control interface.

QoS maps can be configured for VLAN connections on routable Ethernet ports and virtual switches.

The following sections describe how to configure and manage QoS maps for VLAN connections:

- [Section 5.38.7.1, “Viewing a List of QoS Maps”](#)
- [Section 5.38.7.2, “Adding a QoS Map”](#)
- [Section 5.38.7.3, “Deleting a QoS Map”](#)

Section 5.38.7.1

### Viewing a List of QoS Maps

To view a list of QoS maps for a VLAN connection, navigate to either:

- For Switched Ethernet Ports**  
`switch » vlans » all-vlans » {id} » qosmap`, where *{id}* is the ID given to the VLAN.



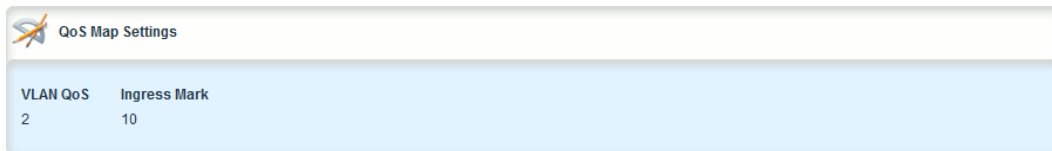
- **For Routable-Only Ethernet Ports**

**interface » eth » {name} » vlan » {id}**, where {name} is the name of the interface and {id} is the ID given to the VLAN.

- **For Virtual Switches**

**interface » virtualswitch » {id} » vlan » {vlan-id}**, where {id} is the ID of the virtual switch and {vlan-id} is the VLAN ID.

If QoS maps have been configured, the **QoS Map Settings** table appears.



VLAN QoS	Ingress Mark
2	10

**Figure 922: QoS Map Settings Table**

If no QoS maps have been configured, add maps as needed. For more information, refer to [Section 5.38.7.2, “Adding a QoS Map”](#).

#### Section 5.38.7.2

### Adding a QoS Map

To add a QoS map for a VLAN connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. In the case of a QoS map for a virtual switch, make sure the desired virtual switch has been configured. For more information, refer to [Section 3.23.2, “Adding a Virtual Switch”](#).
3. Navigate to either:
  - **For Switched Ethernet Ports**  
**switch » vlans » all-vlans » {id} » qosmap**, where {id} is the ID given to the VLAN.
  - **For Routable-Only Ethernet Ports**  
**interface » eth » {name} » vlan » {id} » qosmap**, where {name} is the name of the interface and {id} is the ID given to the VLAN.
  - **For Virtual Switches**  
**interface » virtualswitch » {id} » vlan » {vlan-id} » qosmap**, where {id} is the ID of the virtual switch and {vlan-id} is the VLAN ID.
4. Click **<Add qosmap>**. The **Key Settings** form appears.

**Figure 923: Key Settings Form**

1. VLAN QoS Box 2. Add Button

5. Configure the following parameter(s) as required:

Parameter	Description
VLAN QoS	<b>Synopsis:</b> An integer between 0 and 7 VLAN QoS, which is the priority in the VLAN header.

6. Click **Add** to create the new QoS Map. The **Qosmap** form appears.

**Figure 924: Qosmap Form**

1. Ingress Mark Box

7. Configure the following parameter(s) as required:

Parameter	Description
Ingress Mark	<b>Synopsis:</b> An integer between 0 and 255 Map the ingress to a mark.

8. Add an egress mark for the QoS map. For more information, refer to [Section 5.38.8.2, “Adding an Egress Mark”](#).
9. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
10. Click **Exit Transaction** or continue making changes.

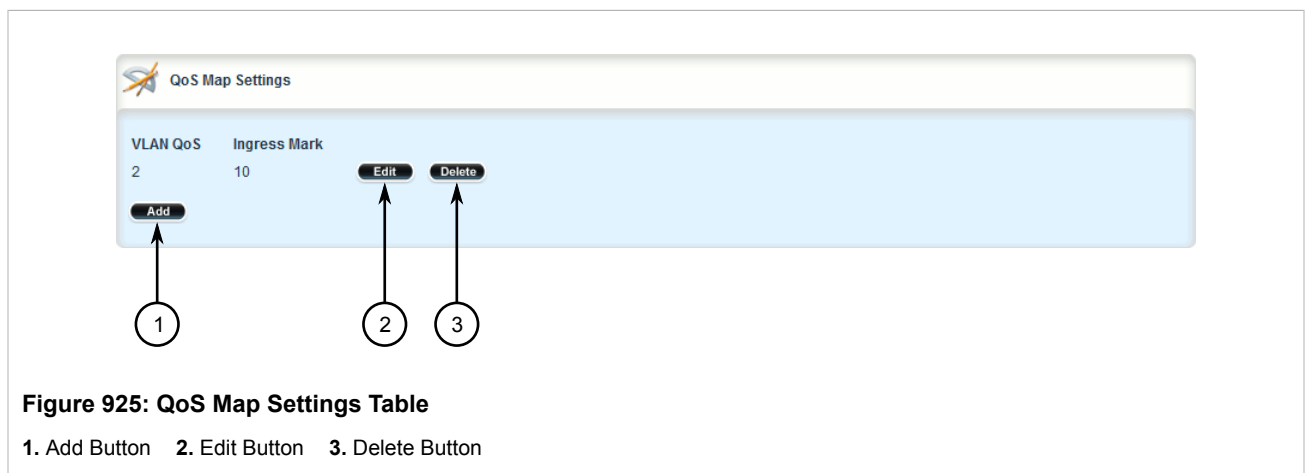
## Section 5.38.7.3

## Deleting a QoS Map

To delete a QoS map for a VLAN connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Switched Ethernet Ports**  
**switch » vlans » all-vlans » {id} » qosmap**, where {id} is the ID given to the VLAN.
  - **For Routable-Only Ethernet Ports**  
**interface » eth » {name} » vlan » {id} » qosmap**, where {name} is the name of the interface and {id} is the ID given to the VLAN.
  - **For Virtual Switches**  
**interface » virtualswitch » {id} » vlan » {vlan-id} » qosmap**, where {id} is the ID of the virtual switch and {vlan-id} is the VLAN ID.

The **QoS Map Settings** table appears.



**Figure 925: QoS Map Settings Table**

1. Add Button   2. Edit Button   3. Delete Button

3. Click **Delete** next to the chosen QoS map.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

## Section 5.38.8

## 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.

The following sections describe how to configure and manage egress markers for QoS maps:

- [Section 5.38.8.1, "Viewing a List of Egress Marks"](#)
- [Section 5.38.8.2, "Adding an Egress Mark"](#)
- [Section 5.38.8.3, "Deleting an Egress Mark"](#)

Section 5.38.8.1


# Viewing a List of Egress Marks

To view a list of egress marks for a QoS map, navigate to either:

Navigate to either:

- **For Switched Ethernet Ports**  
*switch » vlans » all-vlans » {id} » qosmap » {priority} » egress*, where {id} is the ID given to the VLAN and {priority} is the priority assigned to the QoS map.
- **For Routable-Only Ethernet Ports**  
*interface » eth » {name} » vlan » {id} » qosmap » {priority} » egress*, where:
  - {name} is the name of the interface
  - {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} » egress*, where:
  - {id} is the name of the interface
  - {vlan-id} is the ID given to the VLAN
  - {priority} is the priority assigned to the QoS map

If egress marks have been configured, the **Egress Marks Settings** table appears.



Egress Mark
10
11

Figure 926: Egress Marks Settings Table

If no egress marks have been configured, add egress marks as needed. For more information, refer to [Section 5.38.8.2, “Adding an Egress Mark”](#).

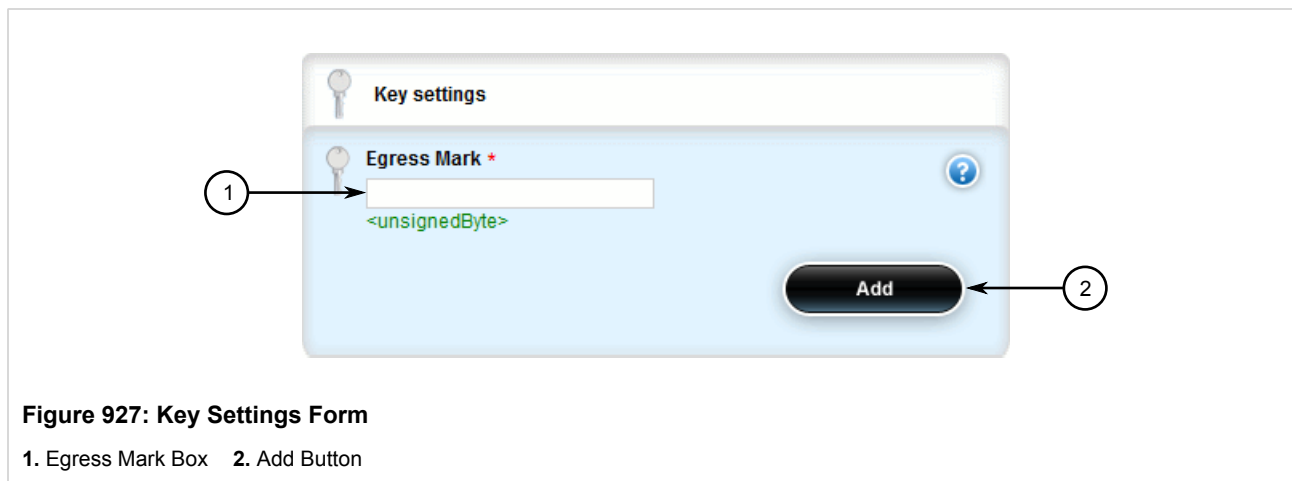
Section 5.38.8.2

# Adding an Egress Mark

To add an egress mark for a QoS Map, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Switched Ethernet Ports**  
*switch » vlans » all-vlans » {id} » qosmap » {priority} » egress*, where {id} is the ID given to the VLAN and {priority} is the priority assigned to the QoS map.
  - **For Routable-Only Ethernet Ports**  
*interface » eth » {name} » vlan » {id} » qosmap » {priority} » egress*, where:
    - {name} is the name of the interface

- *{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} » egress*, where:
    - *{id}* is the name of the interface
    - *{vlan-id}* is the ID given to the VLAN
    - *{priority}* is the priority assigned to the QoS map
3. Click **<Add egress>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
Egress Mark	<b>Synopsis:</b> An integer between 0 and 255 The mark value.

5. Click **Add** to create the new egress mark.
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

### Section 5.38.8.3

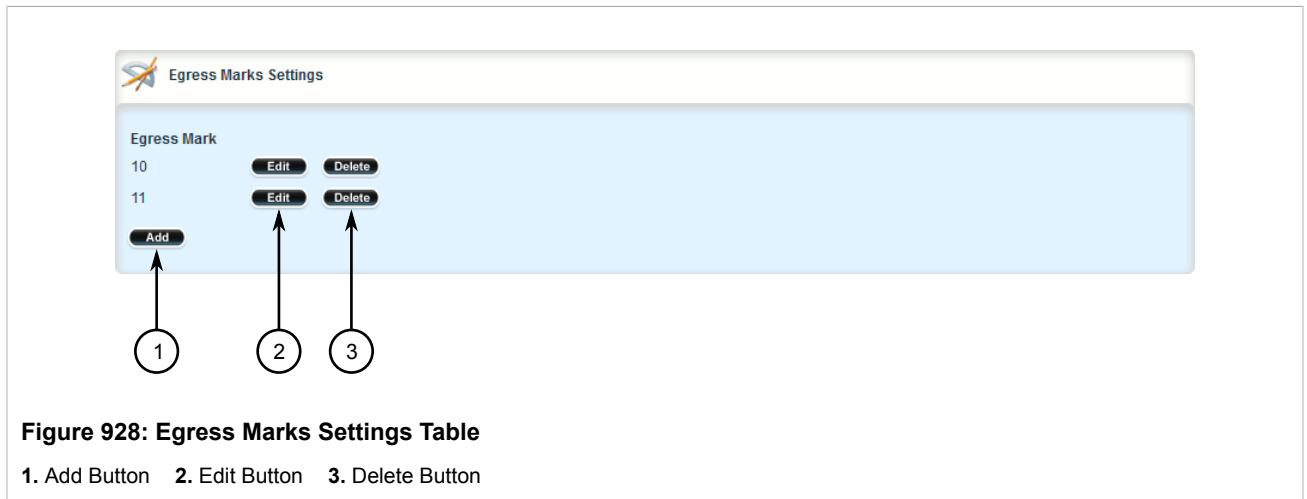
## Deleting an Egress Mark

To delete an egress mark for a QoS map, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
  - **For Switched Ethernet Ports**  
*switch » vlans » all-vlans » {id} » qosmap » {priority} » egress*, where *{id}* is the ID given to the VLAN and *{priority}* is the priority assigned to the QoS map.
  - **For Routable-Only Ethernet Ports**  
*interface » eth » {name} » vlan » {id} » qosmap » {priority} » egress*, where:

- *{name}* is the name of the interface
- *{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} » egress**, where:
  - *{id}* is the name of the interface
  - *{vlan-id}* is the ID given to the VLAN
  - *{priority}* is the priority assigned to the QoS map

The **Egress Marks Settings** table appears.



3. Click **Delete** next to the chosen egress mark.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.38.9

## 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.

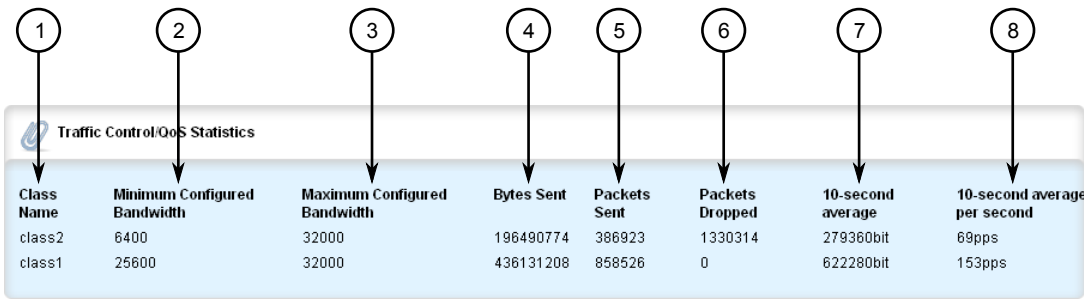
For more information about traffic control classes, refer to [Section 5.38.4, “Managing Traffic Control Classes”](#).



#### NOTE

*Statistics are only available when traffic control is enabled in advanced mode. For more information about enabling traffic control, refer to [Section 5.38.1, “Enabling and Configuring Traffic Control”](#).*

To view the QoS statistics, navigate to **qos » statistics**. The **QoS Statistics** table appears.



**Figure 929: QoS Statistics Table**

1. Class Name   2. Minimum Configured Bandwidth   3. Maximum Configured Bandwidth   4. Bytes Sent   5. Packages Sent  
6. Packages Dropped   7. 10-Second Average   8. 10-Second Average per Second

This table provides the following information:

Parameter	Description
Class Name	<b>Synopsis:</b> A string
Minimum Configured Bandwidth	<b>Synopsis:</b> A string The minimum guaranteed bandwidth. This is based on the device's defined characteristics.
Maximum Configured Bandwidth	<b>Synopsis:</b> A string The maximum guaranteed bandwidth in absence of any higher prioritized traffic. This is based on the device's defined characteristics.
Bytes Sent	<b>Synopsis:</b> A string The number of bytes that were sent through this class.
Packages Sent	<b>Synopsis:</b> A string The number of packets that were sent through this class.
Packages Dropped	<b>Synopsis:</b> A string The number of packets that were dropped in this class.
10-Second Average	<b>Synopsis:</b> A string Based on a 10-second average.
10-Second Average: Packages per Second	<b>Synopsis:</b> A string Based on a 10-second average.

Section 5.39

# Managing IP Addresses for Routable Interfaces

The following sections describe how to configure and manage IP addresses for routable interfaces:

- [Section 5.39.1, “Configuring Costing for Routable Interfaces”](#)
- [Section 5.39.2, “Viewing Statistics for Routable Interfaces”](#)
- [Section 5.39.3, “Managing IPv4 Addresses”](#)
- [Section 5.39.4, “Configuring IPv6 Neighbor Discovery”](#)

- [Section 5.39.5, “Managing IPv6 Network Prefixes”](#)
- [Section 5.39.6, “Managing IPv6 Addresses”](#)

Section 5.39.1

# Configuring Costing for Routable Interfaces

To configure the costing for a routable interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface}**, where {interface} is the name of the routable interface. The **Routable Interfaces** form appears.

**NOTE**  
The **VRF Forwarding** list is not available for the dummy interface.

**Figure 930: Routable Interfaces Form**

1. VRF Forwarding List    2. Auto-Cost Bandwidth Box

3. Configure the following parameter(s) as required:

Parameter	Description
Auto-Cost Bandwidth (kbps)	<b>Synopsis:</b> An integer between 1 and 10000000000 <b>Default:</b> 10000 This value is used in auto-cost calculations for this routable logical interface in kbps.

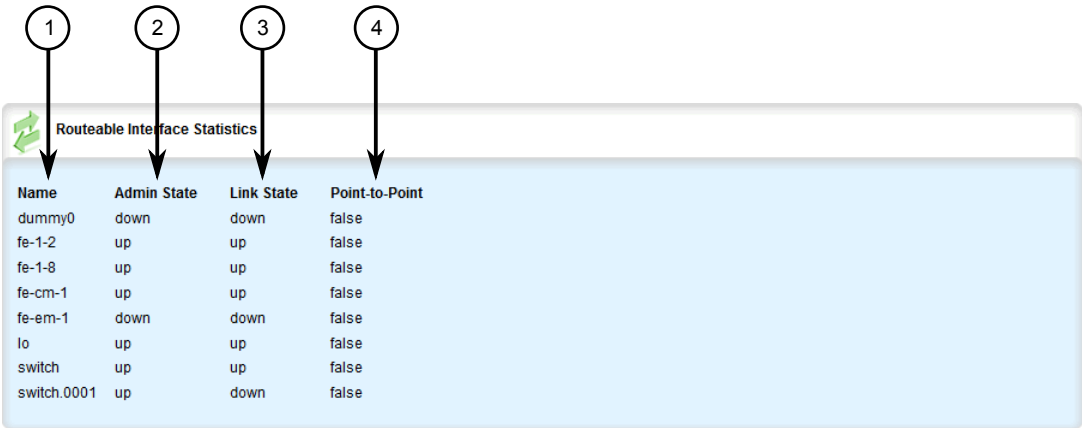
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.



Section 5.39.2

# Viewing Statistics for Routable Interfaces

To view basic statistics for all routable interfaces, navigate to *interfaces » ip*. The **Routeable Interface Statistics** form appears.



**Figure 931: Routeable Interface Statistics Form**  
1. Name    2. Admin State    3. Link State    4. Point-to-Point

This table displays the following information:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 15 characters long The name of the interface.
Admin State	<b>Synopsis:</b> { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status.
State	<b>Synopsis:</b> { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down.
Point-to-Point	<b>Synopsis:</b> true or false The point-to-point link.

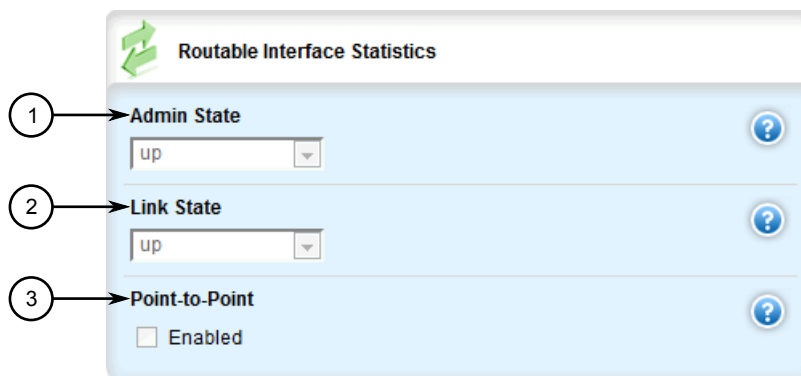
To view statistics for specific routable interfaces, navigate to *interfaces » ip » {interfaces}*, where *{interfaces}* is the name of the routable interface. The **Key Settings**, **Routeable Interface Statistics**, **Receive Statistics** and **Transmit Statistics** forms appear.



The image shows a 'Key settings' form with a key icon. A circled number 1 points to the 'Name' field, which contains the text 'fe-cm-1'. There is a red asterisk next to the field name and a help icon (question mark in a circle) to the right.

**Figure 932: Key Settings Form**

1. Name



The image shows a 'Routeable Interface Statistics' form with a green double arrow icon. It contains three sections: 'Admin State' with a dropdown menu showing 'up', 'Link State' with a dropdown menu showing 'up', and 'Point-to-Point' with an unchecked checkbox labeled 'Enabled'. Each section has a help icon (question mark in a circle) to its right. Circled numbers 1, 2, and 3 point to the Admin State, Link State, and Point-to-Point sections respectively.

**Figure 933: Routeable Interface Statistics Form**

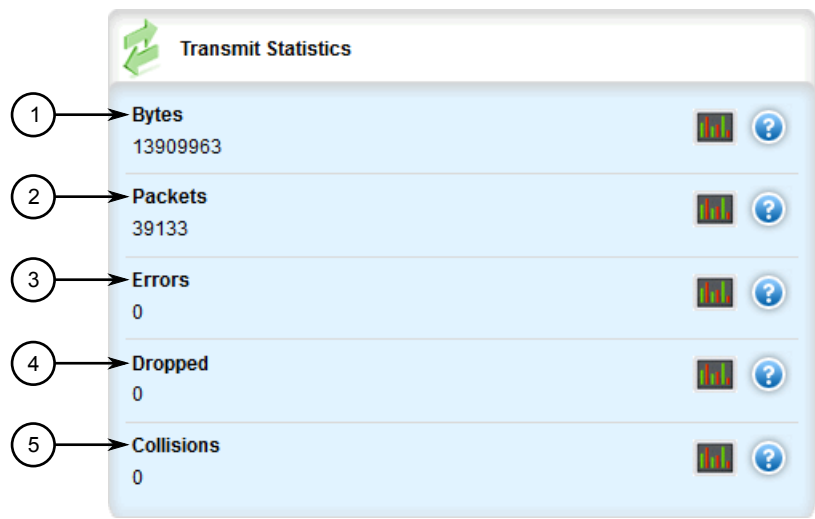
1. Admin State List   2. Link State List   3. Point-to-Point Check Box



The image shows a 'Receive Statistics' form with a green double arrow icon. It displays four statistics: 'Bytes' (34163186), 'Packets' (123429), 'Errors' (0), and 'Dropped' (54). Each statistic has a small bar chart icon and a help icon (question mark in a circle) to its right. Circled numbers 1, 2, 3, and 4 point to the Bytes, Packets, Errors, and Dropped rows respectively.

**Figure 934: Receive Statistics Form**

1. Bytes   2. Packets   3. Errors   4. Dropped



**Figure 935: Transmit Statistics Form**  
1. Bytes    2. Packets    3. Errors    4. Dropped    5. Collisions

These forms display the following information:

Parameter	Description
Name	<b>Synopsis:</b> A string 1 to 15 characters long The name of the interface.
Admin State	<b>Synopsis:</b> { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status.
State	<b>Synopsis:</b> { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down.
Point-to-Point	<b>Synopsis:</b> true or false The point-to-point link.
Bytes	The number of bytes received.
Packets	The number of packets received.
Errors	The number of error packets received.
Dropped	The number of packets dropped by the receiving device.
Bytes	The number of bytes transmitted.
Packets	The number of packets transmitted.
Errors	The number of error packets transmitted.
Dropped	The number of packets dropped by the transmitting device.
Collisions	The number of collisions detected on the port.

## Section 5.39.3

## Managing IPv4 Addresses


The following sections describe how to configure and manage IPv4 addresses:

- [Section 5.39.3.1, “Viewing a List of IPv4 Addresses”](#)
- [Section 5.39.3.2, “Adding an IPv4 Address”](#)
- [Section 5.39.3.3, “Deleting an IPv4 Address”](#)

## Section 5.39.3.1

### Viewing a List of IPv4 Addresses

To view a list of IPv4 address for a routable interface, navigate to **ip » {interface} » ipv4**, where *{interface}* is the name of the routable interface. If addresses have been configured, the **Addresses** table appears.



IP Address	Peer
192.168.0.2/24	not found

**Figure 936: Addresses Table**

If no addresses have been configured, add addresses as needed. For more information, refer to [Section 5.39.3.2, “Adding an IPv4 Address”](#).

## Section 5.39.3.2

### Adding an IPv4 Address

To add an IPv4 address to a routable interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface} » ipv4**, where *{interface}* is the name of the routable interface.
3. Click **<Add address>**. The **Key Settings** form appears.



Figure 937: Key Settings Form

1. Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string 9 to 18 characters long The IPv4/Prefix (xxx.xxx.xxx.xxx/xx).

5. Click **Add** to create the new address. The **Addresses** form appears.

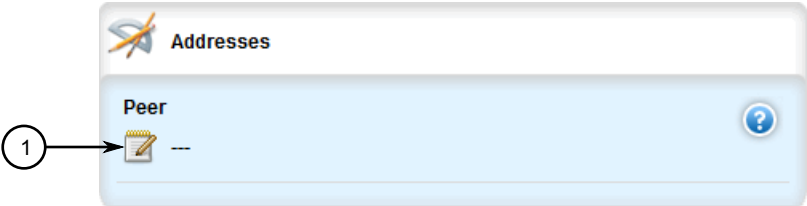


Figure 938: Addresses Form

1. Peer Box

6. Configure the following parameter(s) as required:

Parameter	Description
peer	<b>Synopsis:</b> A string 7 to 15 characters long The peer IPv4 Address (xxx.xxx.xxx.xxx, PPP, MLPPP, FrameRelay link only).

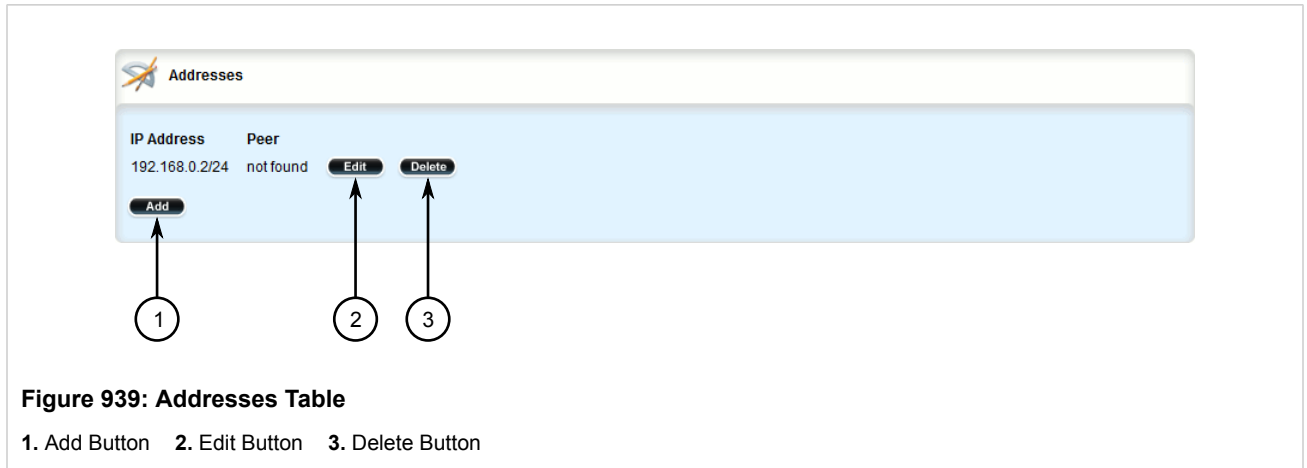
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

### Section 5.39.3.3

## Deleting an IPv4 Address

To delete an IPv4 address for a routable interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface} » ipv4**, where {interface} is the name of the routable interface. The **Addresses** table appears.



3. Click **Delete** next to the chosen address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

### Section 5.39.4

## 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. The goal is to find the link-layer of neighbor nodes on the same link.

- **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. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface} » ipv6 » nd**, where **{interface}** is the name of the routable interface. The **Router Advertisement Interval** and **Neighbor Discovery** forms appear.

Router Advertisement interval

Interval

Unit

1. Interval Box 2. Unit List

**Figure 940: Router Advertisement Interval Form**

1. Interval Box 2. Unit List

The screenshot shows the 'Neighbor Discovery' configuration form. It contains the following fields and callouts:

- 1. Enable Route Advertisement: Check box, currently 'Enabled'.
- 2. Set Advertisement Interval Option: Check box, currently 'Enabled'.
- 3. Set Home Agent Configuration Flag: Check box, currently 'Enabled'.
- 4. Home Agent Lifetime \*: Text box with a calendar icon, value '1800' (1800).
- 5. Home Agent Preference \*: Text box with a calendar icon, value '0' (0).
- 6. Set Managed Address Configuration Flag: Check box, currently 'Enabled'.
- 7. Set Other Statefull Configuration Flag: Check box, currently 'Enabled'.
- 8. Router Lifetime \*: Text box with a calendar icon, value '1800' (1800).
- 9. Reachable Time (Milliseconds) \*: Text box with a calendar icon, value '0' (0).

Figure 941: Neighbor Discovery Form

1. Enable Route Advertisement Check Box    2. Set Advertisement Interval Option Check Box    3. Set Home Agent Configuration Flag Check Box    4. Home Agent Lifetime Box    5. Home Agent Preference Box    6. Set Managed Address Configuration Flag Check Box    7. Set Other Statefull Configuration Flag Check Box    8. Router Lifetime Box    9. Reachable Time Box

3. On the **Router Advertisement Interval** form, configure the following parameter(s) as required:

Parameter	Description
Interval	<b>Synopsis:</b> An integer between 3 and 1800 The interval value. <b>Prerequisite:</b> The value cannot be specified unless the unit is also specified.
Unit	<b>Synopsis:</b> { sec, msec } The interval unit.



Parameter	Description
	<b>Prerequisite:</b> The unit cannot be specified unless the value is also specified.

4. On the **Neighbor Discovery** form, configure the following parameter(s) as required:

Parameter	Description
Enable Route Advertisement	<b>Synopsis:</b> typeless Enable to send router advertisement messages.
Set Advertisement Interval Option	<b>Synopsis:</b> typeless Includes an Advertisement Interval option which indicates to hosts the maximum time in milliseconds, between successive unsolicited router advertisements.
Set Home Agent Configuration Flag	<b>Synopsis:</b> typeless Sets/unsets the flag in IPv6 router advertisements which indicates to hosts that the router acts as a home agent and includes a home agent option.
Home Agent Lifetime	<b>Synopsis:</b> An integer between 0 and 65520 <b>Default:</b> 1800 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent lifetime to hosts. A value of 0 means to place a router lifetime value.
Home Agent Preference	<b>Synopsis:</b> An integer between 0 and 65535 <b>Default:</b> 0 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent preference to hosts.
Set Managed Address Configuration Flag	<b>Synopsis:</b> typeless The flag in IPv6 router advertisements, which indicates to hosts that they should use the managed (stateful) protocol for addresses autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.
Set Other Statefull Configuration Flag	<b>Synopsis:</b> typeless 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.
Router Lifetime	<b>Synopsis:</b> An integer between 0 and 9000 <b>Default:</b> 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 (Milliseconds)	<b>Synopsis:</b> An integer between 0 and 3600000 <b>Default:</b> 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 neighbors. The value zero means unspecified (by this router).

5. If required, add IPv6 network prefixes to the device can be advertised its neighbor. For more information on IPv6 network prefixes, refer to [Section 5.39.5, “Managing IPv6 Network Prefixes”](#).
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Click **Exit Transaction** or continue making changes.

Section 5.39.5

## Managing IPv6 Network Prefixes

An IPv6-capable interface can use Neighbor Discovery to advertise IPv6 network prefixes to its neighbor on the same link.

The following sections describe how to configure and manage IPv6 network prefixes:

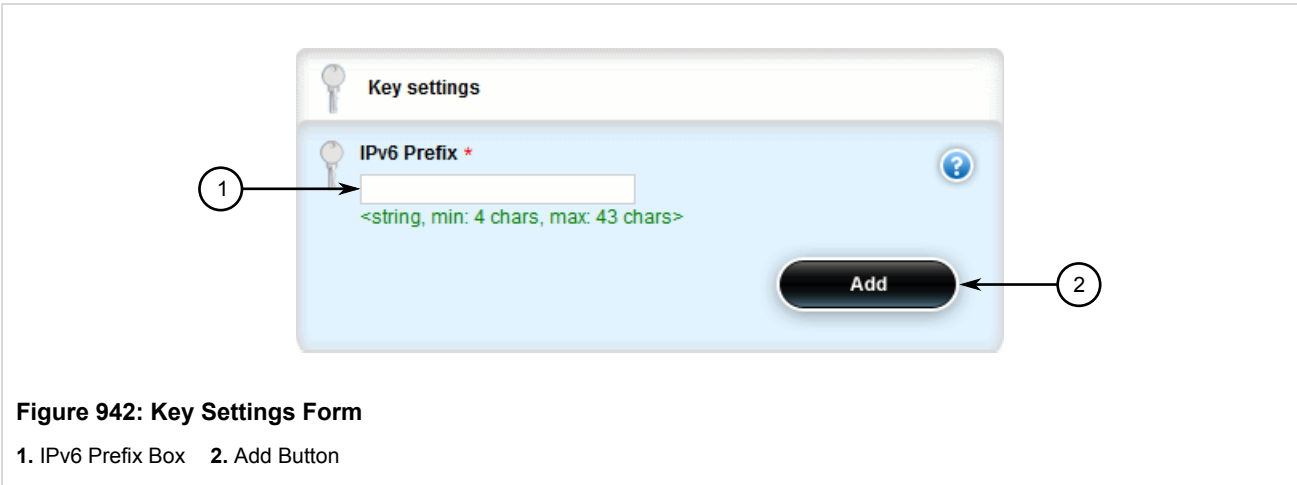
- [Section 5.39.5.1, “Adding an IPv6 Network Prefix”](#)
- [Section 5.39.5.2, “Deleting an IPv6 Network Prefix”](#)

Section 5.39.5.1

### Adding an IPv6 Network Prefix

To add a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface} » ipv6 » nd » prefix**, where *{interface}* is the name of the routable interface.
3. Click **<Add prefix>**. The **Key Settings** form appears.



4. Configure the following parameter(s) as required:

Parameter	Description
IPv6 Prefix	<b>Synopsis:</b> A string 4 to 43 characters long The IPv6 network/prefix.

5. Click **Add** to add the network prefix. The **Lifetime** and **Prefix** forms appear.

**Figure 943: Lifetime Form**  
1. Valid Lifetime Box    2. Preferred Lifetime Box

**Figure 944: Prefix Form**  
1. Off Link Check Box    2. No Autoconfig Check Box    3. Set Router Address Flag Check Box

6. On the **Lifetime** form, configure the following parameter(s) as required:

Parameter	Description
Valid Lifetime	<b>Synopsis:</b> { infinite } or an 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. <b>Prerequisite:</b> The valid lifetime cannot be configured unless the preferred lifetime is configured.
Preferred Lifetime	<b>Synopsis:</b> { infinite } or an integer between 0 and 4294967295 The length of time in seconds during which addresses generated from the prefix remain preferred. <b>Prerequisite:</b> The preferred lifetime cannot be configured unless the valid lifetime is configured.

7. On the **Prefix** form, configure the following parameter(s) as required:

Parameter	Description
Off Link	<b>Synopsis:</b> typeless

Parameter	Description
	Indicates that advertisement makes no statement about on-link or off-link properties of the prefix.
No Autoconfig	<b>Synopsis:</b> typeless Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
Set Router Address Flag	<b>Synopsis:</b> typeless Indicates to hosts on the local link that the specified prefix contains a complete IP address by setting the R flag. <b>Prerequisite:</b> The router address can not be set unless off-link or no-autoconfig are set.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.39.5.2

### Deleting an IPv6 Network Prefix

To delete a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to **ip » {interface} » ipv6 » nd » prefix**, where *{interface}* is the name of the routable interface.
- In the menu, click the - symbol next to chosen network prefix to delete it.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.39.6

### Managing IPv6 Addresses

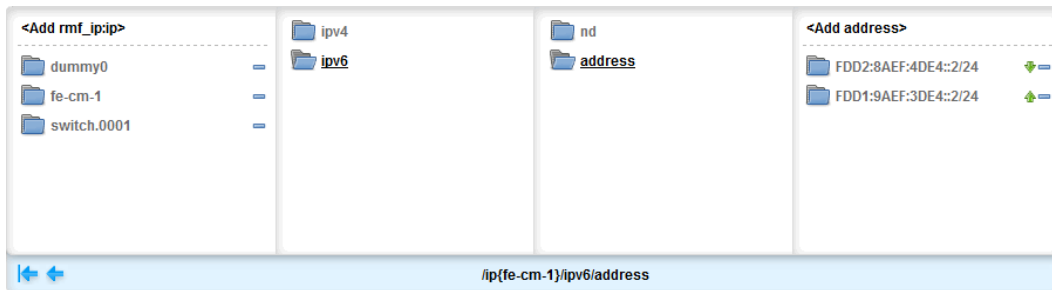
The following sections describe how to configure and manage IPv6 addresses:

- [Section 5.39.6.1, “Viewing a List of IPv6 Addresses”](#)
- [Section 5.39.6.2, “Adding an IPv6 Address”](#)
- [Section 5.39.6.3, “Deleting an IPv6 Address”](#)

#### Section 5.39.6.1

### Viewing a List of IPv6 Addresses

To view a list of IPv6 address for a routable interface, navigate to **ip » {interface} » ipv6 » address**, where *{interface}* is the name of the routable interface. If addresses have been configured, they are listed in the menu.



**Figure 945: IPv6 Address Menu**

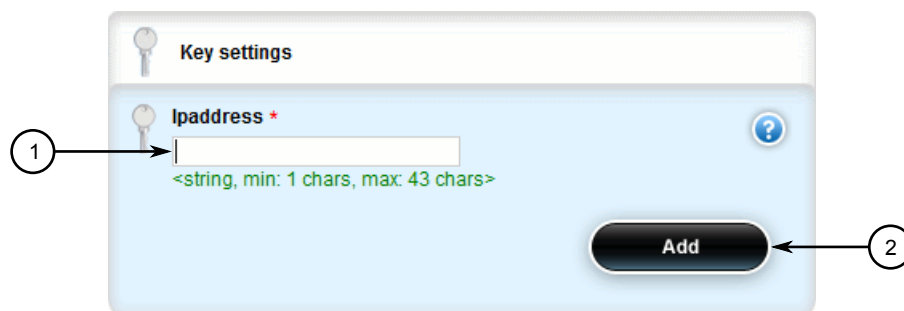
If no addresses have been configured, add addresses as needed. For more information, refer to [Section 5.39.6.2, “Adding an IPv6 Address”](#).

#### Section 5.39.6.2

### Adding an IPv6 Address

To add an IPv6 address to a routable interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface} » ipv6 » address**, where *{interface}* is the name of the routable interface.
3. Click **<Add address>**. The **Key Settings** form appears.



**Figure 946: Key Settings Form**

1. Address Box    2. Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
IP Address	<b>Synopsis:</b> A string 4 to 43 characters long The IPv6 address/prefix of this interface.

5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.

Section 5.39.6.3

## Deleting an IPv6 Address

To delete an IPv6 address for a routable interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **ip » {interface} » ipv6 » address**, where *{interface}* is the name of the routable interface.
3. Click - symbol in the menu next to the chosen address.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

Section 5.40

## 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 it operates on a pre-configured LSPs (Label Switch Paths) that are built based on the dynamic Label Distribution Protocol (LDP), or through static label bindings.

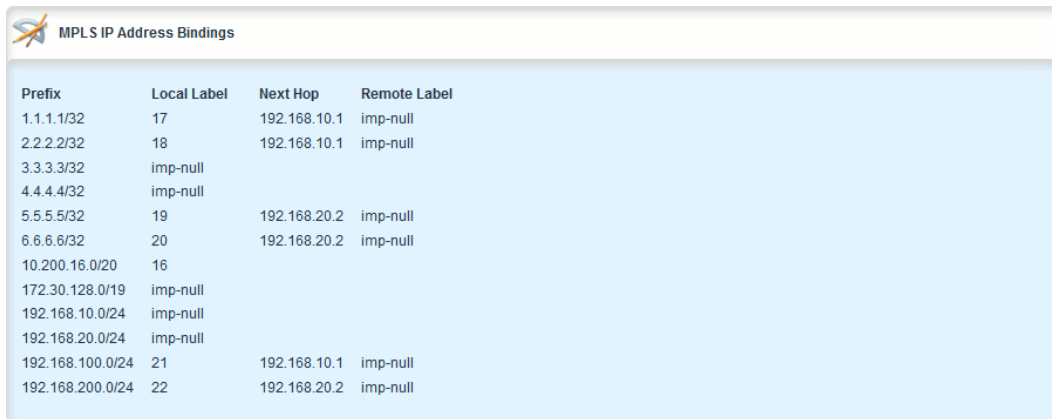
The following sections describe how to configure and manage MPLS:

- [Section 5.40.1, “Viewing the Status of IP Binding”](#)
- [Section 5.40.2, “Viewing the Status of the Forwarding Table”](#)
- [Section 5.40.3, “Enabling/Disabling MPLS Routing”](#)
- [Section 5.40.4, “Managing the MPLS Interfaces”](#)
- [Section 5.40.5, “Managing Static Label Binding”](#)
- [Section 5.40.6, “Managing Static Cross-Connects”](#)
- [Section 5.40.7, “Managing LDP”](#)

Section 5.40.1

### Viewing the Status of IP Binding

To view the status of the IP binding on the device, navigate to **mpls » status » ip-binding**. If IP binding has been configured, the **MPLS IP Address Bindings** table appears.



The screenshot shows a web interface window titled "MPLS IP Address Bindings". It contains a table with four columns: Prefix, Local Label, Next Hop, and Remote Label. The table lists 14 entries with various IP prefixes and their corresponding labels and next hops.

Prefix	Local Label	Next Hop	Remote 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

**Figure 947: MPLS IP Address Bindings Table**

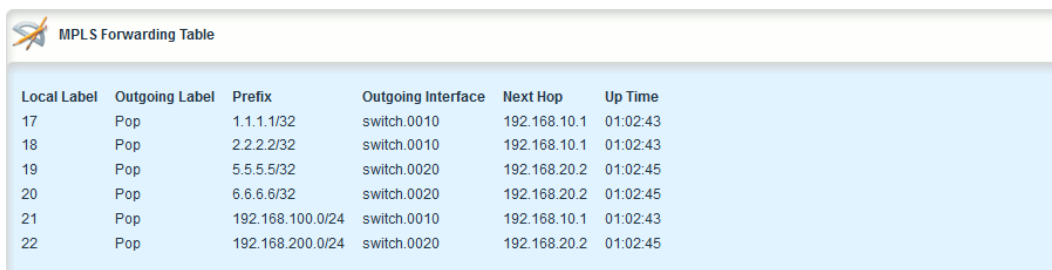
This table provides the following information:

Parameter	Description
Prefix	<b>Synopsis:</b> A string The destination address prefix.
Local Label	<b>Synopsis:</b> A string The incoming (local) label.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.
Remote Label	<b>Synopsis:</b> A string The remote label

## Section 5.40.2

# Viewing the Status of the Forwarding Table

To view the status of the forwarding table on the device, navigate to *mpls » status » forwarding-table*, the **MPLS Forwarding Table** appears.



The screenshot shows a web interface window titled "MPLS Forwarding Table". It contains a table with six columns: Local Label, Outgoing Label, Prefix, Outgoing Interface, Next Hop, and Up Time. The table lists 7 entries showing the status of various MPLS forwarding entries.

Local Label	Outgoing Label	Prefix	Outgoing Interface	Next Hop	Up Time
17	Pop	1.1.1.1/32	switch.0010	192.168.10.1	01:02:43
18	Pop	2.2.2.2/32	switch.0010	192.168.10.1	01:02:43
19	Pop	5.5.5.5/32	switch.0020	192.168.20.2	01:02:45
20	Pop	6.6.6.6/32	switch.0020	192.168.20.2	01:02:45
21	Pop	192.168.100.0/24	switch.0010	192.168.10.1	01:02:43
22	Pop	192.168.200.0/24	switch.0020	192.168.20.2	01:02:45

**Figure 948: MPLS Forwarding Table**

This table provides the following information:

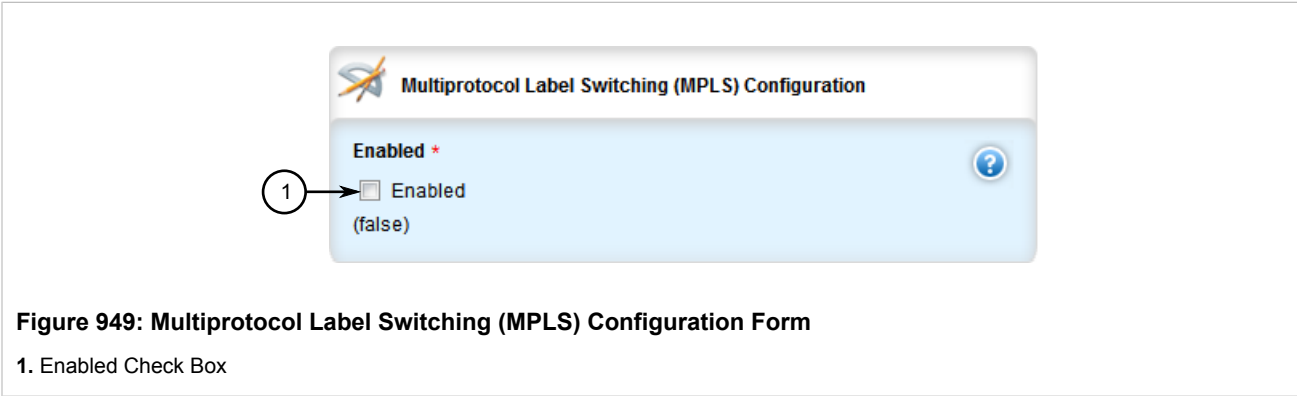
Parameter	Description
Local Label	<b>Synopsis:</b> A string The incoming (local) label
Outgoing Label	<b>Synopsis:</b> A string The outgoing (remote) label.
Prefix	<b>Synopsis:</b> A string The destination address prefix.
Outgoing Interface	<b>Synopsis:</b> A string The outgoing interface.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.
Up Time	<b>Synopsis:</b> A string The time this entry has been up.

Section 5.40.3

# Enabling/Disabling MPLS Routing

To enable MPLS routing, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *mpls*. The **Multiprotocol Label Switching (MPLS) Configuration** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Enable MPLS	<b>Synopsis:</b> true or false <b>Default:</b> false A boolean flag to indicate that MPLS forwarding of IP packets is enabled.

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.



## Section 5.40.4

## Managing the MPLS Interfaces

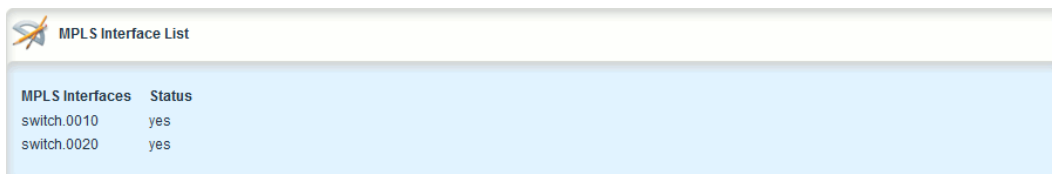
The following sections describe how to manage the MPLS interfaces:

- [Section 5.40.4.1, “Viewing the Status of MPLS Interfaces”](#)
- [Section 5.40.4.2, “Viewing a List of MPLS Interfaces”](#)
- [Section 5.40.4.3, “Enabling/Disabling an MPLS Interface”](#)

## Section 5.40.4.1

### Viewing the Status of MPLS Interfaces

To view the status of the MPLS interfaces on the device, navigate to ***mpls » status » interfaces***. If MPLS interfaces have been enabled on the device, the **MPLS Status Interface List** table appears.



MPLS Interfaces	Status
switch.0010	yes
switch.0020	yes

**Figure 950: MPLS Status Interface List Table**

This table provides the following information:

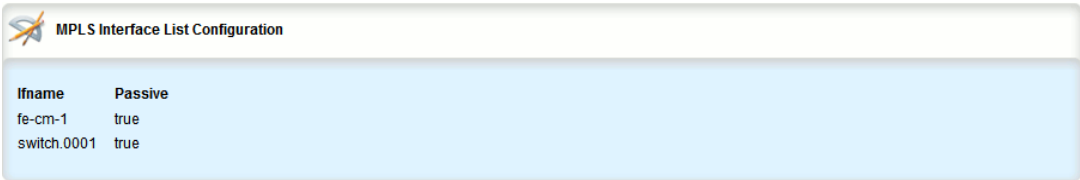
Parameter	Description
MPLS Interfaces	<b>Synopsis:</b> A string The interface that has been enabled for MPLS.
Status	<b>Synopsis:</b> A string The operational status.

If no MPLS interface has been enabled, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to [Section 5.40.4.3, “Enabling/Disabling an MPLS Interface”](#).

## Section 5.40.4.2

### Viewing a List of MPLS Interfaces

To view a list of MPLS interfaces, navigate to ***mpls » interface-mpls***. If MPLS interfaces have been configured, the **MPLS Interface List Configuration** table appears.



The image shows a screenshot of the 'MPLS Interface List Configuration' window. It contains a table with two columns: 'Ifname' and 'Passive'. The table has two rows of data: 'fe-cm-1' with 'true' and 'switch.0001' with 'true'.

Ifname	Passive
fe-cm-1	true
switch.0001	true

Figure 951: MPLS Interface List Configuration Table

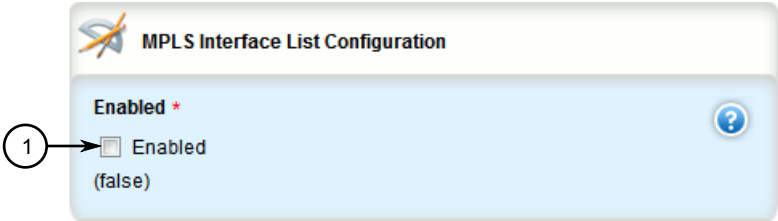
If no MPLS interfaces have been configured, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to [Section 5.40.4.3, “Enabling/Disabling an MPLS Interface”](#).

Section 5.40.4.3

Enabling/Disabling an MPLS Interface

To enable or disable an MPLS interface, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *mpls » interface-mpls » {interface}* where {interface} is the name of the interface to enable or disable for MPLS. The **MPLS Interface List Configuration** form appears.



The image shows a screenshot of the 'MPLS Interface List Configuration' form. A circled number '1' points to a checkbox labeled 'Enabled' with '(false)' below it. The form title is 'MPLS Interface List Configuration'.

Figure 952: MPLS Interface List Configuration Form

1. Enable Check Box

- 3. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false A boolean flag to indicate Multiprotocol Label Switching (MPLS) forwarding of IP packets is enabled on this interface.

- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.

## Section 5.40.5

## Managing Static Label Binding

The following sections describe how to configure and manage static label binding for MPLS:

- [Section 5.40.5.1, “Viewing the Status of Static Label Binding”](#)
- [Section 5.40.5.2, “Viewing a List of Static Labels”](#)
- [Section 5.40.5.3, “Adding a Static Label”](#)
- [Section 5.40.5.4, “Deleting a Static Label”](#)

## Section 5.40.5.1

### Viewing the Status of Static Label Binding

To view the status of all configured static label binding, navigate to **mpls » status » static-binding**. If static label binding has been configured, the **Static MPLS IP Address Bindings** table appears.



The screenshot shows a web interface window titled "Static MPLS IP Address Bindings". Inside the window is a table with the following data:

IP Address	In Label	Out Label	Next Hop
192.168.20.0/24	90	101	192.168.10.2
192.168.200.0/24	95	100	192.168.10.2

**Figure 953: Static MPLS IP Address Bindings Table**

This table provides the following information:

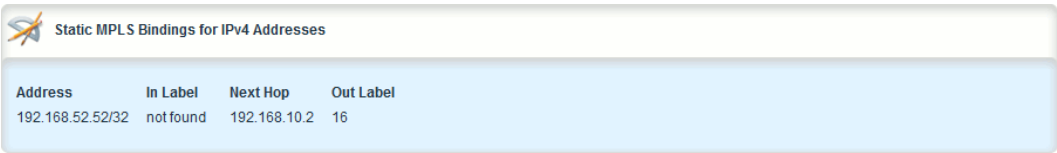
Parameter	Description
IP Address	<b>Synopsis:</b> A string The destination address prefix.
In Label	<b>Synopsis:</b> A string The incoming (local) label.
Out Label	<b>Synopsis:</b> A string The outgoing (remote) label.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.

If no static label binding has been configured, configure binding as needed. For more information about configuring static-binding, refer to [Section 5.40.5.3, “Adding a Static Label”](#).

## Section 5.40.5.2

### Viewing a List of Static Labels

To view a list of static labels, navigate to **mpls » static-mpls » binding » {protocol}**, where *{protocol}* is either *ipv4* or *ipv6*. If static labels have been configured, the **Static MPLS Bindings for IPv4 Addresses** or **Static MPLS Bindings for IPv6 Addresses** table appears.



Address	In Label	Next Hop	Out Label
192.168.52.52/32	not found	192.168.10.2	16

Figure 954: Static MPLS Bindings for IPv4 Addresses Table (Example)

If no static labels have been configured, add labels as needed. For more information about adding static labels, refer to [Section 5.40.5.3, “Adding a Static Label”](#).

Section 5.40.5.3  
**Adding a Static Label**

To add a static label, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *mpls » static-mpls » binding » {protocol}*, where *{protocol}* is either *ipv4* or *ipv6*.
- 3. Click **<Add dest-address>** in the menu. The **Key Settings** form appears.



**NOTE**  
*A route to the destination address must already be present in the routing table.*



Figure 955: Key Settings Form

1. Address Box    2. Add Button

- 4. Configure the following parameter(s) as required:

Parameter	Description
Address	<b>Synopsis:</b> A string 9 to 18 characters long The destination address/prefix. <b>Prerequisite:</b> LDP must be disabled before declaring MPLS label bindings.

- 5. Click **Add** to apply the static label to the destination address. The **Static MPLS Bindings for IPv4 Addresses** or **Static MPLS Bindings for IPv6 Addresses** form appears.

Static MPLS Bindings for IPv4 Addresses

1. In Label U

2. Next Hop

3. Out Label

Figure 956: Static MPLS Bindings for IPv4 Addresses Form (Example)

1. In Label Box    2. Next Hop Box    3. Out Label Box

6. Configure the following parameter(s) as required:

Parameter	Description
In Label	<b>Synopsis:</b> An integer between 16 and 1048575 The incoming label: integer 16 -> 1048575.
Next Hop	<b>Synopsis:</b> A string 7 to 15 characters long The IP address for the destination next-hop router. <b>Prerequisite:</b> The destination out-label must also be defined.
Out Label	<b>Synopsis:</b> { explicit-null, implicit-null } or an integer between 16 and 1048575 The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575.  The outgoing label: <itemizedlist><listitem><emphasis>implicit null</emphasis> - 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</listitem><listitem><emphasis>explicit null</emphasis> - 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</listitem></itemizedlist> <b>Prerequisite:</b> The destination next-hop must also be defined.

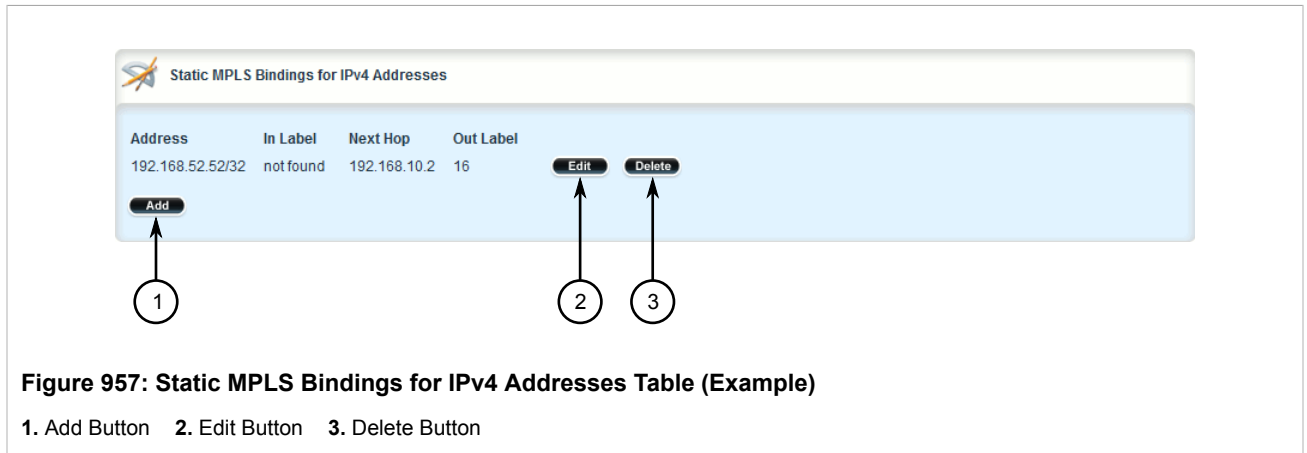
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
8. Click **Exit Transaction** or continue making changes.

Section 5.40.5.4

### Deleting a Static Label

To delete a static label, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **mpls » static-mpls » binding » {protocol}**, where *{protocol}* is either *ipv4* or *ipv6*. The **Static MPLS Bindings for IPv4 Addresses** or **Static MPLS Bindings for IPv6 Addresses** table appears.



3. Click **Delete** next to the chosen static label.
4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.40.6

## 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).

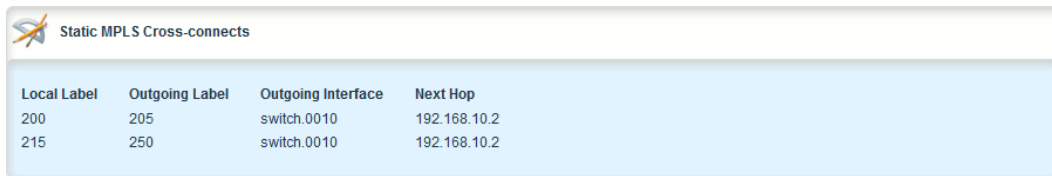
The following sections describe how to configure and manage static cross-connects for MPLS:

- [Section 5.40.6.1, “Viewing the Status of Static Cross-Connects”](#)
- [Section 5.40.6.2, “Viewing a List of Static Cross-Connects”](#)
- [Section 5.40.6.3, “Adding a Static Cross-Connect”](#)
- [Section 5.40.6.4, “Deleting a Static Cross-Connect”](#)

#### Section 5.40.6.1

### Viewing the Status of Static Cross-Connects

To view the status of all configured static cross-connects, navigate to **mpls » status » static-crossconnect**. If static cross-connects have been configured, the **Static MPLS Cross-connects** table appears.



The image shows a screenshot of the 'Static MPLS Cross-connects' table in a web interface. The table has four columns: Local Label, Outgoing Label, Outgoing Interface, and Next Hop. It contains two rows of data.

Local Label	Outgoing Label	Outgoing Interface	Next Hop
200	205	switch.0010	192.168.10.2
215	250	switch.0010	192.168.10.2

**Figure 958: Static MPLS Cross-connects Table**

This table provides the following information:

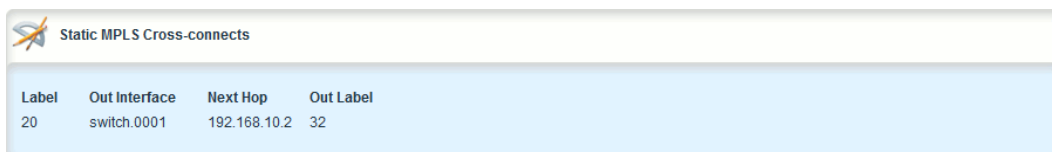
Parameter	Description
Local Label	<b>Synopsis:</b> A string The incoming (local) label.
Outgoing Label	<b>Synopsis:</b> A string The outgoing (remote) label.
Outgoing Interface	<b>Synopsis:</b> A string The outgoing interface.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to [Section 5.40.6.3, “Adding a Static Cross-Connect”](#).

#### Section 5.40.6.2

### Viewing a List of Static Cross-Connects

To view a list of configured static cross-connects, navigate to *mpls » static-mpls » crossconnect*. If cross-connect labels have been configured, the **Static MPLS Cross-Connects** table appears.



The image shows a screenshot of the 'Static MPLS Cross-Connects' table in a web interface. The table has four columns: Label, Out Interface, Next Hop, and Out Label. It contains one row of data.

Label	Out Interface	Next Hop	Out Label
20	switch.0001	192.168.10.2	32

**Figure 959: Static MPLS Cross-Connects Table**

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to [Section 5.40.6.3, “Adding a Static Cross-Connect”](#).

#### Section 5.40.6.3

### Adding a Static Cross-Connect

To add a static cross-connect, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

- Navigate to **mpls » static-mpls » crossconnect** and click **<Add dest-address>**. The **Key Settings** form appears.

**Figure 960: Key Settings Form**

1. Label Box 2. Add Button

- Configure the following parameter(s) as required:

Parameter	Description
label	<b>Synopsis:</b> An integer between 16 and 1048575 The incoming label.

- Click **Add** to add the cross-connect label. The **Static MPLS Cross-Connects** form appears.

**Figure 961: Static MPLS Cross-Connects Form**

1. Out Interface List 2. Next Hop Box 3. Out Label Box

- Configure the following parameter(s) as required:

Parameter	Description
Out Interface	The outgoing interface.
Next Hop	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long



Parameter	Description
	The destination next-hop router (IPv4 or IPv6 format).
Out Label	<b>Synopsis:</b> { explicit-null, implicit-null } or an integer between 16 and 1048575 The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575.

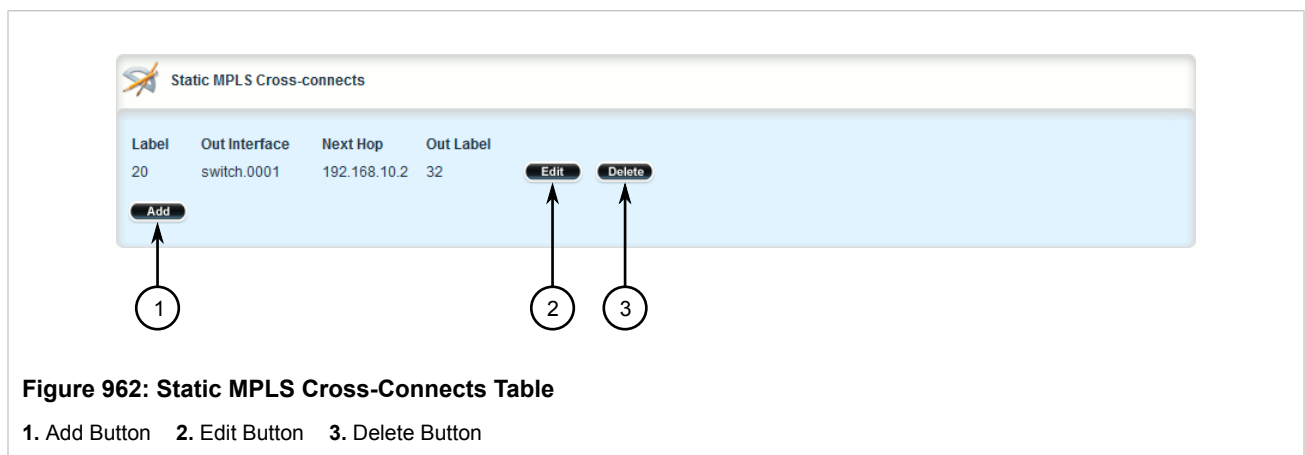
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.40.6.4

## Deleting a Static Cross-Connect

To delete a static cross-connect, do the following:

- Change the mode to **Edit Private** or **Edit Exclusive**.
- Navigate to *mpls » static-mpls » crossconnect*. The **Static MPLS Cross-Connects** table appears.



- Click **Delete** next to the chosen cross-connect label.
- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

## Section 5.40.7

## Managing LDP

LDP (Label Distribution Protocol), defined by [RFC 5036](http://tools.ietf.org/html/rfc5036) [http://tools.ietf.org/html/rfc5036], is a protocol that enables an MPLS capable router to exchange MPLS label information. The labels are distributed in both directions so that an LSP (Label Switched Path) can be established and managed within an MPLS network dynamically, as opposed to configuring static routes. LDP takes advantage of already established routing information (using OSPF or IS-IS) to distribute label information amongst the MPLS enabled routers).

LDP works by enabling Label Switch Routers (LSRs) to discover and bind labels to their neighbors within the MPLS network. The LSRs then identify their peers and exchange their label information with one another. Label information is stored in Label Information Base (LIB) and Label Forwarding Information Base (LFIB) tables.

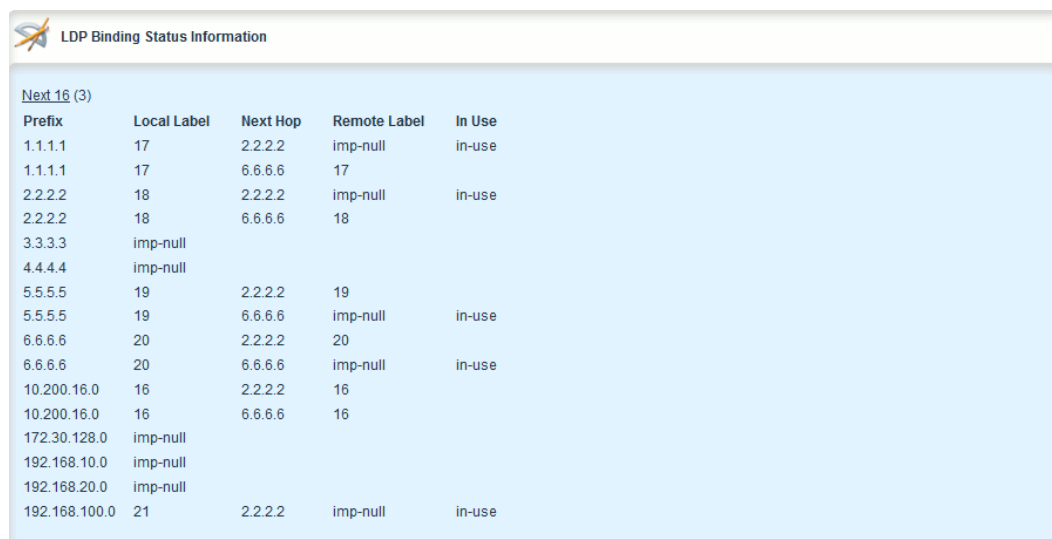
The following sections describe how to configure and manage LDP:

- [Section 5.40.7.1, “Viewing the Status of LDP Binding”](#)
- [Section 5.40.7.2, “Viewing the Status of the LDP Discovery Interfaces”](#)
- [Section 5.40.7.3, “Viewing the Status of the LDP Neighbor Local Node Information”](#)
- [Section 5.40.7.4, “Viewing the Status of the LDP Neighbor Connection Information”](#)
- [Section 5.40.7.5, “Viewing the Status of the LDP Neighbor Discovery Information”](#)
- [Section 5.40.7.6, “Configuring LDP”](#)
- [Section 5.40.7.7, “Configuring Neighbor Discovery”](#)
- [Section 5.40.7.8, “Viewing a List of LDP Interfaces”](#)
- [Section 5.40.7.9, “Enabling/Disabling an LDP Interface”](#)

#### Section 5.40.7.1

### Viewing the Status of LDP Binding

To view the status of the LDP binding on the device, navigate to ***mpls » ldp » status » binding***. If LDP interfaces have been configured, the **LDP Binding Status Information** table appears.



The screenshot shows a web interface window titled "LDP Binding Status Information". Inside, there is a table with 5 columns: Prefix, Local Label, Next Hop, Remote Label, and In Use. The table contains 16 rows of data. A link "Next 16 (3)" is visible above the table.

Prefix	Local Label	Next Hop	Remote 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
6.6.6.6	20	2.2.2.2	20	
6.6.6.6	20	6.6.6.6	imp-null	in-use
10.200.16.0	16	2.2.2.2	16	
10.200.16.0	16	6.6.6.6	16	
172.30.128.0	imp-null			
192.168.10.0	imp-null			
192.168.20.0	imp-null			
192.168.100.0	21	2.2.2.2	imp-null	in-use

**Figure 963: LDP Binding Status Information Table**

This table provides the following information:

Parameter	Description
Prefix	<b>Synopsis:</b> A string The LDP transport prefix.
Local Label	<b>Synopsis:</b> A string

Parameter	Description
	The incoming (local) label.
Next Hop	<b>Synopsis:</b> A string The destination next hop router.
Remote Label	<b>Synopsis:</b> A string The LDP remote label.
In Use	<b>Synopsis:</b> A string The LDP in-use flag.

## Section 5.40.7.2

## Viewing the Status of the LDP Discovery Interfaces

To view the status of the LDP discovery interfaces on the device, navigate to *mpls » ldp » status » discovery » interfaces*. If LDP interfaces have been configured, the **LDP Discovery Interfaces Status Information** table appears.



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

**Figure 964: LDP Discovery Interfaces Status Information Table**

This table provides the following information:

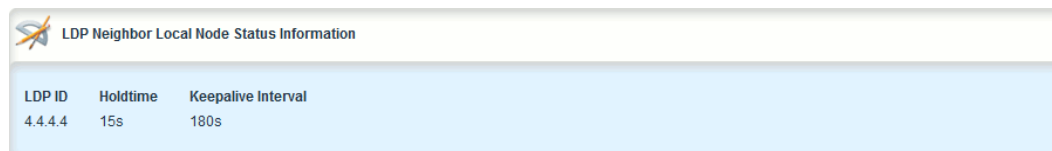
Parameter	Description
Interface	<b>Synopsis:</b> A string The LDP discovery interface.
Src IP Addr	<b>Synopsis:</b> A string The LDP discovery source IP address.
Peer ID	<b>Synopsis:</b> A string The LDP discovery peer ID.
Peer IP	<b>Synopsis:</b> A string LDP discovery peer IP address
State	<b>Synopsis:</b> A string The LDP discovery interface state.

For more information about configuring LDP discovery interfaces, refer to [Section 5.40.7.9, “Enabling/Disabling an LDP Interface”](#).

## Section 5.40.7.3

## Viewing the Status of the LDP Neighbor Local Node Information

To view the status of the local node(s) for the LDP neighbor on the device, navigate to ***mpls » ldp » status » neighbor » local-node-information***. The **LDP Neighbor Local Node Status Information** table appears.



LDP ID	Holdtime	Keepalive Interval
4.4.4.4	15s	180s

**Figure 965: LDP Neighbor Local Node Status Information Table**

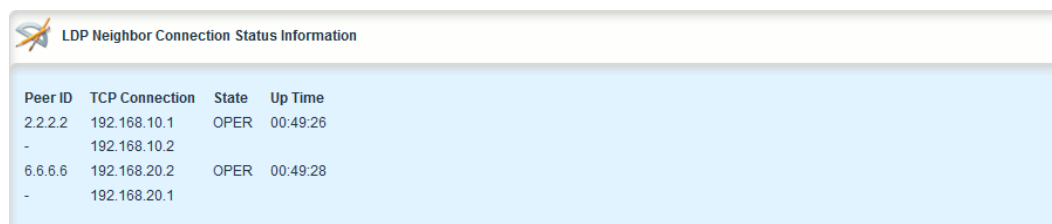
This table provides the following information:

Parameter	Description
LDP ID	<b>Synopsis:</b> A string The LDP ID of the neighbor local node.
Hello Holdtime	<b>Synopsis:</b> A string LDP hello holdtime of the neighbor local node.
Session Holdtime	<b>Synopsis:</b> A string The LDP session holdtime of the neighbor local node.

## Section 5.40.7.4

## Viewing the Status of the LDP Neighbor Connection Information

To view the status of the LDP neighbor connection on the device, navigate to ***mpls » ldp » status » neighbor » connection-information***. The **LDP Neighbor Connection Status Information** table appears.



Peer ID	TCP Connection	State	Up Time
2.2.2.2	192.168.10.1	OPER	00:49:26
-	192.168.10.2		
6.6.6.6	192.168.20.2	OPER	00:49:28
-	192.168.20.1		

**Figure 966: LDP Neighbor Connection Status Information Table**

This table provides the following information:

Parameter	Description
Peer ID	<b>Synopsis:</b> A string The peer ID of the LDP neighbor connection.
TCP Connection	<b>Synopsis:</b> A string The TCP connection of the LDP neighbor connection.

Parameter	Description
state	<b>Synopsis:</b> A string The state of the LDP neighbor connection.
Up Time	<b>Synopsis:</b> A string The up time of the LDP neighbor connection.

## Section 5.40.7.5

## Viewing the Status of the LDP Neighbor Discovery Information

To view the status of the LDP neighbor discovery information on the device, navigate to **mpls » ldp » status » neighbor » discovery-information**. The **LDP Neighbor Discovery Status Information** table appears.



Peer ID	Peer IP	Interface	Local IP	P Holdtime	P Keepalive 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

**Figure 967: LDP Neighbor Discovery Status Information Table**

This table provides the following information:

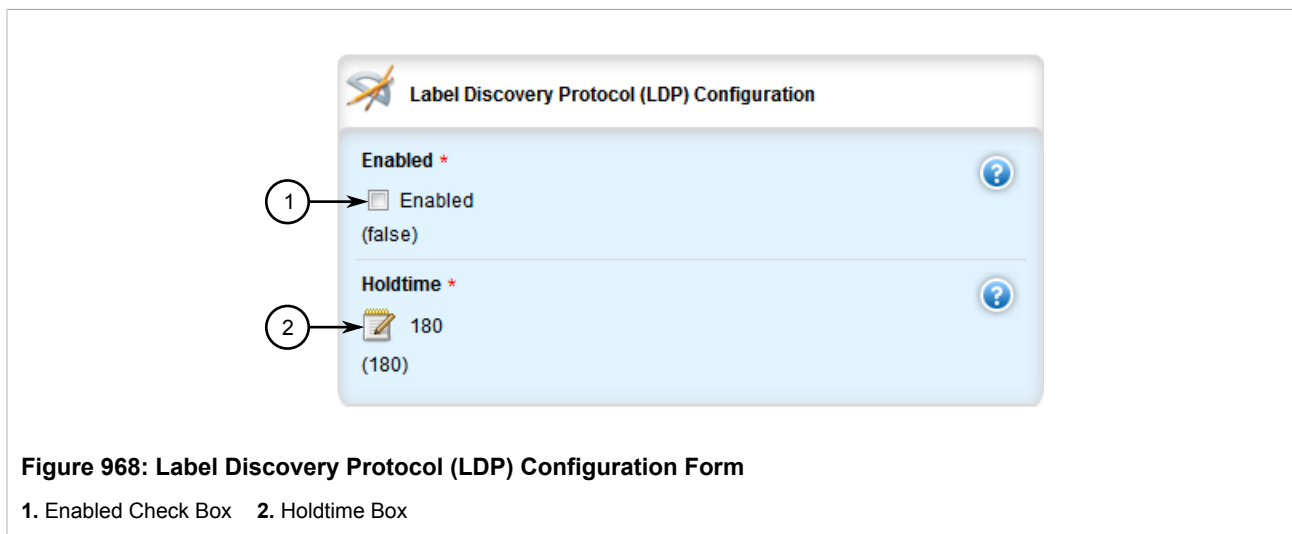
Parameter	Description
Peer ID	<b>Synopsis:</b> A string The peer ID of the LDP neighbor discovery.
Peer IP	<b>Synopsis:</b> A string The peer ID of the LDP neighbor discovery.
Interface	<b>Synopsis:</b> A string The local IP address of the LDP neighbor discovery.
Local IP	<b>Synopsis:</b> A string LDP neighbor discovery state.
Peer Hello Holdtime	<b>Synopsis:</b> A string The peer hello holdtime of the LDP neighbor discovery.
Agreed Hello Holdtime	<b>Synopsis:</b> A string The agreed upon hello holdtime (shorter holdtime of local/peer) of the LDP neighbor discovery.
Peer Session Holdtime	<b>Synopsis:</b> A string The peer session holdtime of the LDP neighbor discovery.

## Section 5.40.7.6

## Configuring LDP

To configure the LDP, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *mpls » ldp*. The **Label Discovery Protocol (LDP) Configuration** form appears.



3. Configure the following parameter(s) as required:

Parameter	Description
Enable LDP	<p><b>Synopsis:</b> true or false  <b>Default:</b> false</p> <p>A boolean flag to indicate that Label Distribution Protocol (LDP) is enabled.</p> <p><b>Prerequisite:</b> MPLS must be enabled before enabling LDP.  <b>Prerequisite:</b> MPLS static bindings must be removed before enabling LDP.</p>
LDP Holdtime	<p><b>Default:</b> 180</p> <p>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.</p>



#### NOTE

*MPLS must be enabled and MPLS label bindings must be removed before enabling LDP. Refer to [Section 5.40.3, “Enabling/Disabling MPLS Routing”](#) and [Section 5.40.5.4, “Deleting a Static Label”](#) for further information.*

4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
5. Click **Exit Transaction** or continue making changes.

#### Section 5.40.7.7

### Configuring Neighbor Discovery

To configure the LDP neighbor discovery, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to *mpls » ldp » discovery*. The **LDP Discovery Hello Configuration** form appears.

**LDP Discovery Hello Configuration**

**LDP Hello Interval \*** 5 (5)

**LDP Hello Holdtime \*** 15 (15)

**Figure 969: LDP Discovery Hello Configuration Form**

1. LDP Hello Interval Box 2. LDP Hello Holdtime Box

- Configure the following parameter(s) as required:

Parameter	Description
LDP Hello Interval	<b>Default:</b> 5 The time (in seconds) between the sending of consecutive Hello messages.
LDP Hello Holdtime	<b>Default:</b> 15 The time (in seconds) that a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.

- Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- Click **Exit Transaction** or continue making changes.

#### Section 5.40.7.8

### Viewing a List of LDP Interfaces

To view a list of LDP interfaces, navigate to **mpls » ldp » interface-ldp**. If IP interfaces have been configured, the **LDP Interface List Configuration** table appears.

**LDP Interface List Configuration**

Transport-ifname	Enabled	Transport-ip-address
fe-cm-1	false	not found
switch.0001	false	not found
switch.0010	true	192.168.10.1
switch.0020	false	not found

**Figure 970: LDP Interface List Configuration Table**

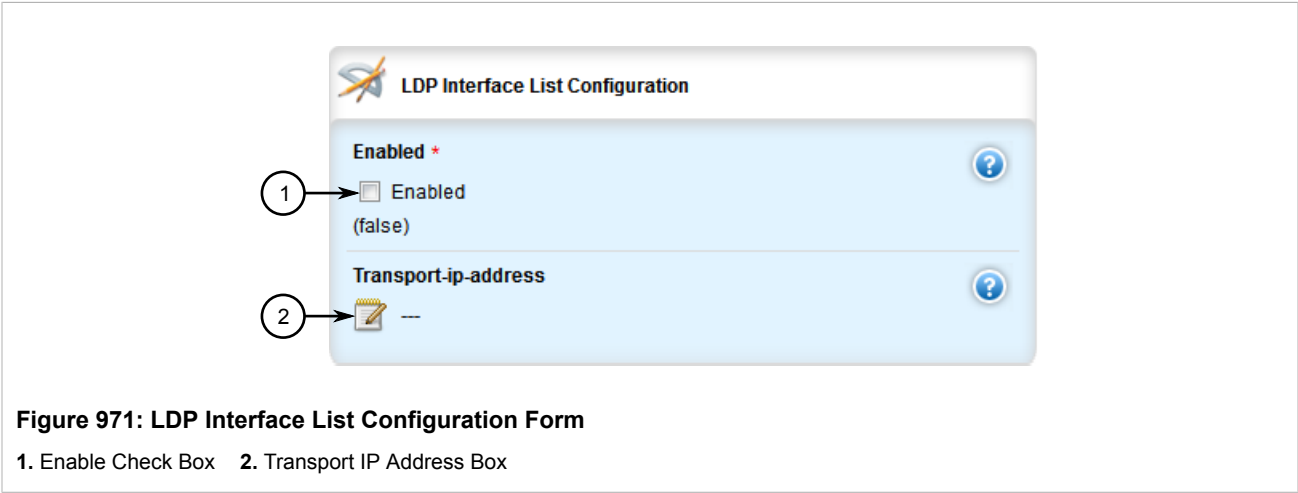
For more information about enabling LDP interfaces, refer to [Section 5.40.7.9, “Enabling/Disabling an LDP Interface”](#).

Section 5.40.7.9

Enabling/Disabling an LDP Interface

To enable or disable an LDP interface, do the following:

- 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 2. Navigate to *mpls » ldp » interface-ldp » interface* where *interface* is the name of the interface to be enabled or disabled for LDP. The **LDP Interface List Configuration** form appears.



**Figure 971: LDP Interface List Configuration Form**  
1. Enable Check Box    2. Transport IP Address Box

- 3. Configure the following parameter(s) as required:

Parameter	Description
Enabled	<b>Synopsis:</b> true or false <b>Default:</b> false A boolean flag to indicate a transport interface is LDP-enabled or not. Only LDP-enabled interfaces are used for LDP.
IP Address	<b>Synopsis:</b> A string 7 to 15 characters long or a string 6 to 40 characters long or a string The transport IP address (IPv4 or IPv6 format). If not provided, <i>interface</i> is used as the transport address.

- 4. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
- 5. Click **Exit Transaction** or continue making changes.



# 6 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 4.6.1, “Pre-Configured Alarms”](#).*

- [Section 6.1, “Feature Keys”](#)
- [Section 6.2, “Ethernet Ports”](#)
- [Section 6.3, “Multicast Filtering”](#)
- [Section 6.4, “Spanning Tree”](#)
- [Section 6.5, “VLANs”](#)

## Section 6.1

# Feature Keys

The following describes common problems related to feature keys.

Problem	Solution
A file-based feature key does not match the hardware	<p>Each file-based feature key is licensed to a particular device. When transferring a feature key from one device to another, such as when configuring a backup unit to replace a malfunctioning device, the device will detect a hardware mismatch with the key and trigger an alarm.</p> <p>Do not transfer file-based feature keys between devices. Contact a Siemens Canada Ltd. sales representative to order a feature key matching the serial numbers of the hardware in the destination device.</p>

## Section 6.2

# Ethernet Ports

The following describes common problems related to Ethernet ports.


Problem	Solution
A link seems fine when traffic levels are low, but fails as traffic rates increase OR a link can be pinged but has problems with FTP/SQL/HTTP/etc.	<p>A possible cause of intermittent operation is that of a '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.</p> <p>At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-</p>

Problem	Solution
	<p>negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable.</p> <p>The ping command with flood options is a useful tool for testing commissioned links. The command <code>ping 192.168.0.1 500 2</code> can be used to issue 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.</p>
Links are inaccessible, even when using the Logical File Inclusion (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 6.3

## Multicast Filtering

The following describes common problems related to multicast filtering.

Problem	Solution
When started, a multicast traffic feed is always distributed to all members of the VLAN.	Is IGMP enabled for the VLAN? Multicasts will be distributed to all members of the VLAN unless IGMP is enabled.
Computers connected to the switch receive multicast traffic, but not when they are connected to a router.	<p>Is the port used to connect the router included in the Router Ports list?</p> <p>To determine whether the multicast stream is being delivered to the router, view the statistics collected for switched Ethernet ports. For more information, refer to <a href="#">Section 3.18.4, "Viewing Switched Ethernet Port Statistics"</a>.</p> <p>Verify the traffic count transmitted to the router is the same as the traffic count received from the multicasting source.</p>
The video stream at an end station is of poor quality.	<p>Video serving is a resource-intensive application. Because it uses isochronous workload, data must be fed at a prescribed rate or end users will see glitches in the video. Networks that carry data from the server to the client must be engineered to handle this heavy, isochronous workload. Video streams can consume large amounts of bandwidth. Features and capacity of both server and network (including routers, bridges, switches and interfaces) impact the streams.</p> <p>Do not exceed 60% of the maximum interface bandwidth. For example, if using a 10 Mbps Ethernet, run a single multicasting source at no more than 6 Mbps, or two sources at 3 Mbps. It is important to consider these ports in the network design, as router ports will carry the traffic of all multicast groups.</p> <div><b>IMPORTANT!</b> <i>Multicasting will introduce latency in all traffic on the network. Plan the network carefully in order to account for capacity and latency concerns.</i></div>
Multicast streams of some groups are not forwarded properly. Some segments without subscribers receive the traffic, while some segments with subscribers do not.	Make sure different multicast groups do not have multicast IP addresses that map to the same multicast MAC address. The switch forwarding operation is MAC address-based and will not work properly for several groups mapping to the same MAC address.
Computers on the switch issue join requests, but do not receive multicast streams from a router.	Is the multicast route running IGMP version 2? It must run IGMP version 2 in order for IGMP Snooping to operate properly.
Unable to connect or disconnect some switch ports, and multicast goes everywhere. Is IGMP broken?	<p>IGMP is not broken. This may in fact be proper switch behavior.</p> <p>When the switch detects a change in the network topology through RSTP, it acts to avoid loss of multicast traffic. If configured to do so, it starts forwarding all multicast traffic to all ports that are not RSTP Edge ports (because they may potentially link to routers). This may result in some undesired flooding of multicast traffic, which will stop after a few minutes.</p>

Problem	Solution
	<p>However, it guarantees that all devices interested in the traffic will keep receiving it without interruption.</p> <p>The same behavior will be observed when the switch resets or when IGMP Snooping is being disabled for the VLAN.</p>

## Section 6.4

## 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.	<p>If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to <a href="#">The network becomes unstable when a specific application is started</a>.</p> <p>Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.</p>
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	<p>Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up.</p> <p>Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port's point-to-point setting to true.</p> <p>Either one will allow the Proposal-Agreement protocol to be used.</p>
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	<p>Is it possible that some ports participating in the topology have been configured to STP mode or that the port's point-to-point parameter is set to false? STP and multi-point ports converge slowly after failures occur.</p> <p>Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow.</p> <p>Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst of all possible designs occurs when the secondary root bridge is located</p>

Problem	Solution
	at the farthest edge of the network from the root. In this case, a configuration message will have to propagate out to the edge and then back in order to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An IED/controller does not work with the device.	Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port.  If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller's bridge to STP.
Polls to other devices are occasionally lost.	Review the network statistics to determine whether the root bridge is receiving TCNs around the time of observed frame loss. It may be possible there are problems with intermittent links in the network.
The root is receiving a number of TCNs. Where are they coming from?	Examine the RSTP port statistics to determine the port from which the TCNs are arriving. Sign-on to the switch at the other end of the link attached to that port. Repeat this step until the switch generating the TCNs is found (i.e. the switch that is itself not receiving a large number of TCNs). Determine the problem at that switch.

## Section 6.5

## VLANs

The following describes common problems related to the VLANs.

Problem	Solution
VLANs are not needed on the network. Can they be turned off?	Yes. Simply leave all ports set to type <i>edge</i> and leave the native VLAN set to 1. This is the default configuration for the switch.
Two VLANs were created and a number of ports were made members of them. Now some of the devices in one VLAN need to 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.